Universidad Nacional Autónoma de Nicaragua
Recinto Universitario "Rubén Darío"
Facultad de Ciencias e Ingenieria
Departamento de Computación

Seminario de Graduación

Tema:

Computación Forense

Sub tema:

Metodología de informática forense para el tratamiento de Evidencias en Servidores Windows

AUTORES:

- **Br. María José Sotelo Castro**
- **Br. Eli Antonio Areas Jarquín**
- **Br. Zabdiel José Zepeda Vega**

TUTOR:

Lic. Juan de Dios Bonilla Anduray

Martes 07 de Junio de 2011

AGRADECIMIENTO

Agradecemos primeramente a Dios nuestro creador por haber permitido cumplir uno de nuestros mayores anhelos, finalizar nuestros estudios universitarios.

A nuestros padres por sus sacrificios, esfuerzos, y gran empeño para que lográramos salir adelante en nuestras metas.

De igual forma a nuestro tutor el Lic. Juan de Dios Bonilla Anduray por su paciencia, dedicación y apoyo en todo este tiempo.

Así mismo queremos agradecer al personal del Proyecto TIC de la UNAN-Managua y a todas aquellas personas que nos brindaron su valioso tiempo y ayuda en la realización de este trabajo.

Y a todos nuestros maestros por habernos trasmitirnos sus conocimientos para que fuéramos profesionales de éxito.

Los autores

DEDICATORIA

Dedico el presente trabajo primeramente a Dios por haberme dado la sabiduría para concluir una de mis grandes metas, alcanzar mi carrera universitaria.

A mis padres por su sacrificio y apoyo incondicional, al brindarme la confianza e inspiración para hacer de mis sueños una realidad.

Y a todas aquellas personas que me han aconsejando en momentos difíciles.

María José Sotelo

DEDICATORIA

Dedico este trabajo a mis padres por todo el apoyo y sacrificio brindado para hacer de mí un excelente profesional, y por darme fuerzas para poder finalizar mis estudios.

A mi esposa Jessika Ortiz Ulloa, por su amor, comprensión y por sus buenos deseos a lo largo de todo este tiempo.

A todos mis amigos que me han ayudado a lograr mis metas que me he propuesto.

Eli Antonio Areas

DEDICATORIA

Este trabajo se lo dedico especialmente a Dios por ser mi mejor amigo y por apoyarme en todos los momentos difíciles de mi vida. Por darme sabiduría y entendimiento. Gracias señor por escuchar mis oraciones.

A mis padres por apoyar y comprender mis decisiones, por todo el amor que me dieron, por todo el esfuerzo y sacrificio realizado.

A mí querida esposa y amiga Natalia Lam, por todo el amor, cariño, entusiasmo, consejos y por toda su dedicación para que mi vida sea cada día mejor.

A mis queridos hermanos, por todo el esfuerzo y lucha para que saliera adelante.

A mis amigos y compañeros de trabajo que día a día me ayudan y comparten sus conocimientos.

Zabdiel J. Zepeda Vega.

Metodología de informática forense para el tratamiento de Evidencias en Servidores Windows

RESUMEN

La administración o gestión de seguridad de la información, tiene como objetivo salvaguardar la confidencialidad, integridad y disponibilidad de la información escrita, hablada y electrónica.

La revisión y aseguramiento de estos factores han formado parte de la agenda de los profesionales en informática desde siempre. Sin embargo, la complejidad y evolución continua de los sistemas de comunicación, sumado a la creciente estadística de ataques y sabotajes informáticos, han convertido estos temas en una preocupación central de cualquier administración de sistemas.

En la actualidad los delincuentes están manipulando la tecnología para facilitar el acometimiento de infracciones. Estos acontecimientos han creado a nivel mundial la necesidad de que instituciones como policía judicial, y ministerios públicos deban capacitarse y en ocasiones especializarse en estas nuevas áreas en donde las **Tecnologías de la Información y la Comunicaciones**, se convierten en herramientas necesarias en auxilio de la justicia y persecución de delitos y delincuente.

El acceso universal a tecnologías de la información y la comunicación (TIC) brinda nuevas oportunidades para que, delincuentes, pornógrafos infantiles, artistas del engaño, quienes realizan toda clase de ataques contra información no autorizada, fraudes informáticos, y para los que atacan la integridad de los sistemas computacionales y de red, actúen de forma excesiva sin que la justica pueda hacer algo, ya que estos han quedado relegados en sus actuaciones por falta de recursos tecnológicos especialmente en los delitos informáticos.

Por tal razón países como Estados Unidos, Alemania o Inglaterra, han creado y desarrollado técnicas y herramientas informáticas a fin de lograr tanto el descubrimiento de los autores de dichas infracciones así como asegurar la prueba de estas.

Una de las herramientas es la informática forense, ciencia criminalística que con el apoyo y utilización de las Tecnologías de la Informática y de la Comunicación, está adquiriendo una gran importancia debido a la globalización de la sociedad de la información. Pero a pesar de esto la ciencia no tiene un método estandarizado, razón por la cual con la presente investigación se **define una metodología de informática forense para el tratamiento de Evidencias en Servidores Windows,** basada en técnicas y guías relacionadas a las mejores prácticas para recolectar y archivar evidencia, y en función a la seguridad informática. La metodología será aplicada en el servidor de Kaspersky del Proyecto TIC, con el propósito de buscar posibles evidencias de ataques, modificación y borrado de la información contenida en dicho servidor para el esclarecimiento de posibles vulnerabilidades que aún no han sido identificadas por los administradores de servidores.

INTRODUCCIÓN

En la medida que crece y se diversifica el uso de Infraestructuras Tecnológicas, se incrementan también los riesgos de que los equipos de cómputo, dispositivos electrónicos y sistemas informáticos, conectados o no a Internet, sean vulnerables a ataques o incidentes que ponen en peligro la integridad, disponibilidad y autenticidad de los datos que en ellos se procesa, almacena o transfiere. Y más allá de los datos, el daño a dichas infraestructuras es latente. Una de las fases más importantes de la respuesta a incidentes consiste en la **investigación** del incidente para saber porque se produjo la intrusión, quien la perpetró y sobre que sistemas. Esta investigación se conoce como **análisis forense**.

En la actualidad, las actividades de los investigadores de cómputo forense, presentan retos cada vez más exigentes para rastrear y detectar un incidente (ataque), debido a las técnicas utilizadas por los intrusos, las cuales tienden a ser más sofisticadas y efectivas en los sistemas informáticos.

La informática forense, aplicando procedimientos estrictos y rigurosos puede ayudar a resolver grandes crímenes apoyándose en el método científico, aplicado a la recolección, análisis y validación de todo tipo de pruebas digitales. Con el crecimiento del uso de internet, se incrementa el número de acciones ilegales contra la seguridad de las redes corporativas. Por lo cual es necesario planificar, analizar e implantar sistemas y políticas de seguridad, así como establecer medidas de control, planes de contingencia y realizar auditorías sobre los sistemas implantados y su correcto cumplimiento.

La informática forense o cómputo forense no tiene parte preventiva, es decir, la informática forense no se encarga de prevenir delitos, para ello se encarga la seguridad informática, es importante tener claro el marco de actuación entre la informática forense, la seguridad informática y la auditoría informática.

El presente trabajo está orientado al tratamiento de evidencias informáticas para el servidor de aplicación Kaspersky ubicado en las instalaciones del Proyecto de Tecnología de Comunicación e Información de la UNAN-Managua.

La metodología de informática forense aplicada para el tratamiento de evidencias informáticas en el servidor kaspersky bajo el entorno de Microsoft Windows Server 2008 permite un enfoque lógico para evaluar el riesgo, detallando las mejores prácticas para identificar, medir, monitorear y controlar los riesgos de seguridad digital.

La aplicación de la metodología de informática forense desarrollada para el tratamiento de evidencias en el servidor Kaspersky permite a los administradores de tecnología informática del Proyecto TIC de la UNAN-Managua conocer las evidencias encontradas y el grado de seguridad en dicho servidor, con el objetivo de prevenir futuras eventualidades a través de controles de seguridad.

ANTECEDENTES

El presente estudio es una primera investigación realizada en la aplicación de metodologías de informática forense para el tratamiento de evidencias en el servidor de Kaspersky del proyecto TIC.

En el proyecto TIC no existe documentación de investigación previas referente a metodologías de informática forense para el tratamiento de evidencias que hayan sido utilizadas en el servidor de Kaspersky.

Las fuentes donde se consultó la bibliografía existente fueron, las oficinas del proyecto TIC, el centro de documentación del Departamento de Computación, y la biblioteca "Salomón de la Selva" de la UNAN-Managua.

DEFINICION DEL PROBLEMA OBJETO DE ESTUDIO

Caracterización del Problema

En informática, un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse al ordenador físico en el cual se ejecutan las aplicaciones, una máquina cuyo propósito es proveer servicios de modo que otras máquinas puedan hacer uso de los mismos. Un servidor sirve información a los ordenadores que se conecten a él. Cuando los usuarios se conectan a un servidor pueden acceder a programas, archivos y otra información del servidor.

En la actualidad los ataques más comunes que se presentan en los servidores son:

1. Ataques de **"Crimeware"** que son programas maliciosos que se instalan de manera encubierta en un servidor. La mayoría de los programas maliciosos o "crimeware" están constituidos por troyanos.
2. Ataque de **hackers** que con regularidad penetran en servidores y en grandes redes. Una vez adentro, pueden instalar programas maliciosos, robar información confidencial, o incluso usar los ordenadores cautivos para distribuir correos spam.
3. Ataque **phishing** que es una forma específica de ciber delincuencia. El ciber delincuente crea una réplica casi perfecta del sitio Web de una institución financiera, luego intenta engañar al usuario para que revele su información confidencial.

En Nicaragua se han presentando los siguientes ataques a Servidores:

1. Bloqueo de 179 sitios web provocados por el ataque de un hacker a los sistemas de Cablenet o Claro TV. El hacker logro control y acceso total, logró hacer una copia completa de la información contenida en el sistema de alojamiento de Cablenet.
2. Acceso al servidor del Consejo Supremo Electoral (CSE).
3. Ataques de "Crimeware" que son programas maliciosos que se instalan de manera encubierta en un servidor.

Delimitación del Problema

El Proyecto TIC de la UNAN Managua, no escapa de estos problemas aunque cuente con un servidor de antivirus (**Kaspersky Lab**). Debido al creciente desarrollo de nuevas estrategias de ataques a servidores, se aplicará el uso de la(s) metodología(s) de informática forense más adecuada(s) para detectar algún posible incidente al que este latente el servidor de kaspersky, debido al crecimiento de la infraestructura de red de la UNAN - Managua.

Formulación del Problema

Podrá la aplicación de la metodología de informática forense mediante el uso de sus herramientas detectar evidencias de posibles incidentes ocurridos en el servidor de kaspersky del proyecto TIC.

Sistematización del problema

- Cuál es el estado del servidor de Kaspersky del proyecto TIC en cuanto al manejo de incidentes?
- Cuáles son las políticas y procedimientos a seguir que el proyecto TIC aplica al servidor actualmente?
- Cómo está la plataforma tecnológica del servidor de Kaspersky del proyecto TIC?
- Cómo fortalecer la seguridad y el manejo del servidor de Kasperky en el proyecto TIC?

OBJETIVO

Objetivo General:

- Desarrollar una metodología de informática forense para el tratamiento de Evidencias en Servidores Windows adecuada al Servidor de Kaspersky del proyecto TIC.

Objetivos Específicos:

1. Describir las metodologías de informática forense de detección y manipulación de evidencias ante delitos informáticos.

2. Elaborar un diagnóstico de hallazgos encontrados a través de la metodología seleccionada.

3. Valorar la efectividad de la metodología utilizada mediante el uso de herramientas de informática forense.

MARCO TEORICO

1.1 Metodologías

1.1.1 Definición de Metodologías

Una metodología es una guía que se sigue a fin de realizar las acciones propias de una investigación. En términos más sencillos se trata de la guía que nos va indicando qué hacer y cómo actuar cuando se quiere obtener algún tipo de investigación. Es posible definir una metodología como el enfoque que permite observar un problema de una forma total, sistemática, y disciplinada.

Al intentar comprender la definición que se hace de lo que es una metodología, resulta de suma importancia tener en cuenta que una metodología no es lo mismo que la técnica de investigación. Las técnicas son parte de una metodología, y se define como aquellos procedimientos que se utilizan para llevar a cabo la metodología, por lo tanto, como es posible percibir, es uno de los muchos elementos que incluye.

En el contexto de la investigación son muchas las metodologías que es posible seguir, sin embargo, existen 2 grandes grupos que incluyen a otras más específicas. Se trata de la metodología de investigación cuantitativa y la cualitativa.

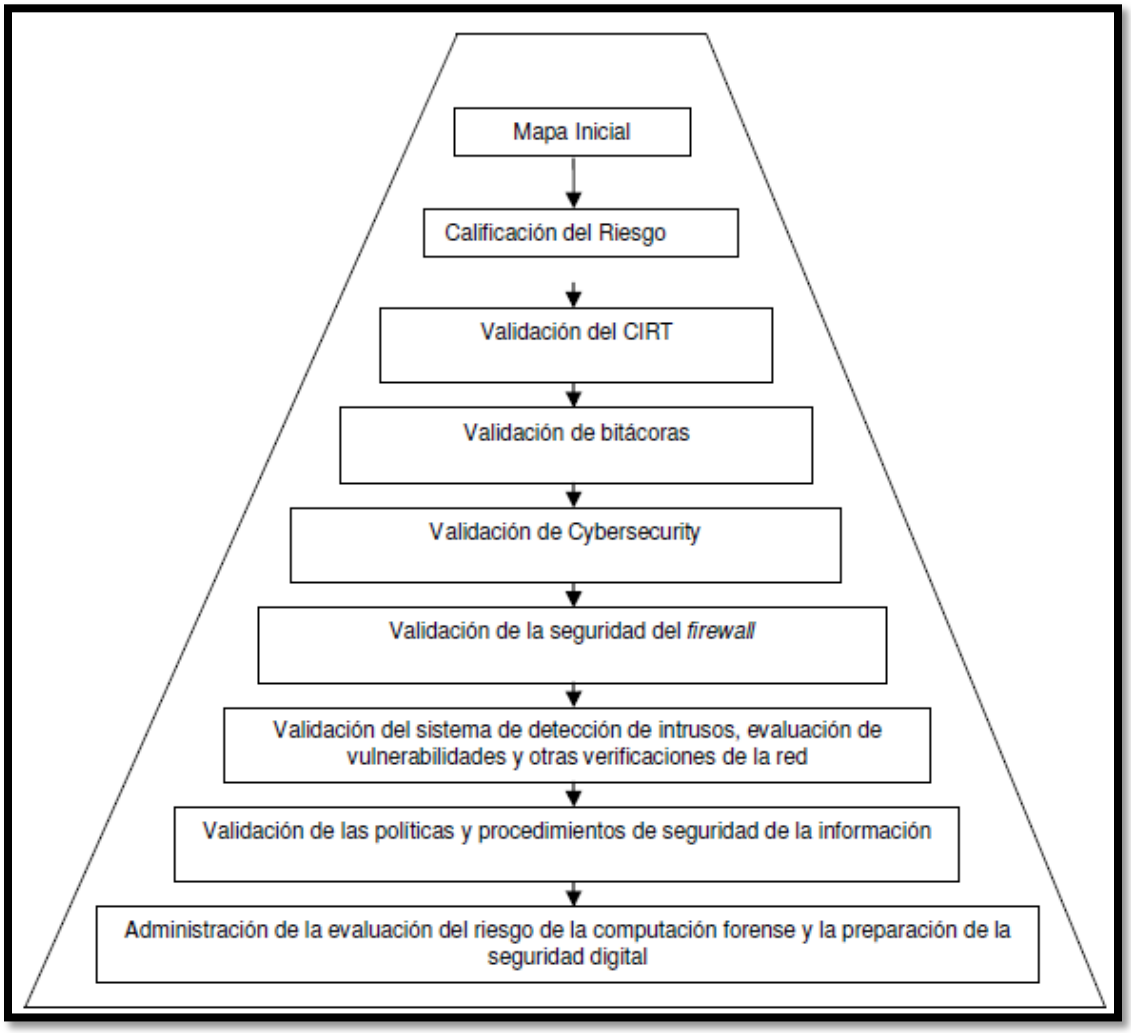
La metodología cuantitativa es aquella que permite la obtención de información a partir de la cuantificación de los datos sobre variables, mientras que la metodología cualitativa, evitando la cuantificación de los datos, produce registros narrativos de los fenómenos investigados. En este tipo de metodología los datos se obtienen por medio de la observación y las entrevistas, entre otros. Como vemos, la diferencia más importante entre la metodología cuantitativa y la cualitativa radica en que la primera logra sus conclusiones a través de la correlación entre variables cuantificadas, y así poder realizar generalizaciones y producir datos objetivos, mientras que la segunda estudia la relación entre las variables obtenidas a partir de la observación en contextos estructurales y situacionales.

1.1.2 Tipos de metodologías aplicables a la informática Forense

1.1.2.1 El modelo de gobernanza de seguridad digital

La computación Forense y el Modelo de Gobernanza de Seguridad (figura 1), proveen un enfoque lógico para evaluar el riesgo. Específicamente, el aseguramiento de los procedimientos de tecnología es desarrollado como un componente mayor de la computación forense y la metodología de verificación de la seguridad digital para proveer la estructura del proceso de enfoque en riesgo.

Figura 1. La Computación Forense y el Modelo de Gobernanza de Seguridad Digital1



Fuente www.isaca.org

El gobierno corporativo sobre la computación forense y la seguridad digital es un aliado entre los empleados, administradores, el comité de auditoría, los directores y consultores. Establecer una relación con cada individuo dentro de la organización es crucial para el éxito del establecimiento y mantenimiento de un modelo de gobernanza funcional.

La ejecución y la autoridad del modelo de gobernanza son regularmente implementadas por un profesional de aseguramiento tecnológico. La cadena de comunicación inicia desde el campo del auditor o evaluador, quien reporta al supervisor, luego al jefe del departamento tecnológico y por último al gerente de la organización.

Las conclusiones alcanzadas y las recomendaciones finales del equipo de aseguramiento tecnológico son comunicadas al comité de auditoría y finalmente al grupo de directores. Cualquier material de tareas de alto riesgo es reportado al personal de seguridad como garantía.

El modelo de proceso de Gobernanza

Este modelo ejecuta tres pasos para el uso efectivo del modelo de gobernanza y para entender si existe o no una intersección entre la seguridad de la información y la computación forense. El plan primario utilizado para llevar a cabo la evaluación de riesgo es la evaluación del proceso del modelo contenido dentro de esta sección para cada uno de los siguientes pasos:

1. **Evaluación del aseguramiento del riesgo de la seguridad de la información (prevención):** Entender el único perfil de riesgo de la información en una organización depende de su infraestructura (sistema operativo, red, etc.) y las aplicaciones. La administración de la organización necesita entender los riesgos específicos de la información asegurando que una evaluación continua es realizada.

   Al finalizar la verificación de los procedimientos del modelo, se elabora una tabla de evaluación del riesgo identificada con colores, basado en la administración de riesgo de la información que fue percibido (ver figuras 2 y 3).

2. **Evaluar la computación forense (detección):** El modelo funciona con una capacidad dual, ambas para el aseguramiento del riesgo de la información (prevención) y para la realización de un análisis forense postmorten (detección) al sospecharse un ingreso no autorizado. Al realizar este paso se provee a la gerencia de un entendimiento claro de las debilidades y vulnerabilidades en la seguridad de la información no identificadas en el paso 1. Al completar este paso de la verificación del proceso del modelo, una tabla de evaluación con colores es preparado para mostrar la administración actual de los riesgos de la información (Ver figuras 2 y 3).

3. **Análisis de la intersección entre la seguridad de la información y la computación forense:** Las tablas de evaluación obtenidas en la seguridad de la información (prevención) y la computación forense (detección), completados en el paso 1 y 2, pueden ahora ser analizados. Específicamente, el análisis de seguridad de la información necesita ser comparado con los hallazgos de las dos tablas para identificar semejanzas y desigualdades entre las dos tablas de evaluación.

   Una intersección existe cuando las calificaciones de prevención y detección son iguales en las tablas de evaluación, lo cual demuestra la validez original de la administración del riesgo (prevención), basado en el análisis de la computación forense efectuada en el paso 2. Una intersección no existe cuando hay disparidad en las calificaciones asignadas a los procesos de la evaluación del riesgo (prevención) y la Computación Forense (detección).

Figura 2. **Metodología de verificación de la Computación Forense y la Seguridad Digital**

Responsabilidad	**Responsabilidad**	**Responsabilidad**	**Responsabilidad**	**Responsabilidad**	**Responsabilidad**
Auto evaluación de la Administración superior	Aseguramiento de la seguridad de la información y las autoridades	Aseguramiento de la seguridad de la información y las autoridades	Aseguramiento de la seguridad de la información y las autoridades	Aseguramiento de la seguridad de la información y las autoridades.	Aseguramiento de la seguridad de la información y las autoridades
Computación Forense	**Computación Forense**	**Computación Forense**	**Computación Forense**	**Computación Forense**	**Computación Forense**

Evaluación de la administración del riesgo ejecutado por la administración como un riesgo de auto aseguramiento **(Revisión del proceso)**	Evaluación del riesgo de la seguridad digital; **"evaluación del proceso"** ejecutado por las autoridades	Evaluación del riesgo de la seguridad digital; **"evaluación del proceso"** ejecutado por las autoridades	Evaluación del riesgo de la seguridad digital; **"revisión de la practica"** ejecutada por aseguramiento y las autoridades	Evaluación del riesgo de la seguridad digital; "la tabla de calificación final" ajustada por aseguramiento y las autoridades luego de una verificación forense	Evaluación del riesgo de la seguridad digital; **"proceso de reporte"** ejecutado por aseguramiento y las autoridades

PASO 1	**PASO 4**	**PASO 6**	**PASO 7**	**PASO 10**	**PASO 11**
Realizar los procedimientos de verificación del modelo de Gobernanza de la computación Forense y Seguridad Digital	Evaluar la tabla de calificación del proceso de riesgo para completar y precisión contra la computación forense, las políticas de seguridad digital y procesos (políticas y procedimientos).	Desarrollar un documento de conclusión del proceso que describa las fortalezas y debilidades del proceso de la computación forense y la seguridad digital **(políticas y procedimientos)**	Realizar la verificación de las prácticas y procedimientos de la computación Forense y la Seguridad Digital.	Realizar una revisión de las tablas de evaluación de los procesos y las prácticas de riesgo y el mapa final basado en una completa revisión de los procedimientos de la computación Forense y la seguridad Digital.	Desarrollar un reporte Ejecutivo que contenga la conclusión final de los riesgos de la Computación Forense y la Seguridad Digital.

PASO 2	**PASO 5**		**PASO 8**		
Llenar las tablas de calificación de procesos y prácticas de riesgo	Verificar los procesos de verificación de Computación Forense y aseguramiento del Riesgo de seguridad digital **(verificación de procesos, políticas y procedimientos)**		Evaluar la tabla de evaluación de la administración del riesgo contra los resultados obtenidos en el paso 7		
PASO 3			**PASO 9**		
Desarrollar el mapa final (Una consolidación de las tablas de calificación en colores)			Desarrollar un documento describiendo las fortalezas y debilidades de la Computación Forense y la Seguridad Digital.		

Figura 3: La Computación Forense y la Gobernanza de la Seguridad Digital

Modelo: Criterio de evaluación del riesgo

A	B	C	D	E
Confidencialidad	**Confidencialidad**	**Confidencialidad**	**Confidencialidad**	**Confidencialidad**
Las políticas y procedimientos de seguridad proveen fuertes controles documentados para proteger la confidencialidad de la información.	Las políticas y procedimientos de seguridad proveen adecuados controles documentados para proteger la confidencialidad de la información	Las políticas y procedimientos de seguridad digital necesitan reforzarse para asegurar fuertes controles documentados para proteger la confidencialidad de la información.	Las políticas y procedimientos de seguridad son inadecuados para asegurar la existencia de fuertes controles documentados para proteger la confidencialidad de la información.	Las políticas y procedimientos de seguridad son muy deficientes para proveer fuertes controles documentados para proteger la confidencialidad de la información.

Integridad	Integridad	Integridad	Integridad	Integridad
Las políticas y procedimientos de seguridad digital **protegen fuertemente la integridad de los datos** por medio de altos niveles de autenticidad y responsabilidad.	Las políticas y procedimientos de seguridad digital **protegen adecuadamente la integridad de los datos** por medio de altos niveles de autenticidad y responsabilidad.	Las políticas y procedimientos de seguridad digital **necesitan reforzarse para asegurar que existe un nivel alto de integridad de los datos** por medio de altos niveles de autenticidad y responsabilidad.	Las políticas y procedimientos de seguridad digital **son inadecuados para asegurar que existe un nivel alto de integridad** por medio de altos niveles de autenticidad y responsabilidad.	Las políticas y procedimientos de seguridad digital **son críticamente deficientes para asegurar que existe un nivel alto de integridad de los datos** por medio de altos niveles de autenticidad y responsabilidad.

Disponibilidad	Disponibilidad	Disponibilidad	Disponibilidad	Disponibilidad
Las políticas y procedimientos de seguridad **proveen un alto estándar de control interno para proteger la disponibilidad en el tiempo de los recursos IT.**	Las políticas y procedimientos de seguridad digital **proveen estándares razonables de control interno para proteger la disponibilidad de los recursos de IT.**	Las políticas y procedimientos de seguridad **necesitan ser mejoradas para proteger la disponibilidad de los recursos IT.**	Las políticas y procedimientos de seguridad **son inadecuados para proteger disponibilidad de los recursos de IT en el tiempo.**	Las políticas y procedimientos de seguridad **son críticamente deficientes y requieren mejoras de fondo para proteger la disponibilidad de los recursos de IT en el tiempo.**

Como un resultado de la disparidad de las calificaciones de riesgo, será necesaria mayor investigación, un análisis de la raíz de la causa y los problemas resueltos para prevenir futuras ocurrencias de las vulnerabilidades de la seguridad digital.

En la figura 5 están incluidos los procedimientos que deben de ser ejecutados por los profesionales de aseguramiento y reguladores cuando se esté implementando el Modelo de Gobernanza de Seguridad Digital y de Computación Forense.

Figura 4: **Referencia de preparación para Computación Forense y Seguridad Digital**

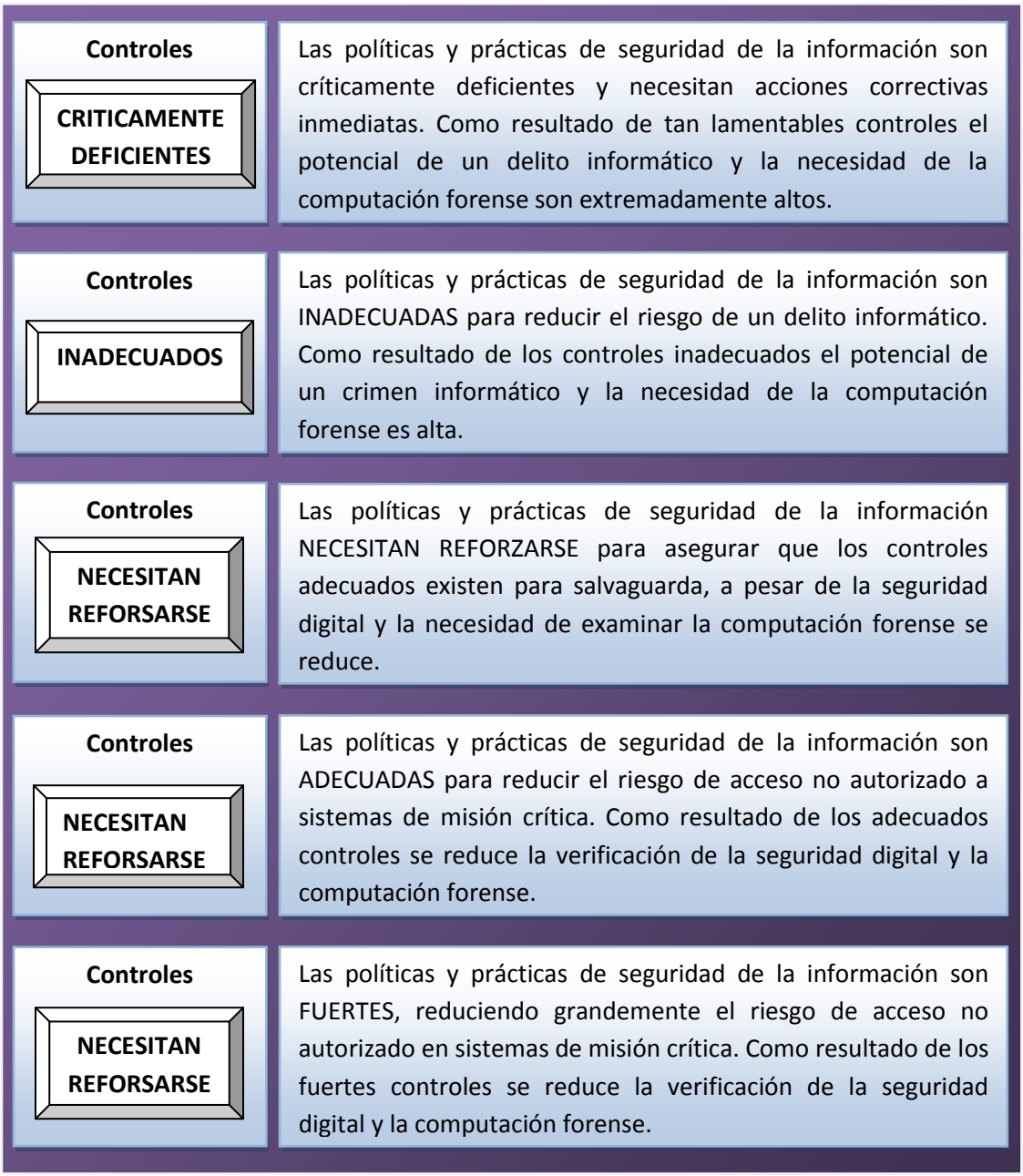


Figura 5. Modelo de gobernanza de la Computación Forense y la seguridad Digital

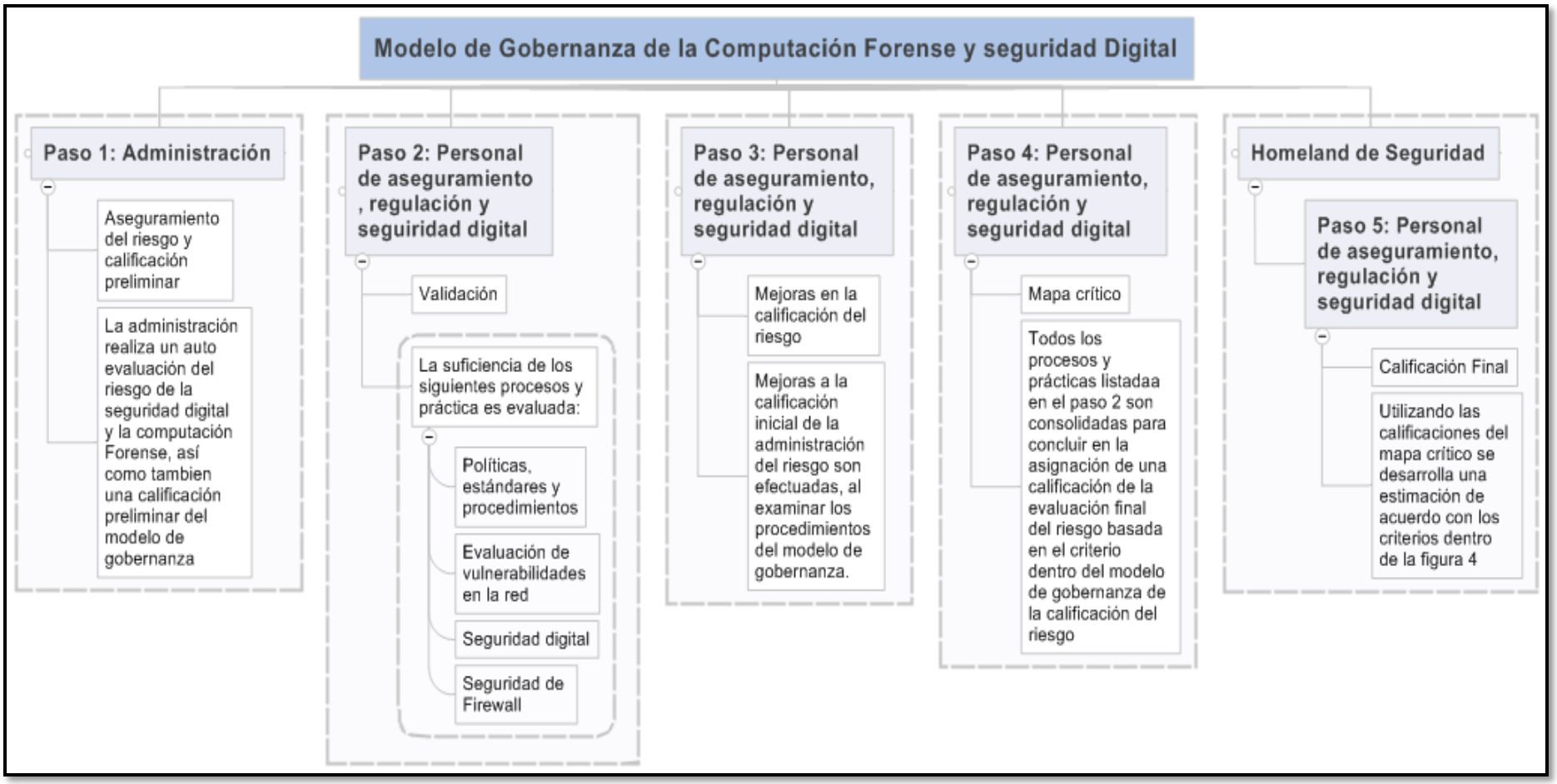


Figura 6. Metodología de los procesos de la computación Forense y la seguridad Digital.

El principal objetivo de la Computación Forense y el Modelo de Gobernanza de seguridad digital es establecer el marco de referencia inicial de Gobernanza que intentara clarificar el rol del aseguramiento de la tecnología al entender el riesgo y los controles que gobiernan la computación forense y la seguridad preventiva de la información.

Al elevar el sentimiento y conocimiento de los riesgos y los controles que gobiernan la computación forense y sus relaciones en las defensas preventivas en la seguridad de la información es crítica para desarrollar controles adecuados necesarios para la salvaguarda de los sistemas de información contra los delitos informáticos y prevenir la necesidad de la computación forense.

Al final el riesgo existe debido a la carencia general de un claro entendimiento de la computación forense y la seguridad digital alrededor de los profesionales de aseguramiento a personal de seguridad de IT.

1.1.2.2 Metodología RFC3227

El "RFC 3227: Guía Para Recolectar y Archivar Evidencia" (Guidelines for Evidence Collection and Archiving) [GuEvCo02], escrito en febrero de 2002 por Dominique Brezinski y Tom Killalea, ingenieros del Network Working Group. Es un documento que provee una guía de alto nivel para recolectar y archivar datos relacionados con intrusiones. Muestra las mejores prácticas para determinar la volatilidad de los datos, decidir que recolectar, desarrollar la recolección y determinar cómo almacenar y documentar los datos. También explica algunos conceptos relacionados a la parte legal.

El RFC 3227 presenta la siguiente estructura:

- **Principios durante la recolección de evidencia**: orden de volatilidad de los datos, cosas para evitar consideraciones de privacidad y legales.
- **El proceso de recolección:** transparencia y pasos de recolección.
- **El proceso de archivo:** la cadena de custodia, donde y como archivar.

El propósito de la RFC 3227 es ofrecer a los administradores de sistemas guías para adelantar la recolección y manejo de evidencia digital relevante a un incidente de seguridad. Tal recolección representa un esfuerzo considerable de parte de los administradores, dada la carga de las labores que desarrollan y los esfuerzos de afinamiento constante de los servicios y aplicaciones de las cuales son responsables. Si la evidencia es recogida de una manera adecuada, habrá mayores posibilidades de establecer una ruta hacia los atacantes y contar con mayores elementos probatorios en el evento de una persecución y juzgamiento del intruso.

1. (RFC3227) Daniel Fernández, Bleda, "Informática Forense"

Entre las principales directrices de la guía RFC 3227 están:

- Mantener adherencia estricta a su política de seguridad organizacional y su relación formal con el equipo de atención de incidentes y las personas responsables del campo jurídico.
- Capturar la escena del incidente lo más preciso posible.
- Mantener notas detalladas, así como fechas y horas.
- Establecer las diferencias entre el reloj del sistema y la hora de referencia internacional, GMT.
- Estar preparado para testificar, detallando las acciones adelantadas.
- Minimizar los cambios en los datos que ha recolectado (Evitar la actualización de horas o fechas en archivos y directorios)
- Primero recolectar la información y luego analizar los hallazgos.
- En la revisión de cada dispositivo o mecanismo presente en el incidente, se debe seguir un acercamiento metódico para la recolección de evidencia. La rapidez y claridad es crítica para una adecuada y oportuna recolección de evidencia.
- Recolectar la evidencia desde la volátil a la menos volátil:
    - Registros, caché
    - Tablas de enrutamiento, tabla de procesos, estadísticas del kernel, memoria
    - Sistema de archivos temporales
    - Diskettes
    - Registro remoto y datos de monitoreo relevante al sistema en estudio
    - Configuración física, Topología de la red
    - Medios de almacenamiento
- Realizar una o varias copias bit a bit del medio de almacenamiento, con el fin de utilizar una de las copias para efectuar sus análisis, preservando el medio original.

- Ejecutar programas de recolección de evidencia apropiados, que protejan adecuadamente los medios originales.
- No ejecutar programas que modifiquen las fechas de acceso a todos los archivos del sistema.
- Al desconectar dispositivos de acceso externo, note que una simple desconexión o filtro de la red puede disparar la alarma de "switches caídos" que una vez detectados pueden eliminar evidencia en la red.

Como se puede observar el RFC 3227 ofrece una guía genérica que puede ser utilizada como marco conceptual básico para incorporarse en las organizaciones al crear grupos de atención de incidentes.

1.1.2.3 CTOSE (Cyber Tools On-Line Search for Evidence)

CTOSE (Cyber Tools On-Line Search for Evidence) es un proyecto de investigación mantenido por la Comisión Europea. Es un proyecto legal diseñado para estudiar los métodos de autenticación para la prueba electrónica en los casos de delitos informáticos a fin de que estas pruebas puedan ser admisibles en procesos judiciales. El proyecto ayuda a identificar, asegurar, integrar y presentar pruebas electrónicas en línea relacionados con los delitos y también asegura la admisibilidad legal de dicha información.

La metodología fue desarrollada para contrarrestar el aumento de la delincuencia cibernética en Europa. Los registros electrónicos, tales como registros de una red informática, correos electrónicos, archivos de procesamiento de textos y archivos de imágenes se recogen a menudo como evidencia en casos criminales en línea.

El proyecto CTOSE se completó el 30 de septiembre de 2003. En el desarrollo de este proyecto participó la empresa francesa Alcatel, la compañía de seguridad británica QinetiQ.

También la Universidad de Namur (Bélgica), la de Saint Andrews (Reino Unido) y la Universidad de Stuttgart (Alemania). También participaron 50 expertos de Europa y los Estados Unidos, con una amplia gama de fondos especializados, tales como Computer Emergency Response Teams, abogados, proveedores de herramientas de informática forense, investigadores de la policía de alta tecnología, y el personal de seguridad de las principales instituciones financieras.

CTOSE ha desarrollado algunas herramientas, tales como:

• **Cyber-Crime Advisory Tool (the C*CAT tool):** Notifica a los investigadores, en todas las fases de una investigación, los procedimientos y decisiones.

• **Asesor Legal:** Ofrece asesoramiento sobre los aspectos jurídicos y de procedimiento de las investigaciones de equipo. Señala los requisitos legales a los investigadores y asegura que la evidencia recogida es admisible, convincente.

• **Especificación basada en XML para la prueba electrónica**: Permite a un investigador empaquetar un elemento de prueba con el fin de establecer un seguro (**cadena de custodia)** para todas las pruebas electrónicas.

• **Simulador:** Esta herramienta muestra lo que sucede en el caso de un ataque, tanto en una página web típica sin protección, y en una página web que ha seguido las directrices del proyecto en la preparación forense.

Las herramientas introducidas por el proyecto CTOSE permiten a los administradores informáticos, personal de seguridad de tecnología de la información, investigadores del equipo de incidentes, policía y a las fuerzas del orden seguir procedimientos coherentes y normalizados en la investigación de incidentes.

1.1.2.4 Metodología CP4DF Código de Prácticas para Digital Forensics

El código de prácticas para Digital Forensics sirve no sólo como guía de trabajo, sino como lista de tareas que hay que hacer en un proceso de investigación. Es una iniciativa española para el desarrollo de una metodología de procedimientos para Análisis Forense.

El proceso tradicional de investigación cuando el delito o evento se haya consumado, consta de las siguientes etapas o metodologías:

a) Aseguramiento de la escena:

El primer paso en un proceso de investigación informática forense, al igual que en cualquier otro proceso criminal, es asegurar (restringir el acceso a la zona del delito para no modificar evidencias) la escena del delito informático. Este primer módulo, idealmente, debería ser realizado por un cuerpo de seguridad del Estado: Policía Nacional.

Normalmente los administradores de los sistemas informáticos serán los primeros en tener contacto con la escena del delito y junto a equipo de respuesta de incidentes realizarán los primeros pasos para "congelar" la escena del delito. El rol fundamental de las primeras personas en responder al delito es no hacer nada que pueda producir daño.

Pasos a realizar:

1. Identificar la escena del delito.
2. Realizar una lista con los sistemas involucrados en el delito.
3. Restringir el acceso a la escena del delito.
4. Preservar toda huella digital.
5. Fotografiar, grabar y esquematizar la escena del delito.

6. Mantener el estado de los dispositivos.
7. Desconectar las conexiones de red.
8. Comprobar y desconectar si existieran las conexiones inalámbricas que puedan permitir la activación de conexiones remotas.
9. Si hay impresoras imprimiendo, dejar que terminen de imprimir.
10. Anotar hora y fecha del sistema antes de apagarlo, documentándolo con fotografías o grabándolo en vídeo si es posible.
11. Los dispositivos encendidos apagarlos quitando la alimentación de la parte posterior del mismo, no del enchufe.
12. Etiquetar cables y componentes.
13. Fotografiar y grabar de nuevo los dispositivos con las etiquetas colocadas en los mismos.

b) **Identificación de la evidencia digital.**

Es el proceso de conocer los datos, dónde están localizados y cómo están almacenados.

Para identificar la evidencia es necesario realizar una primera distinción entre evidencias volátiles y no volátiles.

Evidencias volátiles: Información que se perderá al momento de apagar el equipo

- Información que se perderá al momento de apagar el equipo
- Contenido de la memoria
- Procesos en ejecución
- Programas en ejecución
- Usuarios conectados
- Configuración de red
- Direcciones IP, tabla de rutas, etc

- Conexiones activas, puertos abiertos
- Apagado del equipo afectado
- Sincronizar los discos
- Ficheros abiertos, pero borrados

Evidencias no volátiles: Es la información que permanece tras apagar el equipo. Estas deben ser copiadas al equipo de análisis de forma local o a través de la red.

- Utilizar programas del sistema para hacer la copia
- Montar los sistemas de ficheros en modo escritura
- Logs de IDS/Cortafuegos externos

Información volátil importante:

- Hora y fecha del sistema
- Procesos en ejecución
- Conexiones de red
- Puertos abiertos y aplicaciones asociadas
- Usuarios logados en el sistema

La obtención de evidencias volátiles se puede dar en los siguientes lugares:

- Registros y cache del procesador
- Tablas de rutas
- Cache ARP
- Tabla de procesos
- Estadísticas del kernel y módulos
- Memoria RAM
- Ficheros temporales del sistema
- Estado de la red
- Ficheros abiertos

A continuación se mencionan algunos comandos para la obtención de datos volátiles:

- **Fecha y hora:**

  C:\> date /t & time /t
- **Información tcp/ip:**

  C:\> ipconfig /all
- **Conexiones abiertas y puertos en espera, con PID asociado:**

  C:\> netstat -aon
- **Información del sistema (hardware, software, hotfixes, versiones, etc.):**

  C:\>systeminfo
- **Lista de proceso:**

  C:\> tasklist (o también: **tasklist > liste.txt** para obtener la salida en un archivo texto.)

  C:\>tasklist /M nos indica las DLL utilizadas en cada proceso
  C:\>tasklist /SVC nos permite saber a qué servicio corresponde cada ejecutable presente en la memoria (si es un servicio).
- **Lista de tareas programadas (%windir%\tasks\ folder):**

  C:\>at
- **Muestra tabla de caché ARP**

  C:\>arp -a
- **Muestra tabla de rutado IP**

  C:\>route print

Herramientas con interfaz gráfico:

- **Rootkit revealer:** Detecta rootkits (usermode o kernelmode)
- **Process Explorer (Procexp y Procmon):** Información útil sobre procesos, librerías que usan, recursos accedidos, conexiones de red, etc.
- **Tcpview:** Muestra conexiones de red y aplicaciones asociadas

Adquisición de Datos de Red

Fuentes importantes de información:

- Logs de IDS/IPS
- Logs de Firewall
- Logs de VPN / Radius
- Logs del servidor DHCP
- Logs de otras aplicaciones que puedan estar relacionadas (ftp, www, base de datos, etc)

c) Preservación de la evidencia digital.

Esta es la fase más importante y crítica de la metodología, puesto que una vez que se halla comprobado el delito informático la empresa o institución dañada normalmente deseará llevar a un proceso judicial al atacante. Para ello es necesario poseer evidencias digitales preservadas de tal forma que no haya duda alguna de su similitud y siempre de acuerdo a las leyes.

d) Análisis de la evidencia digital.

El investigador debe intentar contestar a las siguientes preguntas en la fase de análisis:

1. ¿Quién?

Reunir la información sobre el/los individuo/s involucrados en el compromiso.

2. ¿Qué?

Determinar la naturaleza exacta de los eventos ocurridos.

3. ¿Cuándo?

Reconstruir la secuencia temporal de los hechos.

4 ¿Cómo?

Descubrir que herramientas se han usado para cometer el delito. Evidencia almacenada debe ser analizada para extraer la información relevante y recrear la cadena de eventos sucedidos. El análisis requiere un conocimiento profundo de lo que se está buscando y como obtenerlo.

e) Presentación de la evidencia digital.

Basándose en las fases anteriores, en toda la documentación disponible del caso y basándose también en la cadena de custodia, la presentación y/o sustentación del informe pericial es la fase de comunicar el significado de la evidencia digital, los hechos, sus conclusiones y justificar el procedimiento empleado.

El propósito de la presentación de los informes es proporcionar al lector toda la información relevante de las evidencias de forma clara, concisa, estructurada y sin ambigüedad para hacer la tarea de asimilación de la información tan fácil como sea posible.

La forma de presentación es muy importante y debe ser entendible por personas no conocedoras del tema en discusión. Es decisivo que el investigador presente las evidencias en un formato sencillo de entender, acompañado de explicaciones que eviten la jerga y la terminología técnica.

En la elaboración del informe se debe:

1- Detallar todo tipo de información que ayude al análisis en forma consolidada (Ejemplo: Antecedentes, procedimientos, evidencias, etc.)

2- Hacer uso de formatos prediseñados que permitan llevar un control y orden en la elaboración del informe.

3- Elaborarse de forma imparcial.

Herramientas básicas para el análisis de un incidente

El personal que responda al incidente debe llevar consigo todo lo necesario para asegurar la escena del delito y aplicar el procedimiento de gestión de incidencias.

- Destornilladores
- Cinta aislante
- Cortador de cables
- Etiquetas
- Cámara digital de fotografías/vídeo
- Sistemas de creación de imágenes de dispositivos de almacenamiento (Ordenadores portátiles con grabadores CD o DVS, sistemas de copia rápida RAID, etc).
- CDs con sistemas operativos auto arrancables
- Bolsas antiestáticas
- Plásticos con sistema de “burbujas de aire”
- Cajas de cartón
- Backup de los sistemas que se requieran reconstituir siempre y cuando se trate de un equipo crítico.

Toda posible prueba debe ser adecuadamente etiquetada y documentada, además cada paso realizado debe ser registrado y documentado en detalle, para que sirva de Bitácora del Investigador.

1.2 Informática Forense

1.2.1 Introducción

Debido a grandes ataques y delitos informáticos que se vienen presentando hace más de dos décadas, las autoridades policiales en el mundo tomaron cartas en el asunto, creando laboratorios informáticos para apoyar las investigaciones judiciales, departamentos de computación forense para analizar las informaciones de la red y sus comportamientos, para poder atrapar a los delincuentes.

De acuerdo con lo anterior, es posible definir la computación forense como una rama de la informática que se encarga de recolectar y/o recopilar información valiosa desde sistemas informáticos (redes, ordenadores, soportes magnéticos, ópticos, etc) con distintos fines, sirviendo de apoyo a otras disciplinas o actividades, como son las labores de criminalística e investigaciones. Estas evidencias que permite descubrir diferentes datos sirven, por ejemplo, para condenar o absolver a algún imputado.

Esta rama investigativa tuvo su origen en 1984 cuando el FBI y otras agencias de Estados Unidos comenzaron a desarrollar programas para examinar evidencia computacional.

En la actualidad la computación forense trabaja como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso.

El análisis forense involucra aspectos como la preservación, descubrimiento, identificación, extracción, documentación y la interpretación de datos informáticos, analizando, a partir de esto, los elementos que sean evidencia digital, la cual no es más que un tipo de evidencia física, menos tangible que otras formas de pruebas (DNA, huellas digitales, componentes de computadores), que puede ser duplicada de manera exacta y copiada tal como si fuese el original.

1.2.2 Informática Forense

A la fecha, existen múltiples definiciones sobre el tema forense en informática (Mckmmish 1999). Una primera versión nos sugiere diferentes términos para aproximarnos a este tema, dentro de los cuales se tienen: computación forense, *digital forense* (forensia digital), *network forensics* (forensia 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 términos que son de interés para las ciencias forenses aplicadas en medios informáticos.

El hecho de que esta especialidad técnica sea un recurso importante para las ciencias forenses modernas, asume que dentro de sus procedimientos las tareas propias asociadas con la evidencia en la escena del crimen, como son: identificación, preservación, extracción, análisis, interpretación, documentación y presentación de las pruebas en el contexto de la situación bajo inspección.

La computación Forense podría interpretarse de dos maneras:

1. Disciplina de las ciencias forenses, considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso.

2. Disciplina científica y especializada que, entiende los elementos propios de las tecnologías de los equipos de computación, ofrece un análisis de la información residente en dichos equipos.

Estas definiciones no son excluyentes, sino complementarias. Una de ellas hace énfasis en las consideraciones forenses, y la otra en la especialidad técnica, pero en ambas procuran el esclarecimiento y la interpretación de la información en los medios informáticos como valor fundamental, uno por la justicia y otro para la informática.

1.2.3 Evidencia Digital

Este tipo de evidencia es la que brinda a los investigadores la materia prima para trabajar, sin embargo cuenta con algunas desventajas ya que ésta puede ser volátil, anónima, duplicable, alterable, modificable y eliminable. Por esto, los investigadores deben estar al tanto de procedimientos, técnicas y herramientas tecnológicas para obtener, custodiar, analizar, revisar y presentar esta evidencia. Asimismo deben tener conocimiento de las normas, derecho procesal y procedimientos legales para que dichas pruebas sean confiables y den los elementos necesarios para poder inculpar a alguien.

El aspecto más importante al momento de recolectar evidencia, es la preservación de la integridad de ésta; en el caso particular de la información almacenada en medios magnéticos, la naturaleza volátil de ésta hace que dicha labor sea particularmente difícil. La primera gran decisión que se debe tomar a la hora de colectar evidencias, es la cantidad de ésta que se debe tomar.

La evidencia digital o computacional es única, cuando se la compara con otras formas de "evidencia documental". A diferencia de la documentación en papel, la evidencia computacional es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto único de la evidencia computacional es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizó una copia.

Cuando la evidencia se encuentra en formato digital el objetivo de la investigación deberá enfocarse en el contenido del computador, y no el hardware de éste. Para esto existen dos opciones de cómo recolectar la evidencia digital:

1. Crear un Backup o imagen completo de toda la información.
2. Copiar únicamente la información necesaria.

La IOCE (International Organization On Computer Evidence) define los siguientes cinco puntos como los principios para el manejo y recolección de evidencia computacional:

1. Sobre recolectar evidencia digital, las acciones tomadas no deben cambiar por ningún motivo esta evidencia.
2. Cuando es necesario que una persona tenga acceso a evidencia digital original, esa persona debe 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.

Existe una gran categoría de evidencia que puede ser recolectada en el caso de los crímenes informáticos, y es la evidencia presente en las redes. Todo el flujo de información que corre a través de una red, sea interna o externa a una organización, o aún en Internet, podría contener evidencia potencialmente útil a la hora de investigar un crimen.

Adicionalmente, hay ciertos tipos de crímenes, como la falsificación de correos electrónicos, intercambio de información ilegal a través de Usenet (por ej., pornografía infantil) o uso del IRC para concertar crímenes –práctica común entre la comunidad hacker-, que no podrían cometerse sin la utilización de redes.

1.2.4 Tipos de información y datos de un incidente

- **Información volátil:** Este tipo de información puede ser Información de red. Comunicación entre el sistema y la red, procesos activos, programas actualmente activos en el sistema. Usuarios logueados, usuarios y empleados que actualmente utilizan el sistema, ficheros abiertos, librerías en uso, ficheros ocultos, y troyanos.

- **Información no volátil:** Este tipo de información, datos de configuración, ficheros del sistema y datos del registro que son disponibles después del re-arranque. Esta información se investiga y revisa a partir de una copia de backup.

1.2.5 Etapas de la informática forense

Identificación:

Es muy importante conocer los antecedentes, situación actual y el proceso que se quiere seguir para poder tomar la mejor decisión con respecto a las búsquedas y la estrategia de investigación. Incluye muchas veces la identificación del bien informático, su uso dentro de la red, el inicio de la cadena de custodia (proceso que verifica la integridad y manejo adecuado de la evidencia), la revisión del entorno legal que protege el bien y del apoyo para la toma de decisión con respecto al siguiente paso una vez revisados los resultados.

Preservación:

Este paso incluye la revisión y generación de las imágenes forenses de la evidencia para poder realizar el análisis. Dicha duplicación se realiza utilizando tecnología de punta para poder mantener la integridad de la evidencia y la cadena de custodia que se requiere. Al realizar una imagen forense, nos referimos al proceso que se requiere para generar una copia "bit-a-bit" de todo el disco, el cual permitirá recuperar en el siguiente paso, toda la información contenida y borrada del disco duro. Para evitar la contaminación del disco duro, normalmente se ocupan bloqueadores de escritura de hardware, los cuales evitan el contacto de lectura con el disco, lo que provocaría una alteración no deseada en los medios.

Análisis:

Proceso de aplicar técnicas científicas y analíticas a los medios duplicados por medio del proceso forense para poder encontrar pruebas de ciertas conductas. Se pueden realizar búsquedas de cadenas de caracteres, acciones específicas del o de los usuarios de la máquina como son el uso de dispositivos de USB (marca, modelo), búsqueda de archivos específicos, recuperación e identificación de correos electrónicos, recuperación de los últimos sitios visitados, recuperación del caché del navegador de Internet, etc.

Presentación:

Es el recopilar toda la información que se obtuvo a partir del análisis para realizar el reporte y la presentación a los abogados, la generación (si es el caso) de una pericial y de su correcta interpretación sin hacer uso de tecnicismos.

1.2.6 Herramientas de informática forense

La realidad competitiva de las empresas hace imprescindible para ellas acoplarse a las tecnologías de seguridad de la información disponibles, por lo que es prioritario que las empresas tomen medidas para proteger su información estratégica tanto de ataques internos como externos y a todos los niveles.

El uso de herramientas sofisticadas se hace necesario debido a:

- La gran cantidad de datos que pueden estar almacenados en un computador.
- La variedad de formatos de archivos, los cuales pueden variar enormemente, aun dentro del contexto de un mismo sistema operativo.
- La necesidad de recopilar la información de una manera eficiente, y que permita verificar que la copia es exacta.
- Limitaciones de tiempo para analizar toda la información.
- Facilidad para borrar archivos de computadores
- Mecanismos de encriptación, o de contraseñas.

Entre estas herramientas se destacan las siguientes:

- Sleuth Kit -Forensics Kit
- Py-Flag - Forensics Browser
- Autopsy - Forensics Browser for Sleuth Kit
- Air - Forensics Imaging GUI, md5deep - MD5 Hashing Program
- Netcat - Command Line
- Cryptcat - Command Line
- NTFS-Tools
- Qtparted - GUI Partitioning Tool

- Regviewer - Windows Registry, Viewer
- X-Ways WinTrace
- X-Ways WinHex
- R-Studio Emergency (Bootable Recovery media Maker)
- R-Studio Network Edition
- Hélix
- Net resident
- Encase 4.20
- Snort (Sistema Detector de Intrusos)
- **GetData – Recovery My Files**
- **SPlunk**

GETDATA - Recovery My Files:

El programa para recuperación de datos Recover My Files, recuperará fácil y rápidamente archivos borrados que se han eliminado de la Papelera de reciclaje o que se han perdido por dar formato al disco duro, por corrupción del mismo, por infección mediante un virus o por un bloqueo inesperado del sistema o por un fallo de software.

El programa de recuperación de datos Recover My Files busca cualquier tipo de archivo, pero tiene un tratamiento específico para más de 350 tipos de archivos clasificados de manera amplia en las siguientes categorías:

- Recuperación de correo electrónico borrado
- Recuperación de documentos borrados
- Recuperación de archivos borrados
- Recuperación de fotografía digital
- Recuperación de música y vídeo borrado

SPlunk: Es un software que le permite indexar, buscar, alertar e informar sobre datos online, o datos históricos de TI, dándole visibilidad en toda su infraestructura de TI desde una ubicación en tiempo real. Reduce el tiempo para solucionar problemas de TI y los incidentes de seguridad a minutos o segundos en lugar de horas o días. Monitorea toda su infraestructura de TI para evitar la degradación del servicio y tiempo de inactividad. Reporta todos sus controles de cumplimiento a un menor costo y en una fracción del tiempo

Splunk es una herramienta lo suficientemente flexible que permite indexar cualquier tipo de datos de tecnología de la información de cualquier fuente en tiempo real, permite apuntar los servidores o syslogs de los dispositivos de red, vigilar archivos de registro, seguimiento del cambio en el sistema de archivos o el registro de windows, o programar una secuencia de comandos para tomar mediciones del sistema. Los datos en bruto y el índice de riqueza se almacenan en un eficiente y comprimido sistema de almacenamiento de datos con opciones firmados y auditados para la integridad de los datos. Hace de la información una herramienta indispensable para la toma de decisiones, ya que permite analizarla mediante estadísticas.

.

1.3 Servidores

1.3.1Introducción

Un servidor es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.[] Es una computadora en la que se ejecuta un programa que realiza alguna tarea en beneficio de otras aplicaciones, tanto si se trata de un ordenador central (mainframe), un miniordenador, un ordenador personal.

1.3.2 Tipos de Servidores

- **Servidor de archivo:** es el que almacena varios tipos de archivos y los distribuye a otros clientes en la red. Permite balanceo entre seguridad y facilidad de uso.

- **Servidor de impresiones:** controla una o más impresoras y acepta trabajos de impresión de otros clientes de la red, poniendo en cola los trabajos de impresión.

- **Servidor de correo:** almacena, envía, recibe, enruta y realiza otras operaciones relacionadas con email para los clientes de la red.

- **Servidor Proxy:** realiza un cierto tipo de funciones a nombre de otros clientes en la red para aumentar el funcionamiento de ciertas operaciones, también proporciona servicios de seguridad, o sea, incluye un cortafuego. Permite administrar el acceso a Internet en una red de computadoras permitiendo o negando el acceso a diferentes sitios Web.

Servidores Windows server 2008, www.microsoft.com/security

- **Servidor de fax:** almacena, envía, recibe, en ruta y realiza otras funciones necesarias para la transmisión, la recepción y la distribución apropiadas de los fax.

- **Servidor del acceso remoto (RAS):** controla las líneas de módem de los monitores u otros canales de comunicación de la red para que las peticiones conecten con la red de una posición remota.

- **Servidor web:** almacena documentos HTML, imágenes, archivos de texto, escrituras, y demás material Web compuesto por datos (conocidos colectivamente como contenido), y distribuye este contenido a clientes que la piden en la red.

- **Servidor de base de datos:** provee servicios de base de datos a otros programas u otras computadoras, como es definido por el modelo cliente-servidor.

- **Servidor Controlador de Dominio:** Son los servidores más importantes de la infraestructura. Poseen la información de todos los objetos del Active Directory.

- **Servidores de infraestructura:** es el que proporciona los servicios DHCP o la funcionalidad de WINS. Se utilizará una plantilla de seguridad incremental específica para Servidor de infraestructuras, se configurarán manualmente las opciones adicionales.

- **Servidores Bastionados (con acceso público):** son servidores expuestos a ataques externos.

1.3.3 Windows Server 2008

Windows Server 2008 es el nombre de un sistema operativo de Microsoft diseñado para servidor. Es el sucesor de Windows Server 2003, distribuido al público casi cinco años antes. Al igual que Windows Vista, Windows Server 2008 se basa en el núcleo Windows NT 6.0. Posteriormente se lanzó una segunda versión, denominada Windows Server 2008 R2.

Características

Hay algunas diferencias con respecto a la arquitectura del nuevo Windows Server 2008, que pueden cambiar drásticamente la manera en que se usa este sistema operativo. Estos cambios afectan la manera en que se gestiona el sistema hasta el punto de que se puede llegar a controlar el hardware de forma más efectiva, se puede controlar mucho mejor de forma remota y cambiar de forma radical la política de seguridad.

Entre las mejoras que se incluyen, están:

- **Nuevo proceso de reparación de sistemas NTFS:** proceso en segundo plano que repara los archivos dañados.

- **Creación de sesiones de usuario en paralelo:** reduce tiempos de espera en los Terminal Services y en la creación de sesiones de usuario a gran escala.

- **Sistema de archivos SMB2:** de 30 a 40 veces más rápido el acceso a los servidores multimedia.

- **Address Space Load Randomization (ASLR):** protección contra malware en la carga de controladores en memoria.

- **Windows Hardware Error Architecture (WHEA):** protocolo mejorado y estandarizado de reporte de errores.

- **Virtualización de Windows Server:** mejoras en el rendimiento de la virtualización.

- **PowerShell:** inclusión de una consola mejorada con soporte GUI para administración.

- **Server Core:** el núcleo del sistema se ha renovado con muchas y nuevas mejoras.

Entre los servicios más utilizados en Servidores Windows 2008 se destacan los siguientes:

- Servidor de archivos
- Servidor de impresiones
- Servidor de aplicaciones
- Servidor de correo (SMTP/POP)
- Servidor de terminal
- Servidor de Redes privadas virtuales (VPN) (o acceso remoto al servidor)
- Controlador de Dominios (mediante Active Directory)
- Servidor DNS
- Servidor DHCP
- Servidor de Streaming de Video
- Servidor WINS
- Servidor de aplicaciones

Ediciones

La mayoría de las ediciones de Windows Server 2008 están disponibles en x86-64 (64 bits) y x86 (32 bits).

Microsoft ha anunciado que Windows Server 2008 será el último sistema operativo para servidores disponible en 32 bits. Windows Server 2008 está disponible en las ediciones que figuran a continuación, similar a Windows Server 2003.

- Windows Server 2008 Standard Edition (x86 y x86-64)
- Windows Server 2008 R2 Todas las Ediciones (Solo 64Bit)
- Windows Server 2008 Enterprise Edition (x86 y x86-64)
- Windows Server 2008 Datacenter Edition (x86 y x86-64)
- Windows HPC Server 2008 (Reemplaza Windows Compute Cluster Server 2003)
- Windows Web Server 2008 (x86 y x86-64)
- Windows Storage Server 2008 (x86 y x86-64)
- Windows Small Business Server 2008 (Nombre clave "Cougar") (x86-64) para pequeñas empresas
- Windows Essential Business Server 2008 (Nombre clave "Centro") (x86-64) para empresas de tamaño medio[
- Windows Server 2008 para sistemas basados en Itanium
- Windows Server 2008 Foundation Server

1.3.4 Introducción al DNS

El Domain Name System (DNS) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. El DNS se utiliza principalmente para la resolución de nombres, esto es, decidir qué dirección IP pertenece a determinado nombre completo de host.

El **DNS** se utiliza para distintos propósitos. Los más comunes son:

- **Resolución de nombres**: Dado el nombre completo de un host (por ejemplo blog.smaldone.com.ar), obtener su dirección IP (en este caso, 208.97.175.41).
- **Resolución inversa de direcciones**: Es el mecanismo inverso al anterior. Consiste en, dada una dirección IP, obtener el nombre asociado a la misma.
- **Resolución de servidores de correo**: Dado un nombre de dominio (por ejemplo gmail.com) obtener el servidor a través del cual debe realizarse la entrega del correo electrónico (en este caso, gmail-smtp-in.l.google.com).

1.3.5 Usuarios del Servidor y Editores de Directivas

El Editor de directivas del sistema es la herramienta que los administradores utilizan para crear y modificar las directivas del sistema. Las directivas del sistema proporcionan a los administradores un mayor control de los equipos Microsoft Windows dentro de un dominio.

Las directivas del sistema son una lista de reglas que determinan lo que un usuario ve en su escritorio y qué puede hacer en un equipo. El Editor de directivas del sistema se puede utilizar para crear directivas en las siguientes áreas:

- Restricción de opciones del Panel de control
- Personalización de partes del escritorio
- Control de inicio de sesión y del acceso a la red

Se puede aplicar una directiva individual a todo un dominio. Si las directivas predeterminadas no son adecuadas para todos los usuarios o todos los equipos del dominio, se pueden definir directivas del sistema adicionales para usuarios, grupos o equipos individuales.

1.3.5.1 Directivas de equipo y directivas de usuario

Cuando se crea una nueva directiva, el Editor de directivas del sistema presenta dos iconos, Equipo predeterminado y Usuario predeterminado. Estos iconos presentan las opciones de directivas que permiten la configuración de las directivas de equipo para todos los equipos del dominio y las directivas de usuario para todos los usuarios que inicien sesiones en dichos equipos.

1.3.5.2 Funcionamiento de las directivas del sistema

Un archivo de directivas del sistema es una colección de valores del Registro que sobre escribe las áreas del usuario y del equipo local actuales del Registro.

Las directivas del sistema se inician a través del siguiente proceso:

1. Cuando un usuario inicia una sesión en un dominio desde un equipo Windows NT, el sistema operativo carga el perfil del usuario. Windows NT busca en el directorio de red compartido Netlogon del servidor de inicio de sesión el archivo NTConfig.pol.

2. Si el archivo Ntconfig.pol define directivas de usuario para dicho usuario, estas configuraciones se combinan con la parte del Registro correspondiente al usuario actual.

3. Si no hay definidas directivas de usuario para dicho usuario, pero sí las hay para grupos, las configuraciones de las directivas de los grupos a los que pertenezca el usuario se combinan con la parte del Registro correspondiente al usuario actual, en orden de prioridad. Después Windows NT combina las directivas del usuario predeterminado en el Registro.

4. Si las directivas del sistema no están definidas para el usuario ni para ninguno de los grupos del usuario, los valores de las directivas del usuario predeterminados se combinan en la parte del Registro de usuario actual.

5. Si hay directivas del sistema definidas para el equipo en el que el usuario ha iniciado sesión, esos valores de directiva se combinan en la parte correspondiente al equipo local del Registro. De lo contrario, los valores de las directivas del equipo predeterminados se combinan en la parte correspondiente al equipo local del Registro.

Las entradas del Editor de directivas del sistema cambian los valores del Registro del equipo local de las siguientes formas:

Las directivas del sistema para los usuarios modifican el subárbol **HKEY_CURRENT_USER** del Registro. Esto define el contenido del perfil de usuario en vigor para el usuario.

Las directivas del sistema para los equipos modifican el subárbol **HKEY_LOCAL_MACHINE** del Registro.

1.3.5.3 Creación de las directivas del sistema

Para crear nuevas directivas del sistema, en el menú **Archivo**, haga clic en **Nueva directiva** y, a continuación, haga doble clic en Equipo predeterminado o Usuario predeterminado para ver el cuadro de diálogo **Propiedades de Equipo predeterminado** o **Propiedades de Usuario predeterminado**.

Las directivas predeterminadas disponibles en el cuadro de diálogo **Propiedades de Equipo predeterminado**, son:

- **Red:** Las opciones actualización remota incluyen la elección entre dos modos: una ruta de acceso automática predeterminada (se actualiza desde Ntconfig.pol en un controlador de dominio) o una ruta de acceso escrita manualmente para actualizar las directivas del sistema desde otro equipo distinto de los controladores de dominio.

- **Sistema:** Configurar SNMP y las entradas que se van a ejecutar al iniciar.

- **Red de Windows NT:** Activar la creación de recursos compartidos en cada unidad al iniciar.

- **Impresoras de Windows NT:** Impedir que la cola de impresión envíe información de la impresora compartida a otros servidores de impresión, modificar la prioridad de las asignaciones de los trabajos de impresión.

- **Acceso remoto de Windows NT:** Establecer el número máximo de intentos de autenticación incorrectos y el límite de tiempo máximo para la autenticación.

- **Shell de Windows NT:** Crear carpetas personalizadas compartidas para todos los usuarios del equipo.

- **Sistema de Windows NT:** Modificar opciones de inicio de sesión: alterar la pantalla de inicio de sesión, activar el apagado desde el cuadro de diálogo **Autentificación**, desactivar la presentación del nombre del último usuario que inició una sesión y ejecutar secuencias de comandos de forma síncrona.

- **Perfiles de usuario de Windows NT:** Definir una conexión lenta con un servidor de inicio de sesión y permitir que el equipo detecte automáticamente una conexión lenta cuando un usuario intenta iniciar una sesión. Utilice estos valores y las opciones de la ficha **Perfil de usuario** del programa Sistema del Panel de control para optimizar el rendimiento cuando se inician sesiones en conexiones lentas.

Las directivas predeterminadas disponibles en el cuadro de diálogo **Propiedades de Usuario predeterminado, son:**

- **Panel de control:** Restringir la actividad del usuario en el programa Pantalla del Panel de control o para denegar el acceso al programa Pantalla.

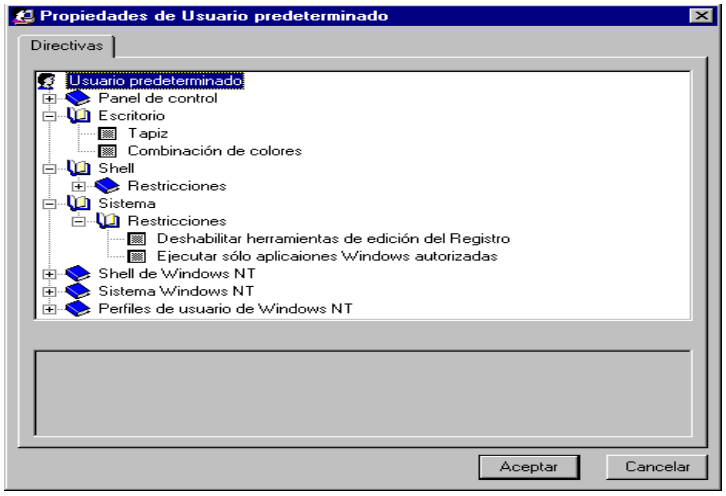
- **Escritorio:** Especificar el papel tapiz de fondo y la combinación de colores del escritorio.

- **Shell:** Restringir qué aparece en el escritorio y restringir el uso de los comandos **Ejecutar**, **Buscar** y **Apagar el sistema**.

- **Sistema:** Desactivar el Editor del Registro del sistema de Windows NT (Regedt32.exe)

- **Shell de Windows NT:** Personalizar las carpetas del escritorio. Cree carpetas personalizadas escribiendo rutas a elementos de programa, iconos de escritorio, elementos de Entorno de red y los elementos del menú Inicio que quiera que provengan de otra ubicación distinta de las carpetas de los perfiles de usuario.

- **Sistema de Windows NT:** Combinar las variables de entorno del archivo Autoexec.bat con las variables de entorno del usuario.



1.3.5.4 Protección de equipos

Las directivas permiten la modificación del cuadro de diálogo **Información de inicio de sesión** para proteger los equipos. Se puede hacer de dos maneras:

- Presentar una advertencia contra el uso no autorizado del sistema. En las directivas del equipo, configure la opción **Sistema de Windows NT\Inicio de sesión\Indicador de inicio de sesión**.

- Impedir la presentación del último usuario que inició una sesión. De forma predeterminada, cada vez que se presiona CTRL+ALT+SUPR, el cuadro de diálogo Información de inicio de sesión presenta el nombre de usuario de la última persona que inició sesión.

- Para impedir dicha presentación, en las directivas del equipo apropiado, seleccione la opción **Sistema de Windows NT\Inicio de sesión\No mostrar último usuario que inició una sesión**.

1.3.5.5 Restricción del entorno del usuario

El Editor de directivas del sistema proporciona opciones de directivas que restringen el entorno de los usuarios. Para seleccionar dichas opciones, en el menú **Archivo**, haga clic en **Abrir directiva** y, a continuación, ubíquese en el directorio raíz_sistema\System32\Repl\Import\Scripts\Ntconfig.pol. Abra Usuario predeterminado, expanda Shell y, a continuación, expanda Restricciones.

Algunas opciones de directivas para la restricción de los entornos de los usuarios:

- **Eliminar el comando Ejecutar del menú Inicio:** El comando **Ejecutar** ya no aparece como opción del menú **Inicio**.
- **Ocultar el icono Entorno de red:** Entorno de red no aparece en el escritorio.
- **Ocultar todos los elementos del escritorio:** En el escritorio no se presenta ningún elemento.
- **Deshabilitar el comando Cerrar el sistema:** El comando **Cerrar el sistema** ya no aparece como opción del menú **Inicio**.

1.3.6 Tipos de ataques que se dan en Servidores

Un "**ataque**" consiste en aprovechar una vulnerabilidad de un sistema informático (sistema operativo, programa de software o sistema del usuario) con propósitos desconocidos por el operador del sistema y que, por lo general, causan un daño.

Para bloquear estos ataques, es importante estar familiarizado con los principales tipos de ataques entre los cuales se mencionan los siguientes:

- Obtener acceso al sistema
- Robar información
- Recopilar información personal acerca de un usuario
- Obtener información de cuentas bancarias
- Obtener información acerca de una organización (la compañía del usuario, etc.)
- Afectar el funcionamiento normal de un servicio
- Utilizar el sistema de un usuario como un "rebote" para un ataque
- Usar los recursos del sistema del usuario, en particular cuando la red en la que está ubicado tiene un ancho de banda considerable.

Ataques de autenticación:

Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y clave. También se le denomina TCP FIN Scanning-Stealth Port Scanning, Fragmentation Scanning y Eavesdropping-Packet Sniffing.

Ataques de modificación:

Esta categoría se refiere a la modificación desautorizada de los datos o el software instalado en el sistema víctima (incluyendo borrado de archivos). Son particularmente serios cuando el que lo realiza ha obtenido derechos de Administrador o Supervisor, con la capacidad de ejecutar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema. Aún así, si no hubo intenciones de "bajar" el sistema por parte del atacante; el Administrador posiblemente necesite darlo de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

1.4 Virus

1.4.1 Introducción

Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, no se replican a sí mismos porque no tienen esa facultad como el gusano informático, son muy nocivos y algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado, en la mayoría de las ocasiones, por desconocimiento del usuario. El código del virus queda residente (alojado) en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma entonces el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables que sean llamados para su ejecución. Finalmente se añade el código del virus al programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa.

1.4.2 Historia

El primer virus atacó a una máquina IBM Serie 360 (y reconocido como tal). Fue llamado Creeper, creado en 1972. Este programa emitía periódicamente en la pantalla el mensaje: «I'm a creeper... catch me if you can!» (¡Soy una enredadera... agárrame si tú puedes!). Para eliminar este problema se creó el primer programa antivirus denominado Reaper (cortadora).

Sin embargo, el término virus no se adoptaría hasta 1984, pero éstos ya existían desde antes. Sus inicios fueron en los laboratorios de Bell Computers. Cuatro programadores (H. Douglas Mellory, Robert Morris, Victor Vysottsky y Ken Thompson) desarrollaron un juego llamado Core War, el cual consistía en ocupar toda la memoria RAM del equipo contrario en el menor tiempo posible.

Después de 1984, los virus han tenido una gran expansión, desde los que atacan los sectores de arranque de disquetes hasta los que se adjuntan en un correo electrónico.

1.4.3 Métodos de propagación

Existen dos grandes clases de contagio. En la primera, el usuario, en un momento dado, ejecuta o acepta de forma inadvertida la instalación del virus.

En la segunda, el programa malicioso actúa replicándose a través de las redes. En este caso se habla de gusanos. En cualquiera de los dos casos, el sistema operativo infectado comienza a sufrir una serie de comportamientos anómalos o imprevistos. Dichos comportamientos pueden dar una pista del problema y permitir la recuperación del mismo.

Dentro de las contaminaciones más frecuentes por interacción del usuario están las siguientes:

1. Mensajes que ejecutan automáticamente programas (como el programa de correo que abre directamente un archivo adjunto).
2. Ingeniería social, mensajes como ejecute este programa y gane un premio, o, más comúnmente: Haz 2 click y gana 2 tonos para móvil gratis..
3. Entrada de información en discos de otros usuarios infectados.
4. Instalación de software modificado o de dudosa procedencia.

En el sistema Windows puede darse el caso de que el ordenador pueda infectarse sin ningún tipo de intervención del usuario (versiones Windows 2000, XP y Server 2003) por virus como Blaster, Sasser y sus variantes por el simple hecho de estar la máquina conectada a una red o a Internet. Este tipo de virus aprovechan una vulnerabilidad de desbordamiento de búfer y puertos de red para infiltrarse y contagiar el equipo, causar inestabilidad en el sistema, mostrar mensajes de error, reenviarse a otras máquinas mediante la red local o Internet y hasta reiniciar el sistema, entre otros daños.

En las últimas versiones de Windows 2000, XP y Server 2003 se ha corregido este problema en su mayoría.

1.4.4 Métodos de protección y tipos

Los métodos para disminuir o reducir los riesgos asociados a los virus pueden ser los denominados activos o pasivos.

a) Activos

- **Antivirus:** son programas que tratan de descubrir las trazas que ha dejado un software malicioso, para detectarlo y eliminarlo, y en algunos casos contener o parar la contaminación. Tratan de tener controlado el sistema mientras funciona parando las vías conocidas de infección y notificando al usuario de posibles incidencias de seguridad. Por ejemplo, al verse que se crea un archivo llamado Win32.EXE.vbs en la carpeta C:\Windows\%System32%\ en segundo plano, ve que es comportamiento sospechoso, salta y avisa al usuario.

- **Filtros de ficheros:** consiste en generar filtros de ficheros dañinos si el ordenador está conectado a una red. Estos filtros pueden usarse, por ejemplo, en el sistema de correos o usando técnicas de firewall. En general, este sistema proporciona una seguridad donde no se requiere la intervención del usuario, puede ser muy eficaz, y permitir emplear únicamente recursos de forma más selectiva.

b) Pasivos

- Evitar introducir a tu equipo medios de almacenamiento extraíbles que consideres que pudieran estar infectados con algún virus.
- No instalar software "pirata".
- Evitar descargar software de Internet.
- No abrir mensajes provenientes de una dirección electrónica desconocida.

1.4.5 Tipos de virus e imitaciones

Existen diversos tipos de virus, varían según su función o la manera en que éste se ejecuta en nuestra computadora alterando la actividad de la misma, entre los más comunes están:

Troyano: Consiste en robar información o alterar el sistema del hardware o en un caso extremo permite que un usuario externo pueda controlar el equipo.

Gusano: Tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

Bombas lógicas o de tiempo: Son programas que se activan al producirse un acontecimiento determinado. La condición suele ser una fecha (Bombas de Tiempo), una combinación de teclas, o ciertas condiciones técnicas (Bombas Lógicas). Si no se produce la condición permanece oculto al usuario.

Hoax: Los hoax no son virus ni tienen capacidad de reproducirse por si solos. Son mensajes de contenido falso que incitan al usuario a hacer copias y enviarla a sus contactos. Suelen apelar a los sentimientos morales ("Ayuda a un niño enfermo de cáncer") o al espíritu de solidaridad ("Aviso de un nuevo virus peligrosísimo") y, en cualquier caso, tratan de aprovecharse de la falta de experiencia de los internautas novatos.

Joke: Al igual de los hoax, no son virus, pero son molestos, un ejemplo: una página pornográfica que se mueve de un lado a otro, y si se le llega a dar a cerrar es posible que salga una ventana que diga: OMFG!! No se puede cerrar!

1.4.6 Acciones de los virus

Algunas de las acciones de algunos virus que pueden provocar son:

- Unirse a un programa instalado en el ordenador permitiendo su propagación.
- Mostrar en la pantalla mensajes o imágenes humorísticas, generalmente molestas.
- Bloquear el ordenador.
- Destruir la información almacenada en el disco, en algunos casos vital para el sistema, que impedirá el funcionamiento del equipo.
- Reducir el espacio en el disco.

1.5 Antivirus

1.5.1 Introducción

Un antivirus es una aplicación orientada a prevenir, detectar, y eliminar programas maliciosos denominados virus, los cuales actúan dañando un sistema informático con diversas técnicas.

La base fundamental de un programa antivirus es su capacidad de actualización de la base de datos. A mayor frecuencia de actualización, mejor protección contra nuevas amenazas.

Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, ha hecho que los antivirus hayan evolucionado hacia programas más avanzados que no sólo buscan detectar virus informáticos, sino bloquearlos, desinfectarlos y prevenir una infección de los mismos.

1.5.2 Tipos de antivirus

Dentro de los antivirus se encuentran diversas sub categorías: antivirus activo, antivirus pasivo, antivirus online, antivirus offline y antivirus gratuito.

Antivirus populares

- Kaspersky Anti-virus.
- Panda Security.
- Norton antivirus.
- McAfee.
- avast! y avast! Home
- AVG Anti-Virus y AVG Anti-Virus Free.
- BitDefender.
- F-Prot.
- F-Secure.
- NOD32.
- PC-cillin.
- ZoneAlarm AntiVirus.

1.5.3 Antivirus Kaspersky

Kaspersky Anti-Virus es desarrollado por Kaspersky Lab desde 1997, y es considerado uno de los mejores antivirus en la actualidad. Es un popular antivirus para computadoras de escritorio y móviles, sirve para proteger la computadora de virus, troyanos, gusanos, espías, y otros programas malignos.

Tiene capacidad para monitorear el tráfico entrante y saliente de Internet, defensa proactiva frente a nuevos programas maliciosos, actualización constante de su base de datos de virus, etc.

1.5.3.1 Requerimientos de Hardware/Software

- 50 MB de espacio en disco
- Microsoft Internet Explorer 5.5 y superior (para actualizar la base antivirus y los módulos de la aplicación vía Internet)
- Microsoft Windows Installer 2.0.

Compatible con Sistemas Operativos:

- Microsoft Windows 2000 Professional (Service Pack 4 o superior)
- Microsoft Windows XP Home Edition (Service Pack 2 o superior)
- Microsoft Windows XP Professional (Service Pack 2 o superior)
- Microsoft Windows XP Professional x64 Edition
- Intel Pentium procesador 300 MHz o más rápido (o compatible)
- Microsoft Windows Vista Home Premium (32/64 bit)
- Microsoft Windows Vista Home Basic (32/64 bit)
- Microsoft Windows Vista Business (32/64 bit)
- Microsoft Windows Vista Enterprise (32/64 bit)
- Microsoft Windows Vista Ultimate (32/64 bit)
- Intel Pentium processor 800 MHz 32-bit(x86)/64-bit(x64) or faster (o compatible)

1.5.3.2 Productos Kaspersky

- **Kaspersky Internet Security:**

Kaspersky Internet Security 2011 es un producto nuevo de Kaspersky Lab para usuarios particulares que provee protección completa a las computadoras personales contra todas las amenazas en Internet. La solución incluye HIPS (Sistema de Prevención contra Intrusos en computadoras Anfitrionas, por sus siglas en inglés), una tecnología

de control de actividad de aplicación avanzada que asigna categorías de seguridad a nuevos programas hasta el momento desconocidos.

Es el primer producto antivirus en incluir la tecnología sandbox, que usa la virtualización para ofrecer un ambiente de ejecución de seguridad aislada. Kaspersky Internet Security 2011 también ofrece a los usuarios las ventajas de Kaspersky Security Network, un sistema distribuido innovador de control de malware.

- **Kaspersky Mobile Security**

Es una solución amigable y confiable que protege dispositivos móviles contra ataques de red, malware que ataca plataformas móviles y spam SMS. En caso de que el Smartphone se pierda, la información de su memoria también permanece protegida

- **Kaspersky Open Space Security R2**

Incluye una versión actualizada del Kaspersky Administration Kit, la herramienta propietaria de protección antivirus, así como tres aplicaciones que protegen estaciones de trabajo y servidores Windows.

Las herramientas avanzadas de administración y protección incluidas en el producto actualizado proveen seguridad, desempeño y manejo significativamente mejorados para todos los nodos en la red corporativa.

Kaspersky Administration Kit 8.0

Incluye más de cuarenta características nuevas y mejoradas que permiten que las organizaciones con red de computadoras de cualquier tamaño, desde varias PCs hasta red distribuida en una estructura de administración compleja, implementen un modelo flexible de administración de protección antivirus.

Kaspersky Anti-Spam

Está diseñado para proteger a usuarios de sistemas de correo corporativo y a proveedores de Internet contra correo masivo no solicitado o spam.

1.5.3.3 Herramientas de Kaspersky

Cortafuegos (Firewall)

Programa que funciona como muro de defensa, bloqueando el acceso a un sistema en particular. Se utilizan principalmente en computadoras con conexión a una red, fundamentalmente Internet. El programa controla todo el tráfico de entrada y salida, bloqueando cualquier actividad sospechosa e informando adecuadamente de cada suceso.

Anti espías (Antispyware)

Aplicación que busca, detecta y elimina programas espías (spyware) que se instalan ocultamente en el ordenador. Los anti espías pueden instalarse de manera separada o integrado con paquete de seguridad (que incluye antivirus, cortafuegos, etc.).

Antipop-ups

Utilidad que se encarga de detectar y evitar que se ejecuten las ventanas pop-ups cuando navegas por la Web. Muchas veces los pop-ups apuntan a contenidos pornográficos o páginas infectadas. Algunos navegadores Web como Mozilla Firefox o Internet Explorer 7 cuentan con un sistema antipop-up integrado.

Antispam

Aplicación o herramienta que detecta y elimina el spam y los correos no deseados que circulan vía email. Funcionan mediante filtros de correo que permiten detectar los emails no deseados. Estos filtros son totalmente personalizables.

1.6 Proyecto TIC – UNAN-Managua

1.6.1 Introducción

A través del desarrollo del Proyecto de Tecnología de Comunicación e Información en las cuatro (4) Universidades públicas de Nicaragua, UNAN-Managua, UNAN-León, UNA y UNI se tiene como visión:

Integrar a las Universidades Públicas a una red de información y comunicación confiable, amplia y estable para el uso del conocimiento global y la mejora de la comunicación e intercambio de información local.

El Proyecto de Desarrollo de la Tecnología de Comunicación e Información a ser propuesto para el financiamiento de parte ASDI debe derivarse de las Políticas de Tecnología de Comunicación e Información y un Plan Maestro de implementación de tales Políticas. Así mismo debe derivarse de la propuesta de organización, administración y funcionamiento de un nodo de comunicaciones a INTERNET para las cuatro Universidades en mención.

ASDI ha mostrado interés en facilitar fondos para la fase de preparación y documentación de las Políticas, Planes Maestros de Tecnología de Comunicación e Información de cada Universidad en Nicaragua (UNAN-Managua, UNAN-León, UNA y UNI), posibilitando para esta fase el papel de contraparte a la Universidad de Lund , Suecia, la asistencia de la Universidad Tecnológica de Delft , Holanda.

1.6.2 Objetivos del Proyecto TIC

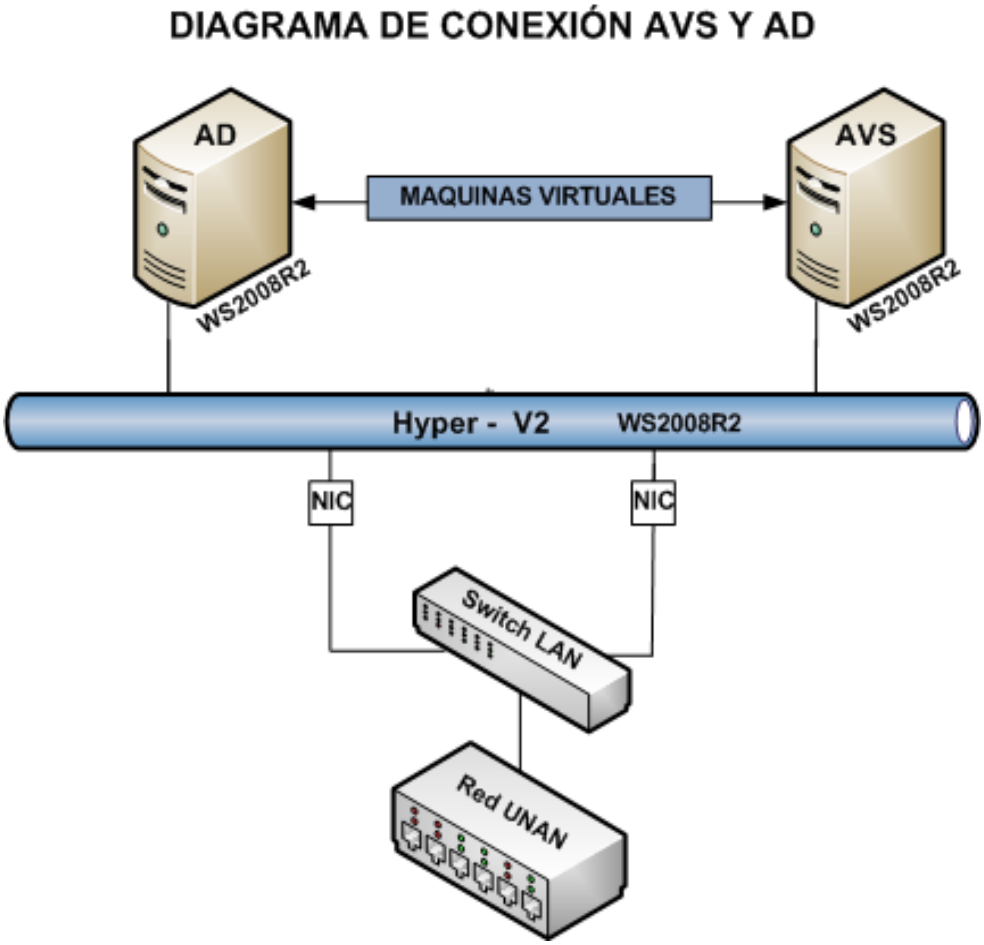
- Fortalecer la capacidad nacional en Tecnología de Comunicación e Información que permitirá a las Universidades públicas de educación superior de Nicaragua a ser parte y beneficiarios de la red de información global.

- Democratizar el acceso, de la comunidad universitaria, a los recursos de comunicación e información local y globalmente disponible.

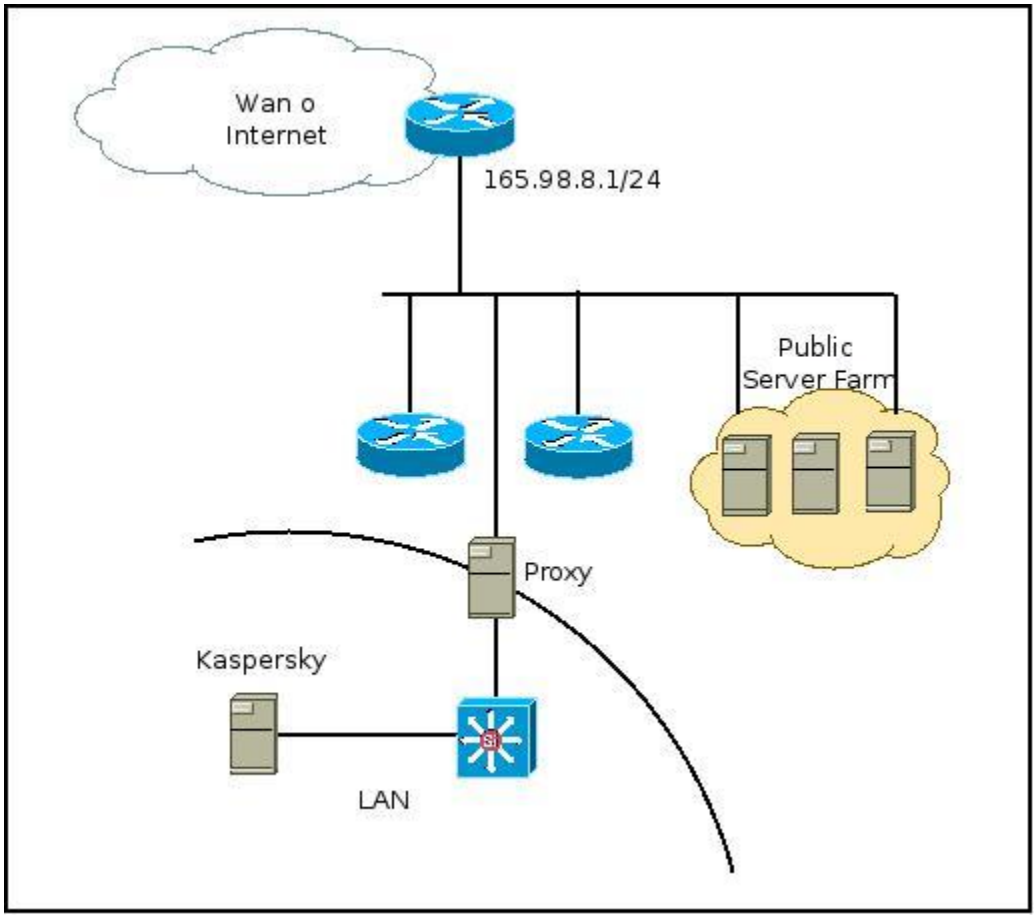
- Promover el uso aplicable de la información global en la educación superior y en proyectos o iniciativas de beneficios sociales y productivos en Nicaragua a través de la Universidades públicas.

1.6.3 Infraestructura de la Red en la que se encuentra el servidor de Kaspersky del Proyecto TIC (UNAN- Managua)

El servidor Kaspersky trabaja en conjunto con el servidor de dominio "Active Directory", mediante la consola, la cual permite agregar los usuarios pertenecientes al dominio de Active Directory.



La siguiente imagen muestra como el servidor de kaspersky está siendo protegido por el servidor proxy.



HIPOTESIS

La metodología de informática forense para el tratamiento de servidores permitirá conocer el nivel de riesgo de seguridad y las evidencias de ataques encontrados en el proyecto TIC de la UNAN – Managua.

DISEÑO METODOLOGICO

1. Tipo de estudio

El presente trabajo es de tipo investigación Descriptiva, ya que primeramente se realizó un análisis del problema, luego de la información recolectada, se procedió a la comparación de las distintas metodologías y guías para recolectar y archivar evidencias ante un delito informático. Como resultado de este análisis se desarrollo una metodología a seguir para el tratamiento de evidencias en el servidor del Proyecto TIC.

2 Métodos de recolección de datos

Se identificó la problemática y necesidades planteadas por el área de informática del proyecto TIC con relación al servidor de antivirus (Kaspersky Lab). Los problemas detectados fueron lentitud, el servidor se apaga constantemente debido al crecimiento en los logs, la consola del antivirus pierde conexión a la red, aumento de recurso en los procesadores y posibles amenazas de seguridad en la red.

Para el desarrollo de la investigación se necesitó obtener información relacionada al funcionamiento y utilización que se le está dando al servidor, así como el acceso al mismo, para lo cual se utilizó el siguiente método:

- Entrevista realizada al encardo de administrar el servidor de antivirus Kaspersky Lab, así como también a los demás empleados involucrados en la seguridad y administración de la red del Proyecto TIC de la UNAN – Managua. **Ver anexo 1**

En consecuencia de lo anterior se definieron los objetivos, y los procesos a desarrollar para crear una metodología para búsqueda y tratamiento de evidencias encontradas en el servidor.

3 POBLACION

La población de esta investigación son todas las personas que laboran dentro las instalaciones del Proyecto TIC.

4 MUESTRA

La muestra de esta investigación son todas las personas que tienen acceso al servidor de Kaspersky del Proyecto Tic.

Administrador de Servidor Kaspersky (2 persona)
Administrador de la red del Proyecto TIC (1 persona)

5 METODOLOGÍA DE INFORMÁTICA FORENSE PARA EL TRATAMIENTO DE EVIDENCIAS EN SERVIDORES WINDOWS

La presente metodología es un documento que provee técnicas y procesos para recolectar, analizar y manipular información relacionada con amenazas y ataques en servidores Windows.

El objetivo de esta metodología es brindar a los administradores de servidores una guía o pasos a seguir para la recolectar y manipular las evidencias digitales ante un delito informático. De tal manera que les permita mantener un orden en la investigación y obtener mayor integridad en la recolección de evidencia con el propósito de esclarecer la intrusión y alcanzar mayores elementos probatorios para inculpar al responsable del delito.

Principales criterios de la metodología:

- Conocer el perfil de riesgo de la información en la institución de acuerdo a su infraestructura y aplicaciones.
- Mantener estricta relación con las políticas de seguridad y con el personal encargado de manejar el incidente.
- Capturar la escena del incidente lo más preciso posible.
- Recolectar la información y analizar el hallazgo.
- Ejecutar técnicas de recolección de evidencias apropiadas protegiendo adecuadamente los medios de datos originales.
- No ejecutar programas que modifiquen las fechas de acceso a todos los archivos del sistema.

Pasos a seguir:

1. **Recolección de datos:** Para dar inicio a una investigación de análisis forense es necesario estar bien informado de lo sucedido, para esto se recomienda entrevistarse con el personal a cargo, con el objetivo de conocer que fue lo sucedido. En este primer paso es importante conocer cuál es la forma en la que operan los empleados o usuarios, que tipo de privilegios puede llegar a tener un empleado, normas o políticas de seguridad informática, forma de administrar un delito por parte de la institución.

   Una vez que el investigador este consciente de lo que está sucediendo en la institución, y tenga el consentimiento de los propietarios en cuanto al equipo deberá plantear el método que utilizará para operar el equipo.

2. **Resguardo de la escena:** En esta etapa de la investigación se debe asegurar la información, restringiendo acceso al mismo y en caso de ser necesario se debe realizar una confiscación del equipo. Una vez que se tenga control del equipo, y se haya identificado la escena del delito, se debe tener presente lo siguiente:

   - Realizar una check list de los sistemas involucrados en el delito.
   - Restringir el acceso a la escena del delito.
   - Preservar toda huella digital.
   - Desconectar las conexiones de red local e inalámbrica, ya que estas pueden permitir la activación de conexiones remotas.
   - Anotar hora y fecha del sistema antes de apagarlo, documentándolo con fotografías o grabándolo en vídeo si es posible.
   - Apagar el dispositivo primeramente del botón de encendido ubicado en el case del equipo y luego desconectar el cable de alimentación de energía ubicado en la parte posterior del case, y no del enchufe.

- Etiquetar cables y componentes.
- Fotografiar y grabar los dispositivos con las etiquetas colocadas.

3. **Capturar la escena:** Generar imágenes forenses de la escena del delito para poder realizar el análisis de información sin alterar la información origen. Esta captura de imágenes puede ser realizada con ayuda de herramientas altamente calificadas para la creación de imágenes de sistema operativo, o bien haciendo copias de disco a disco, o únicamente realizando copia de información que el investigador crea necesaria según el evento ocurrido.

4. **Custodia:** De ser necesario, realizar encriptación de las imágenes o copias realizada, con el propósito de asegurar la confidencialidad de la información en caso de extravío.

5. **Análisis de información:** El investigador debe utilizar una serie de herramientas y técnicas para localizar y extraer la evidencia, en este análisis debe descartar todos los elementos que no tienen valor como evidencia.
   En este análisis de evidencias se recomienda hacer una revisión en las siguientes bitácoras:

   - Logs de Auditorias de Seguridad (Local)
   - Logs de Sistema (Local)
   - Logs de Firewall
   - Logs de IDS/IPS
   - Logs de VPN
   - Logs del servidor DHCP
   - Logs de otras aplicaciones que puedan estar relacionadas (ftp, www, base de datos)

6. **Generar informe de hallazgo:** En base al seguimiento de los pasos mencionados anteriormente y a la cadena de custodia llevada a cabo, se debe finalizar el proceso de investigación de un delito informático mediante un informe de hallazgo encontrado, en el cual se debe detallar paso a paso las acciones realizadas durante el proceso de investigación, en este informe se debe mostrar un resumen del hallazgo encontrado, lo más claro posible, preciso y estructurado de tal manera que sea fácil de entender por las personas involucradas no expertas en el ámbito tecnológico.

   Se debe comunicar el significado de la evidencia digital encontrada, los hechos, sus conclusiones y justificar el procedimiento empleado, este informe puede ser entregado a los responsables de auditoría interna en caso de existir, al área de seguridad informática, al responsable del área involucrada, dueños y/o accionistas de la institución.

   Este documento será la garantía para inculpar al responsable del incidente ocurrido, ya sea para despido o para acusación judicial si así lo dispone la institución víctima del delito ocurrido.

6 ANALISIS DE EVIDENCIAS DEL REGISTRO DE EVENTOS DE WINDOWS DEL SERVIDOR KASPERSKY

Nombre del equipo: AVS

Sistema Operativo: Windows Server 2008 R2

Funcionalidad: Servidor de Kaspersky Administration Kit

Fecha y hora de inicio: 18 de abril de 2010

Institución: Oficinas **del Proyecto TIC, UNAN – Managua, Pabellón -14**

Para el análisis de la investigación realizada fue necesario instalar **ACRONIS TRUE IMAGE SERVER V.8.0.** en una laptop **Sony Vaio** con sistema Operativo **Windows 7** y anti virus **Kaspersky v.6.0.** la cual será asignada para el análisis de evidencias de la información respaldada.

Para la búsqueda de evidencias registradas en el servidor se ejecutaron las siguientes acciones:

Búsqueda de archivos eliminados: Se escaneó la imagen realizada con la herramienta **GetData Recover My Files,** permitiendo hacer una búsqueda completa de archivos borrados.

El escaneo realizado por Recover My Files permitió recuperar e identificar 1,677 archivos borrados, entre ellos los siguientes tipos de datos:

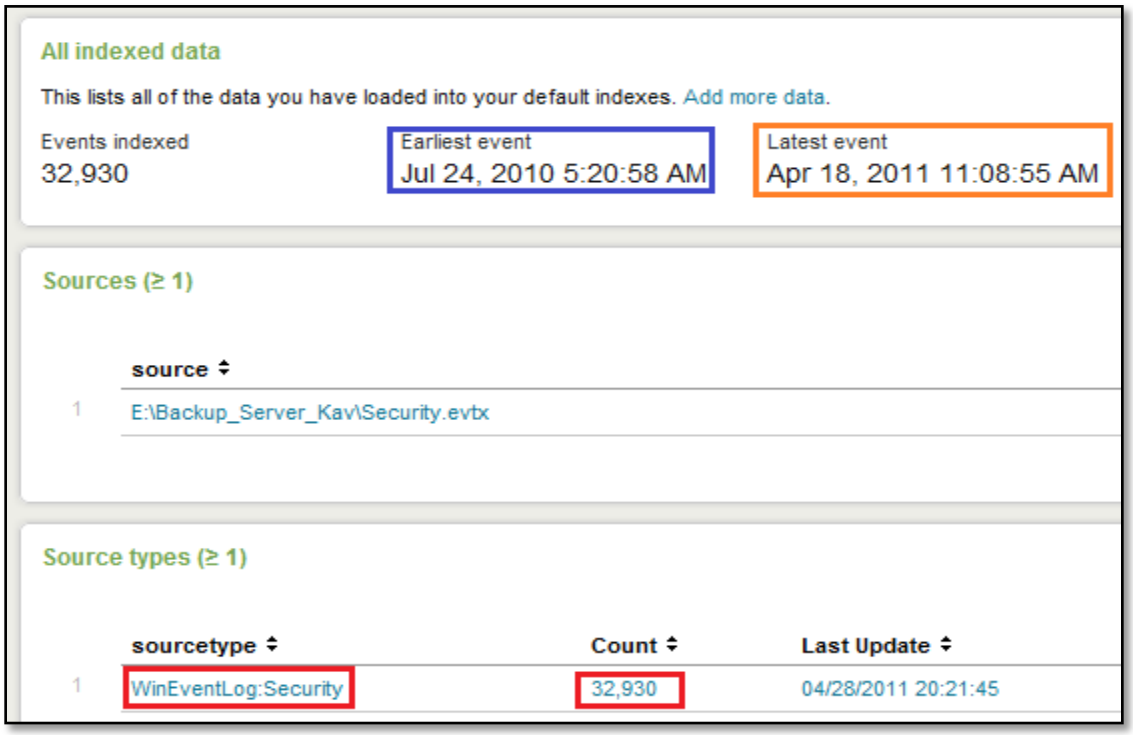
Tipo Archivos	Encontrados
*.pdf (Acrobat PDF)	6
*.doc (Word)	4
*.xls (Excel)	12
*.txt	15
*.bmp (imagen)	14
*.jpeg (imagen)	33
*.zip (compreso)	50
Otros	1555

Los archivos recuperados deberán ser revisados por los administradores de servidores del Proyecto TIC en supervisión del jefe inmediato o delegado, quienes establecerán parámetros para determinar si la información recuperada hace referencia a las funciones realizadas por ellos mismos en el servidor y si existe justificación del porque fue eliminada.

Análisis de Registros generados por el Servidor: Estos registros son generados como efecto de la programación del servidor, y son inalterables por una persona, los mismo son llamados registros de eventos de seguridad (Logs)

La revisión del Logs de seguridad del servidor fue realizada con la aplicación **Splunk**, servicio en línea que permite buscar, alertar e informar sobre datos online, o datos históricos de Tecnología de la información.

El archivo log de seguridad analizado contiene información de eventos registrados en el servidor kaspersky del Proyecto TIC desde el 24 de julio de 2010 a las 05:20:58 a.m. hasta el 18 de Abril de 2011 a las 11:08:55 a.m. en el cual se identificaron 23 eventos con diferentes acciones, entre ellos se analizaron los más importantes.



Detalle de eventos ocurridos en el servidor:

Código de evento	Frecuencia	Porcentaje	Descripción
4624	10028	30,45 %	Una cuenta ha iniciado sesión correctamente.
4672	7922	24,06 %	Privilegios especiales asignados al nuevo inicio de sesión
4634	7293	22,15 %	Una cuenta ha cerrado la sesión
4625	3557	10,8 %	Una cuenta no pudo iniciar sesión
4648	1947	5,91 %	Se ha intentado un inicio de sesión mediante credenciales explícitas
4907	346	1,05 %	Se han cambiado la configuración de auditoría en objeto
5038	334	1,01 %	Integridad de código determinó que el hash de imagen de un archivo no es válido. El archivo podría estar dañado debido a modificación no autorizada o no es válido el valor de hash podría indicar un posible error de dispositivo de disco
4616	297	0,9 %	Se cambió la hora del sistema
5061	228	0,69 %	Operación criptográfica
5058	228	0,69 %	Operación de archivo de clave
5033	129	0,39 %	El controlador de Firewall de Windows se ha iniciado correctamente
5024	129	0,39 %	El servicio Firewall de Windows se ha iniciado correctamente
4902	129	0,39 %	Se creó la tabla de directivas de auditoría por usuario
4608	129	0,39 %	Windows se está iniciando
4647	93	0,28 %	Cierre de sesión del usuario iniciado
1101	88	0,27 %	Los sucesos de auditoría se han caído por el transporte
1100	40	0,12 %	El servicio de registro de eventos se ha apagado

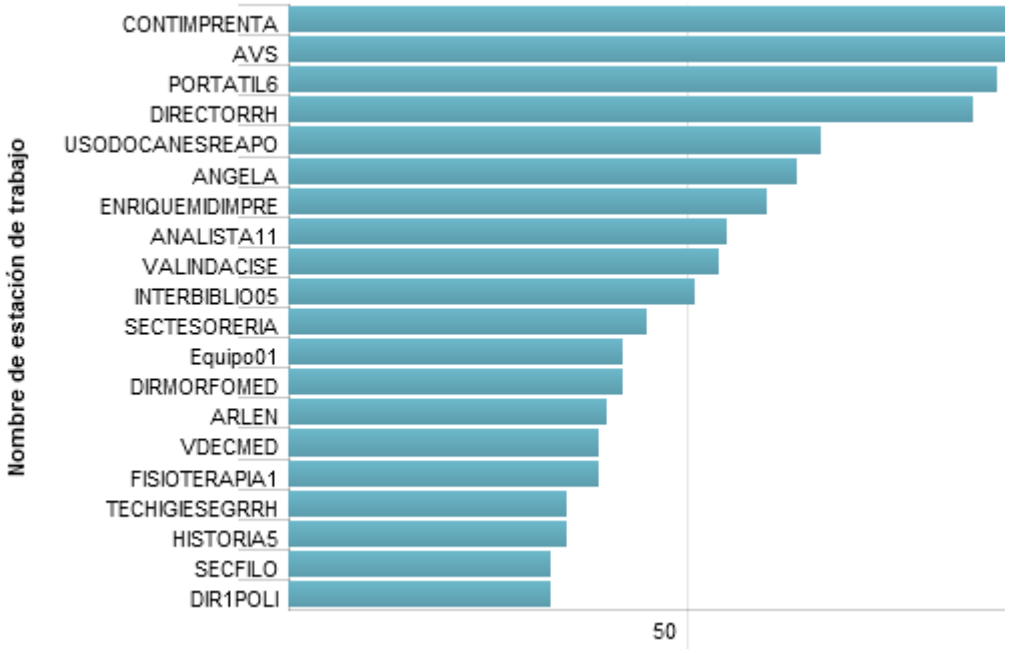
Código de evento	Frecuencia	Porcentaje	Descripción
4776	4	0,01 %	El controlador de dominio intentaba validar las credenciales para una cuenta
4732	3	0,01 %	Se agregó un miembro a una seguridad habilitada grupo local
4739	2	0,01 %	Se cambió la directiva de dominio
4733	2	0,01 %	Se ha quitado un miembro de un grupo local con seguridad habilitada
4738	1	0 %	Se ha modificado una cuenta de usuario
4724	1	0 %	Se intentó restablecer la contraseña de una cuenta

Evento 4625 – "Una cuenta no pudo iniciar sesión" porque el **usuario es desconocido o la contraseña es incorrecta:** El evento retorno 123 nombre de cuentas utilizadas.

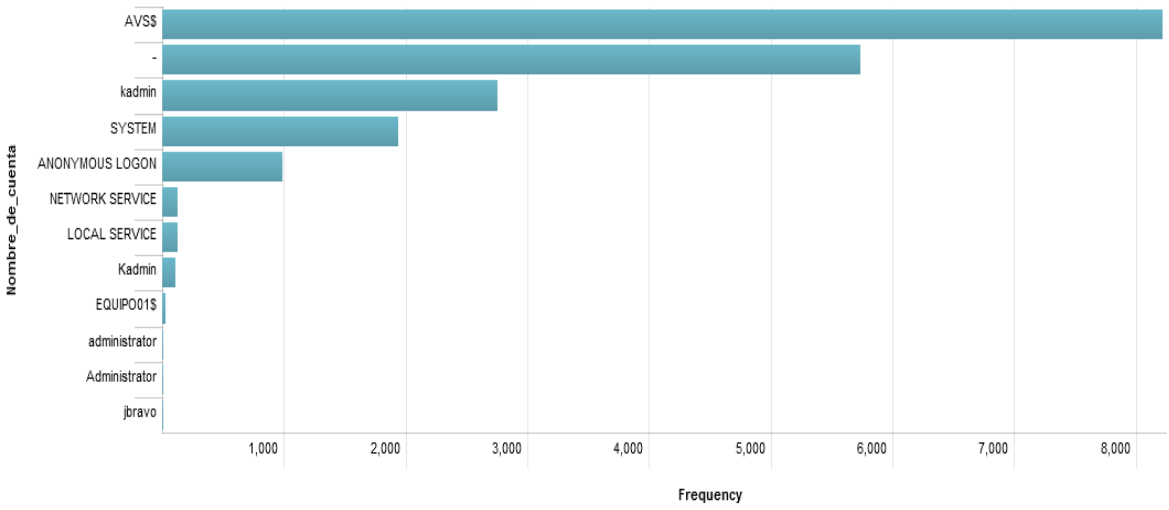
Cuentas de usuarios que presentaron intentos fallidos elevados

Nombre_de_cuenta	Intentos	percentaje
- (Administrador)	3389	47.64 %
Administrador	604	8.49 %
William Barberena	245	3.44 %
kadmin	169	2.38 %
AVS$	168	2.36 %
Angelical	104	1.46 %
Usuario Lapto	89	1.25 %
Abel MembreÃ±o	82	1.15 %
Martha	74	1.04 %
Marcia	65	0.91%

Gráfica de los equipos que intentaron conectarse y generaron el evento 4625



Evento 4624 – "Una cuenta ha iniciado sesión correctamente"



El evento 4624 muestra la siguiente información:

Campos de red, indican dónde se originó una solicitud de inicio de sesión remota (información del equipo que realizo algún tipo de conexión en algunos casos podría ser el atacante), no siempre es posible disponer del nombre del usuario y dirección IP.

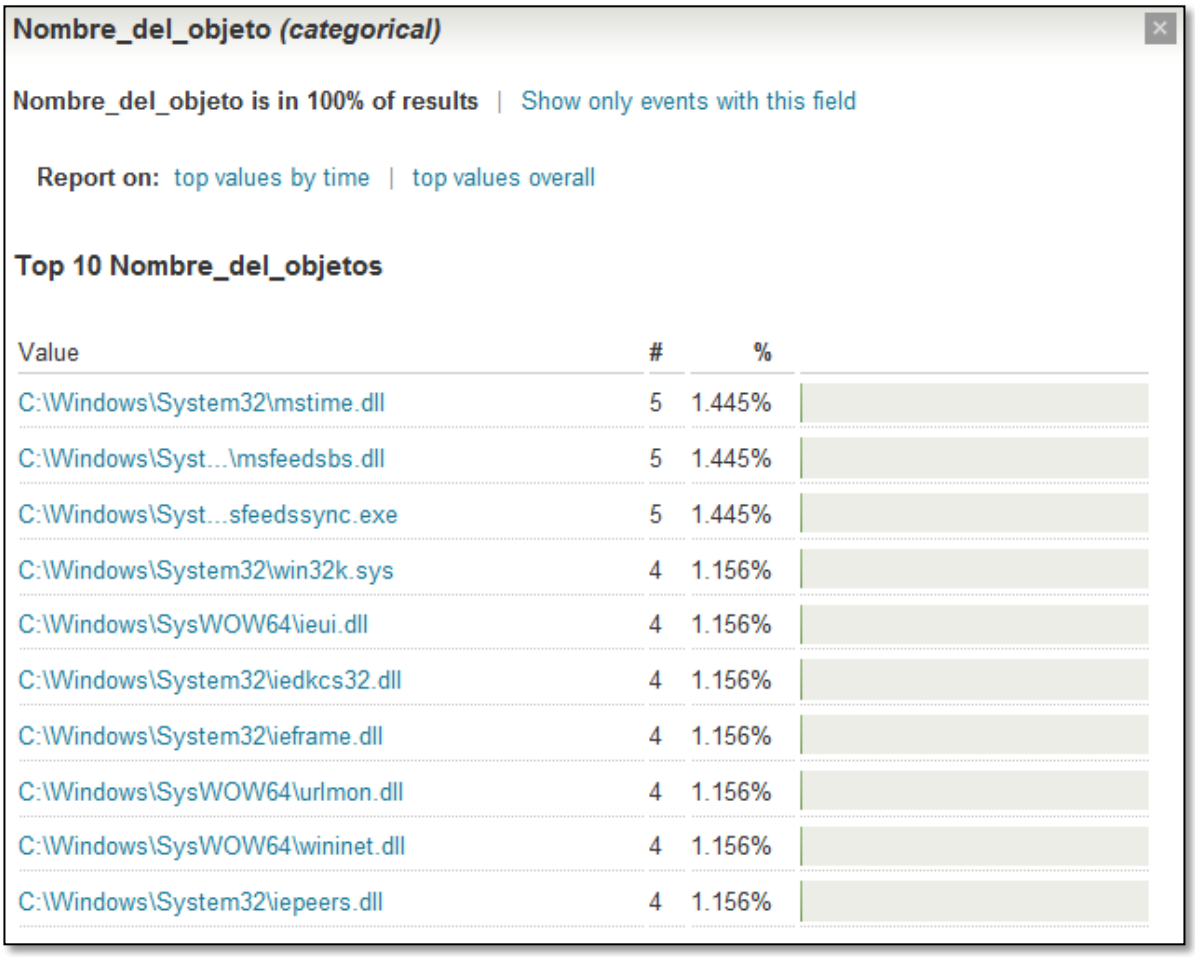
```
Información de red:
Nombre de estación de trabajo: AVS
Dirección de red de origen: 10.1.120.30
Puerto de origen: 59022

Información de autenticación detallada:
Proceso de inicio de sesión: User32
Paquete de autenticación: Negotiate
Servicios transitados: -
Nombre de paquete (sólo NTLM): -
Longitud de clave: 0
```

Se logro detectar que la mayor frecuencia de conexión realizada hacia el servidor fue mediante el tipo de inicio 3, este tipo de inicio se refiere a conexiones a carpetas compartidas en el servidor de Kaspersky, en este caso se logro detectar que la carpeta compartida a la que se está accediendo es la **carpeta de actualización de bases de datos del antivirus**. La otra forma de conexión utilizada al servidor fue el tipo de conexión 5 por conexión remota o terminal services.

Evento 4907 – "Se ha cambiado la configuración de auditoría en objeto"

En el analisis del **evento 4907** se detectaron 346 registros por cambio en la configuración de auditoría de 184 objetos ubicados en 2 carpetas con auditorias de seguridad, **archivos de programas (Internet explorer, Windows mail, Worpad.exe) y en la carpeta Windows y System32 del sistema operativo, (librerías dll)**



Nombre_del_objeto *(categorical)*

Nombre_del_objeto is in 100% of results | Show only events with this field

Report on: top values by time | top values overall

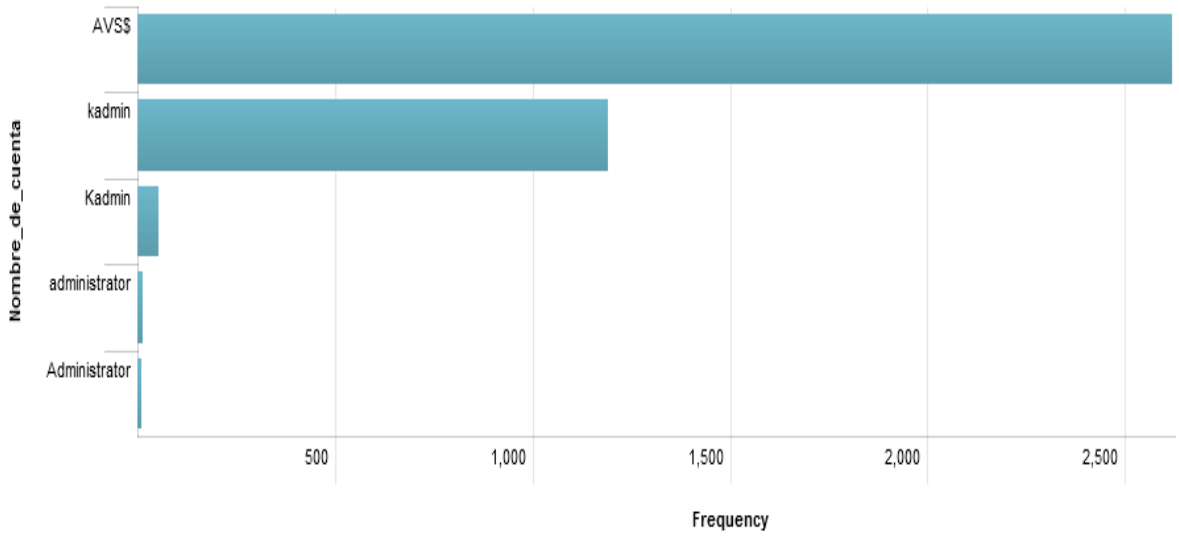
Top 10 Nombre_del_objetos

Value	#	%
C:\Windows\System32\mstime.dll	5	1.445%
C:\Windows\Syst...\msfeedsbs.dll	5	1.445%
C:\Windows\Syst...sfeedssync.exe	5	1.445%
C:\Windows\System32\win32k.sys	4	1.156%
C:\Windows\SysWOW64\ieui.dll	4	1.156%
C:\Windows\System32\iedkcs32.dll	4	1.156%
C:\Windows\System32\ieframe.dll	4	1.156%
C:\Windows\SysWOW64\urlmon.dll	4	1.156%
C:\Windows\SysWOW64\wininet.dll	4	1.156%
C:\Windows\System32\iepeers.dll	4	1.156%

Evento 4648 – "Se ha intentado un inicio de sesión mediante credenciales explícitas"

Este evento se genera cuando un proceso intenta iniciar sesión en una cuenta especificando explícitamente las credenciales de la cuenta. Suele producirse en configuraciones de tipo de lote como tareas programadas, o cuando se usa el comando RUNAS (Opción click derecho sobre el ejecutable y luego se selecciona la opción ejecutar como).

Gráfica de cuentas que generaron el evento 4648



Evento 4738 – "Se ha modificado una cuenta de usuario

De este evento se encontró un único cambio de cuenta de usuario, el cual no representa ninguna anomalía.

En el análisis de logs realizado no se logro determinar ningún delito informático realizado en el servidor de Kaspersky. – ***Ver anexo 6 Informe de hallazgo***

7 Estudio de factibilidad

7.1 Factibilidad Técnica

Para el análisis de la metodología se consideró necesario los siguientes recursos.

7.1.1 Recursos de Software

Recursos	Descripción
Sistema operativo	Windows Server 2008 R2
Antivirus	kaspersky Adminstration kit
Herramienta para recuperación de archivos borrados	GetData – Recover My Files
Analizador de logs	Splunk

7.1.2 Recursos Humanos

Recursos	Cantidad
Investigadores	3

7.2 Factibilidad Económica

7.2.1 Hardware

Descripción	Cantidad	Costo Unitario (U$)	Total (U$)
Servidor de Antivirus Procesador 2 dual Core Memoria RAM 4 GB Disco Duro 50 GB Tarjeta de red 1 (Ethernet) Unidad de CD-ROM Estabilizador Bacteria Mouse, y teclado Tarjeta de Red 1 (Ethernet)	1	2,000	2,000
Impresora Epson TX210 Series	1	100	100
Total			**2,100**

7.2.2 Software

Disponibilidad de software	Costo
Sistema Operativo: Windows Server 2008 R2	**U$ 2899.00**
Kaspersky Lab 6.0 Corporativo	**U$ 00.00**
GetData – Recovery My Files	**U$ 69.95**
SPlunk (Versión Gratis por un mes)	**U$ 00.00**
Acronis True Image Server	**U$ 99.00**
Total	**U$ 69.95**

7.2.3 Recursos Humanos

Recursos	Cantidad	Costo
Investigadores	3	U$ 1,200.00

Se ha estimado el costo mínimo necesario para el desarrollo de la investigación:

Descripción	Cantidad	Costo
CD Re-escribible	2	$1.00
Papel Bond (Resmas)	3	$7.00
Cartuchos para Impresora	4	$60.00
Alimentación	-	$150.00
Transporte		$150.00
Cuadernos	2	$2.00
Fotocopias	-	$5.00
Encolochados	5	$10.00
Horas máquina	-	$150.00
Total		**$535.00**

La investigación tiene un costo total de U$ 1,804.95 dólares

Actualmente el Proyecto TIC cuenta con el equipo necesario y las licencias de Windows Server 2008 y Kaspersky Lab para el desarrollo de la investigación.

7.3 Factibilidad operacional

Para el cumplimiento de esta metodología no será necesario contratar más personal.

CONCLUSIONES

Después de preservar y analizar las evidencias encontradas en el servidor de Kaspersky del proyecto TIC se concluye lo siguiente:

- La elaboración de la metodología para el tratamiento de evidencias en servidores Windows permite documentar todo el proceso de investigación y elaborar paso a paso un informe de hallazgo ante un incidente o delito informático.

- Se aplicaron herramientas para capturar, preservar y analizar de forma eficaz la información del servidor.

- El análisis de evidencias realizado en el servidor Kaspersky no presentó indicios de ataques.

Por lo anterior, la metodología aplicada para el tratamiento de evidencias en el servidor Kaspersky del Proyecto TIC, cumple con las necesidades planteadas que dieron origen al alcance del presente trabajo.

RECOMENDACIONES

Para mejorar la seguridad del Servidor se recomienda lo siguiente:

1- Implementar políticas de seguridad basado en estándares internacionales.

2- Capacitar e informar al personal seguridad en los temas de delitos informáticos.

3- Hacer una revisión en la configuración del agente de Kaspersky anti virus, para solventar el problema de actualización de las bases de datos del anti virus en los equipos clientes, ya que esto es lo que provoca se registre gran cantidad de conexión hacia la carpeta compartida de actualización.

4- Instalar actualizaciones y parches de seguridad de Microsoft Windows Server 2008 R2

5- Configurar alertas a través de Kaspersky Administration Kit **(en los eventos)** que se consideren importantes **(críticos)** para que puedan ser almacenados y visualizados desde el visor de sucesos.

6- Crear configuración de seguridad personalizadas según la necesidad de los grupos de trabajo de la institución.

7- Crear proceso de revisión de reportes de protección de anti virus con el objetivo de detectar, corregir y prevenir infecciones por virus en la institución.

BIBLIOGRAFÍA

1. Cano Martínez, Jeimy J. Computación Forense, Edición 2009, Editorial ALFAOMEGA GRUPO EDITOR.

2. Ferreyra Cortez, Gonzalo. Virus en las Computadoras. Segunda Edición, 1991. Macrobit Editores, S.A de C.V.

3. Tamayo y Tamayo, Mario. Metodología formal de la investigación científica. Primera Edición, 1977. Editorial LIMUSA.

WEB GRAFÍA

2. La Computación Forense y el Modelo de Gobernanza de Seguridad Digital
   www.isaca.org

3. Proyecto CTOSE
   http://www.belt.es/noticias/2003/noviembre/3/La_ue.htm
   http://www.observa.com.uy/MasLeidas/nota.aspx?id=6849

4. Daniel Fernández, Bleda, "Informática Forense"
   http://www.isecauditors.com/downloads/present/hm2k4.pdf

5. Juan David, Gutiérrez, Giovanni Zuccardi, "Informática Forense", Noviembre 2006

6. Pasos de la Computación Forense
   http://es.wikipedia.org/wiki/C%C3%B3mputo_forense#Pasos_del_c.C3.B3mputo_forense

7. Servidores Windows 2008 R2
   http://www.microsoft.com/windowsserver2008/es/xl/default.aspx

8. Directivas del sistema
   http://fmc.axarnet.es/winnt4svr/administracion/tema_05.htm

9. Kaspersky Anti-virus
   http://latam.kaspersky.com/productos

ANEXOS

ANEXO 1

Entrevista 1:

Entrevistado: Derman Zepeda Vega

Cargo: Administrador de Redes

Entrevistador: Zabdiel Zepeda Vega

Estudiante de Lic. en Ciencias de la Computación

Fecha: 18 de abril de 2011

1. **¿Cuántos servidores tiene el proyecto TIC de la UNAN – Managua?**

   R= Actualmente tenemos una cantidad de 16 servidores físicos y un total de 32 servidores físicos y virtuales.

2. **¿Qué tipo de servicios ofrecen estos servidores y bajo que plataforma se ejecutan (LINUX, WINDOWS, etc)?**

   R= Linux en todos los servicios de redes y windows 2003 y 2008 R2 para las aplicaciones.

3. **¿Qué tipo de amenazas y ataques han surgido en estos servidores?**

   R= La amenaza de un ataque por parte de un hacker siempre son tomadas en cuenta, sin embargo por los cortafuegos solo se ha detectado intentos de acceso por medio de puertos ssh.

4. **¿Quiénes son los responsables de ofrecer mantenimiento a los servidores?**

   R= Existen dos personas a cargo de esta área, uno encargado de los servidores en **Windows** y uno a cargo de los servidores **Linux.**

5. **¿Alguna vez los servidores han recibido soporte externo, por qué?**

   R= No, hasta la fecha el soporte se realiza por personal interno, el soporte externo cubre únicamente garantía de hardware.

6. **¿Qué metodología utilizan para resolver incidentes de ataques en los servidores?**

   R= Aun no tenemos una metodología para este tipo de problemas.

7. **¿Se ha implementado alguna vez algún tipo de metodología de informática forense, para detectar y manipular las evidencias de ataques?**

   R= No en este momento.

8. **¿Estarían de acuerdo en realizar un estudio aplicando una metodología para detectar, analizar y manipular evidencias de los ataques que se hayan dado al servidor?**

   R= Si, por supuesto que estaríamos dispuestos a implementar una en algún momento.

Entrevista 2:

Entrevistado: Derman Zepeda Vega

Cargo: Administrador de redes

Entrevistador: Zabdiel Zepeda Vega

Estudiante de Lic. En Ciencias de la Computación

Fecha: 18 de Abril de 2011

1. **¿El proyecto TIC o la UNAN-Managua dispone de nomas de seguridad informática documentadas y aprobadas por las autoridades superiores?**

   R= En este momento no poseemos ninguna norma aprobada.

2. **¿Alguna vez el proyecto TIC ha realizado una propuesta formal a las autoridades superiores en donde se dé a conocer la importancia de aplicar normas de seguridad informática con el propósito de dar respaldo a las políticas de seguridad, las cuales deben ser cumplidas por los empleados?**

   R= En el año 2010 se realizó una propuesta de políticas de uso de equipos informáticos, uso de internet y del correo electrónico, con el fin de disminuir los riesgos en los equipos finales.

3. **¿En base a qué criterios clasifican la importancia de la información y el nivel de riesgo de los activos?**

   R= En base a los costos de los equipos activos y en base a la importancia de la información (Unicidad de la misma)

Entrevista 3:

Entrevistado: Juan Navas

Cargo: Administrador de Servidores

Entrevistador: Zabdiel Zepeda Vega

Estudiante de Lic. en Ciencias de la Computación

Fecha: 18 de abril de 2011

1. **¿Qué medidas de seguridad ofrece el TIC a los servidores?**

   R= A nivel físico, se encuentran ubicados en un local, fuera del alcance de los usuarios, y luego existen dos niveles de firewall para poder acceder a los mismo, se está trabajando por mejorar las políticas de acceso en los firewall.

2. **¿Existe algún procedimiento para la instalación y configuración de Servidores?**

   R= No, aun no existe, lo único es que hemos estandarizado las versiones de sistemas operativos que se instalan.

3. **¿En los servidores realizan algún tipo de configuración a las auditorias de seguridad locales de los servidores o prefieren mantener la configuración que por default se instala al momento de instalar el sistema operativo?**

   R= No se lleva ningún tipo de auditoría en los servidores.

4. **¿Los servidores o la red en la que estos se alojan disponen de sistemas de detección de intrusos (IDS)?**

   R= En este momento no tenemos un sistema IDS instalado. Estamos en proceso de instalación de uno.

5. **¿Qué tipo de reglas son consideradas en estos sistemas IDS?**

   R= No aplica

6. **¿Qué herramientas utilizan para monitorear el tráfico o ancho de banda de la red?**

   R= Utilizamos herramientas de software libre para gestionar las interfaces de los equipos de comunicación por medio de snmp

7. **¿Cuál es el seguimiento que se le da a este monitoreo?**

   R= El seguimiento es diario, y esto nos indica el flujo de tráfico desde los usuarios hasta los servidores o desde los servidores hacia el internet.

8. **¿La UNAN – Managua dispone de herramientas para la administración de usuarios?**

   R= Por el momento se está realizando el despliegue de un active directory y kaspersky para mejorar la administración de los endpoint.

9. **¿Qué dominio o control tienen con los host (equipos) de la red?**

   R= El control a los equipos aun no se ha implementado, debido a falta de políticas del uso de TICs

10. **Qué tipo de direccionamiento IP se utiliza en los servidores? Por qué?**

    R= Tenemos dos tipos de direccionamiento Privado para los servidores de acceso a la LAN de manera estática y direccionamiento publico también estático, para los servidores de servicios en Internet.

Entrevista 4:

Entrevistado: Ángela López Tórrez

Cargo: Encargada de Soporte Técnico de Redes

Entrevistador: Zabdiel Zepeda Vega

Estudiante de Lic. en Ciencias de la Computación

Fecha: 18 de abril de 2011

1. **¿Cuál es el problema que está presentando el Servidor de kaspersky?**

   R= Actualmente se ha detectado lentitud en el servicio. El servidor se apaga constantemente debido al crecimiento en los logs, la consola del antivirus pierde conexión a la red, no hay una buena sincronización entre los equipos que están registrados en la consola, debido a que el DNS tiene problemas con la resolución de nombre y debido a esto el estado de los equipos físicamente, no es el que se refleja en la consola.

2. **¿Cuántas personas tienen acceso al servidor de kaspersky?**

   R= Dos personas: Ángela López y Edison Cuevas.

3. **¿Qué tipos de acceso tienen estos usuarios?**

   R= Administrador

4. **¿Qué sistema operativo tiene instalado y que versión?**

   R= Windows Server 2008 R2 Enterprise.

5. **¿Qué tipo de actualizaciones tiene habilitada el Servidor de Kaspersky?**

   R = Actualización diaria.

6. **¿Cuántos equipos administra la consola de Kaspersky Admistration Kit?**

   R= Actualmente la consola de Kaspersky Administration Kit tiene instalado 300 equipos.

7. **¿Cuál es la versión de Kasperky Administration Kit?**

   R = Kaspersky Lab 6.0 Corporativo

8. **¿Qué tipo de mantenimiento se realiza en el servidor y con qué frecuencia?**

R= El mantenimiento que se realiza es:

- Realizar un respaldo mensual de la base de datos de la consola, es decir se respalda la estructura que actualmente tiene la consola.

- Verificar que las tareas programadas en la consola, se estén realizando correctamente en los equipos.

- En el repositorio de virus, ver cuales equipos son los que están infectados y dependiendo de la cantidad y el tipo de virus, se desinfecta desde la consola y se le informa al técnico en reparación y mantenimiento para que proceda a eliminar los virus al equipo. Para esto se tienen que usar herramientas adicionales al kaspersky en el caso de que se encuentren virus que no se puedan eliminar con kaspersky.

- Se realice una visión constante en los grupos ya creados para que los equipos estén en el que les corresponde.

- Revisar las directivas de protección cuando hay bloqueo de los equipos, en la instalación de algún software, configuración de impresora, acceso a módems para internet, etc.

- Instalar y desinstalar aplicaciones de forma remota en los equipos.

- Actualizar las instalaciones de antivirus en los equipos que se les ha realizado cambio de los parámetros de red, como dirección IP, nombre etc.

- Instalación de licencias en los equipos que todavía no se ha instalado.

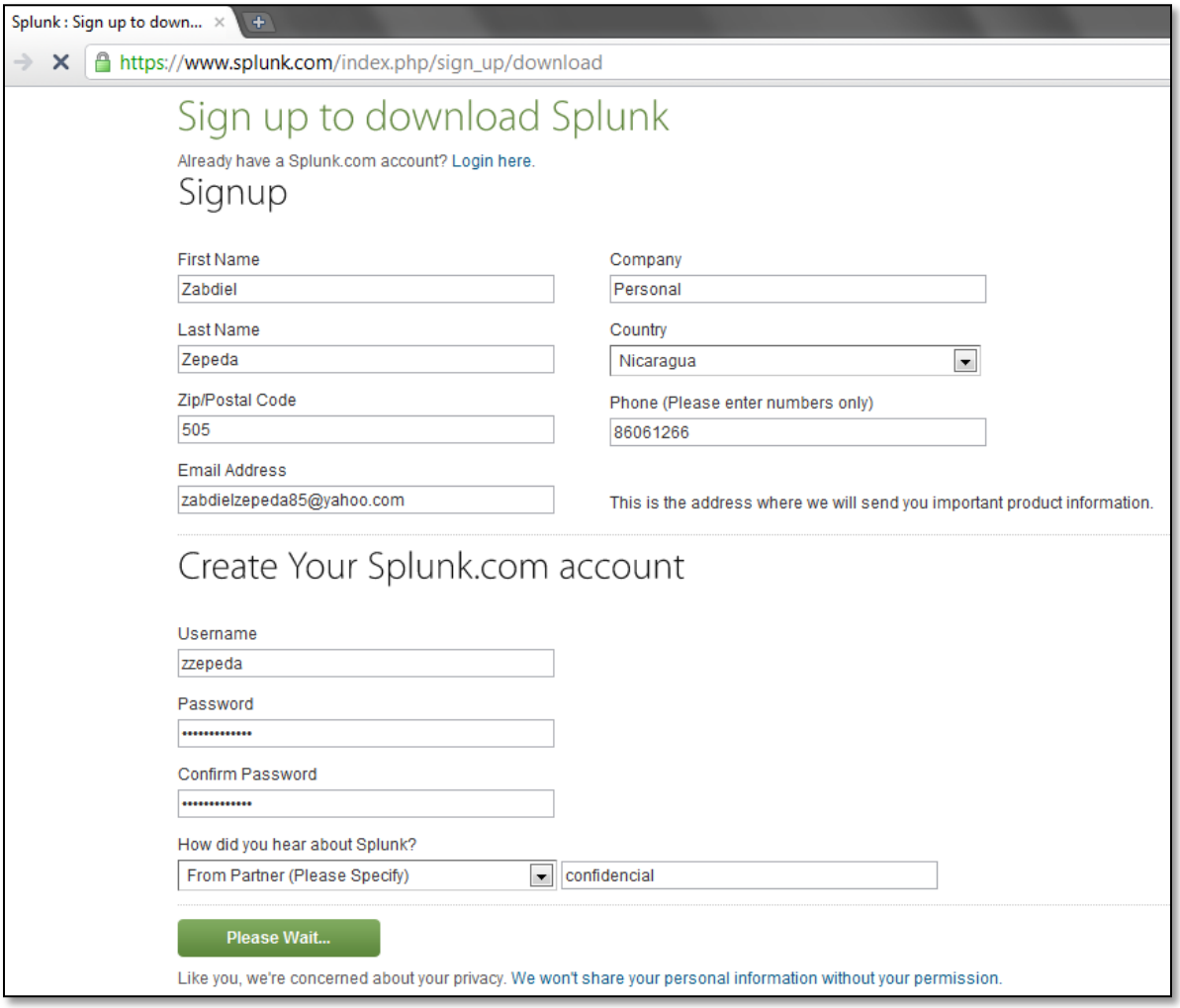
ANEXO 2

Instalación de herramienta para el análisis del log de seguridad windows del Servidor de Kaspersky del Proyecto TIC.

Nombre de aplicación: SPLUNK

Versión Gratuita (30 días)

Para descargar aplicación es necesario registrarse en la web de Splunk (www.splunk.com)



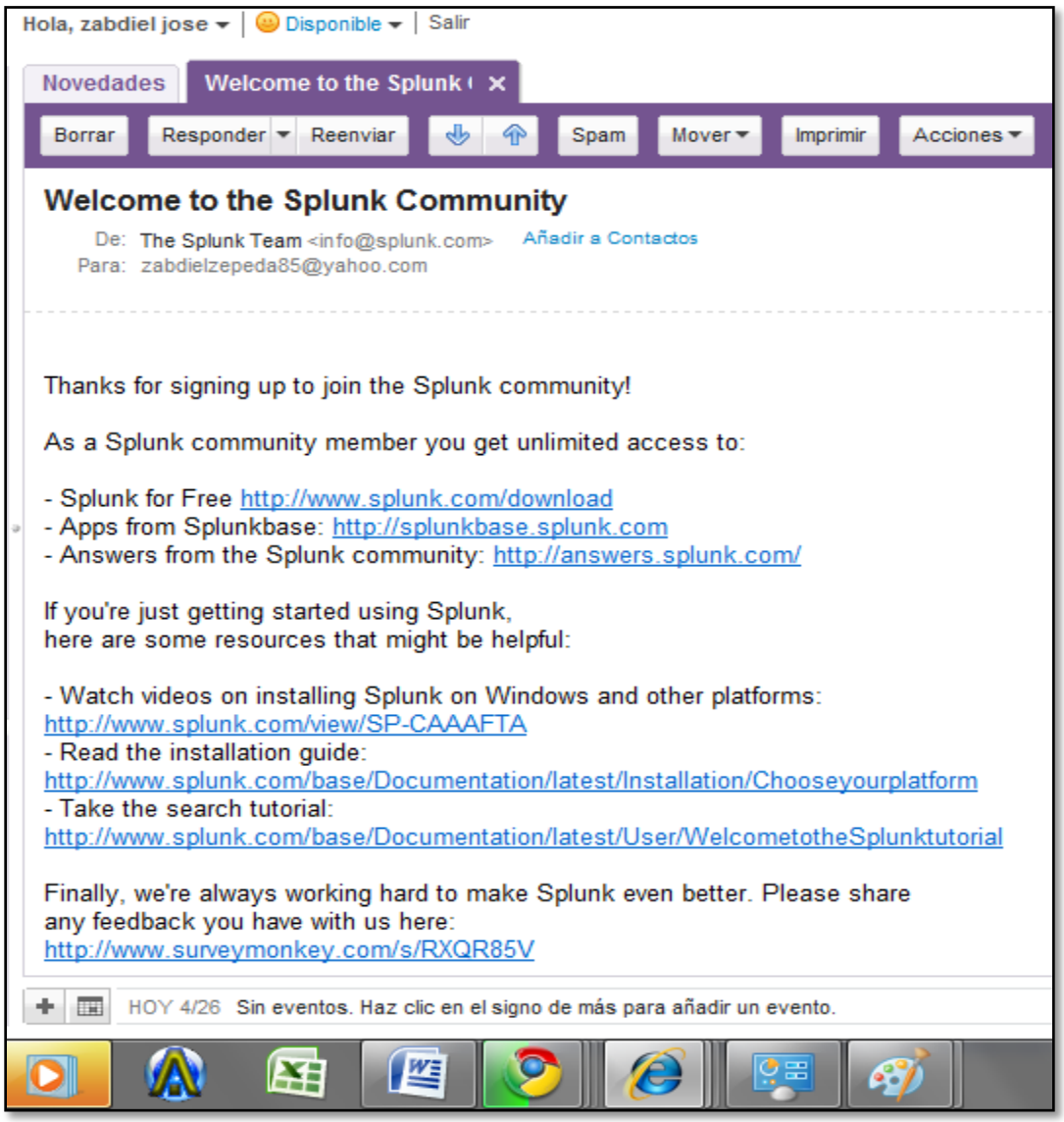
Una vez registrado automáticamente el sitio web de **Splunk** se encarga de enviar el siguiente mensaje de notificación vía correo electrónico:

Como miembro de la comunidad Splunk, tendrá acceso ilimitado a:

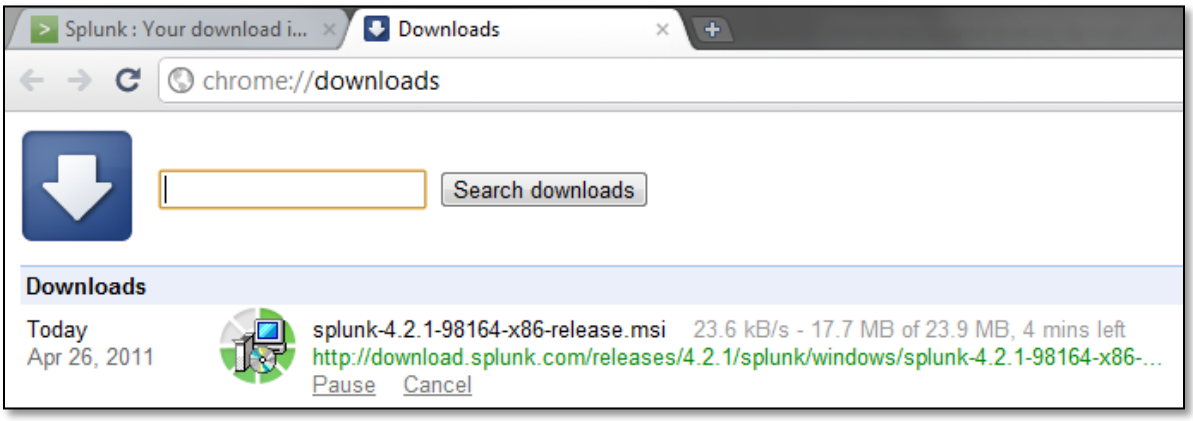
Splunk (gratis)

Aplicaciones de Splunkbase

Respuestas de la comunidad splunk

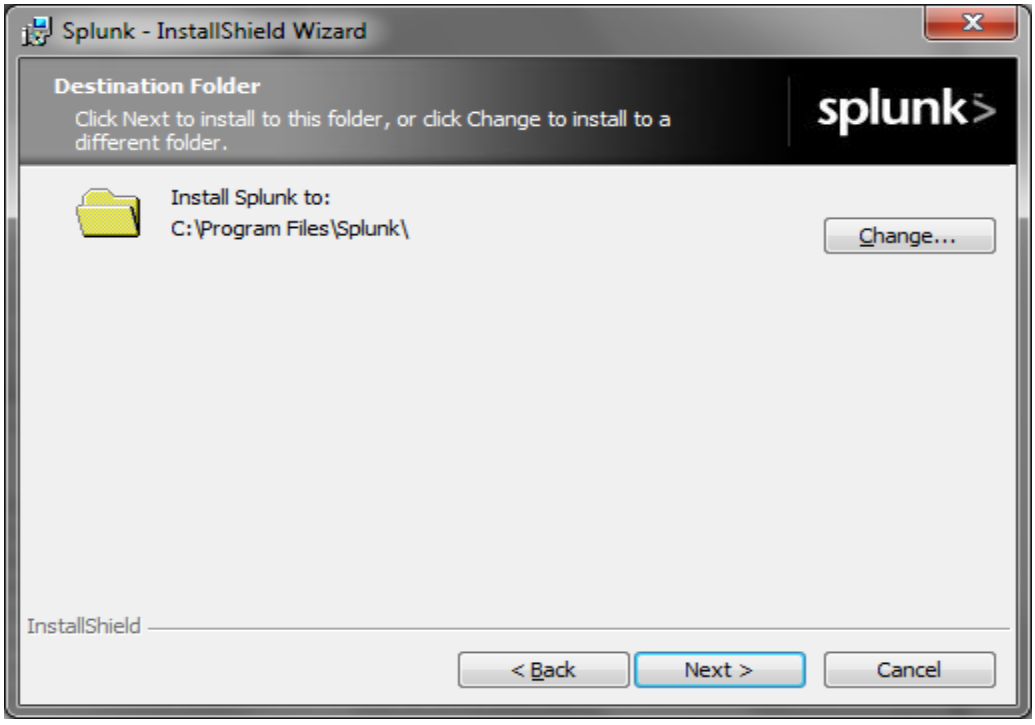


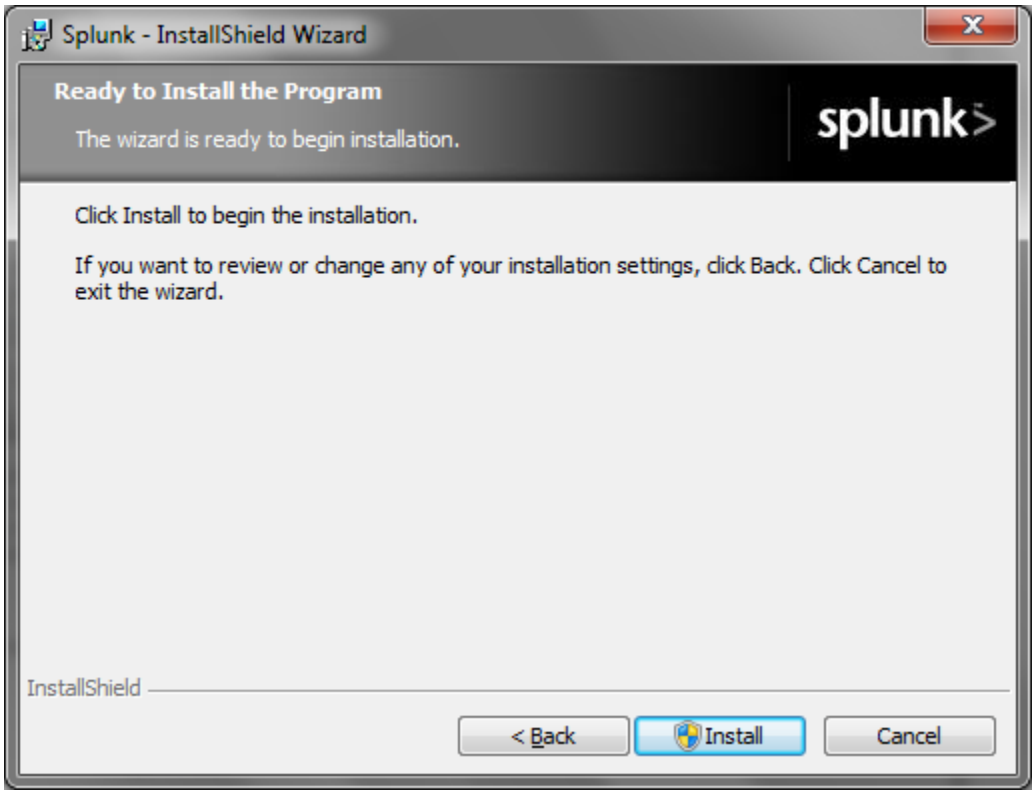
Descarga del Software Splunk

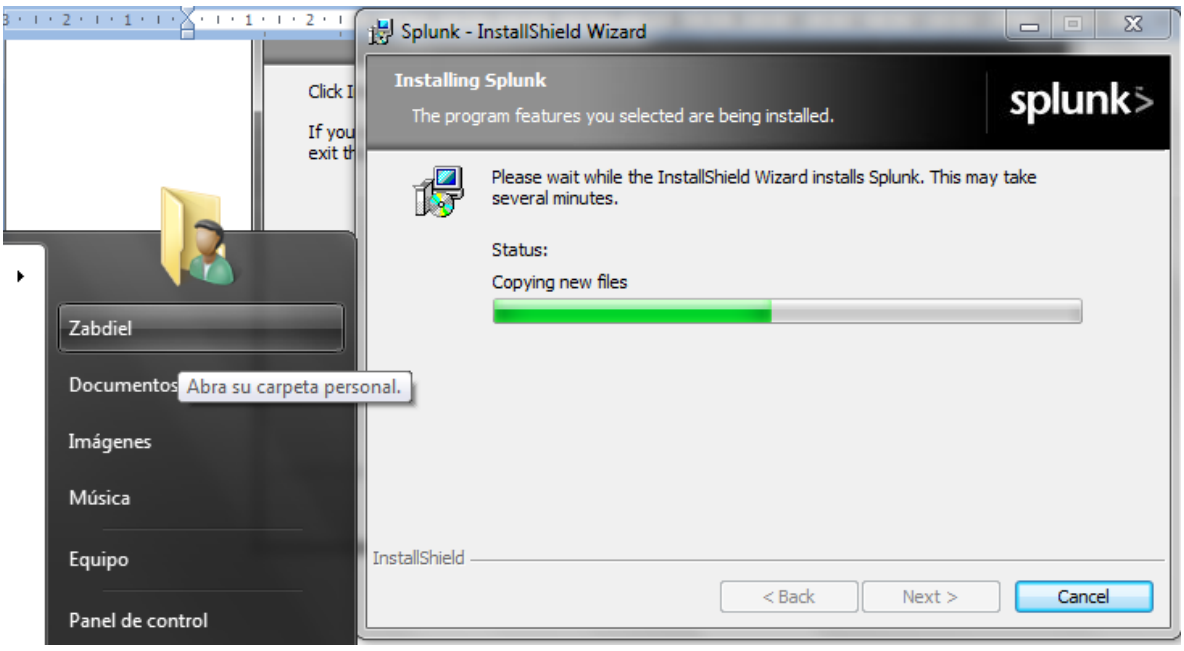


Instalación del Software:


Splunk - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
splunk>
SPLUNK SOFTWARE LICENSE AGREEMENT
THIS SPLUNK SOFTWARE LICENSE AGREEMENT (THE "AGREEMENT") GOVERNS ALL SOFTWARE PROVIDED BY SPLUNK INC. ("SPLUNK") INCLUDING FREE SPLUNK SOFTWARE ("FREE SOFTWARE") AND SOFTWARE PURCHASED THROUGH SPLUNK'S ONLINE STORE OR OTHER CHANNELS ("PURCHASED SOFTWARE"), COLLECTIVELY THE SPLUNK SOFTWARE ("SOFTWARE") AND ANY AND ALL UPDATES, UPGRADES, AND MODIFICATIONS THERETO. CONFIRMATION OF YOUR ORDERS ("ORDER CONFIRMATION") WILL BE DEEMED INCORPORATED INTO AND MADE PART OF THIS AGREEMENT.
I accept the terms in the license agreement
I do not accept the terms in the license agreement
Print
InstallShield
< Back
Next >
Cancel


Splunk - InstallShield Wizard
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
splunk>
Install Splunk to:
C:\Program Files\Splunk\
Change...
InstallShield
< Back
Next >
Cancel

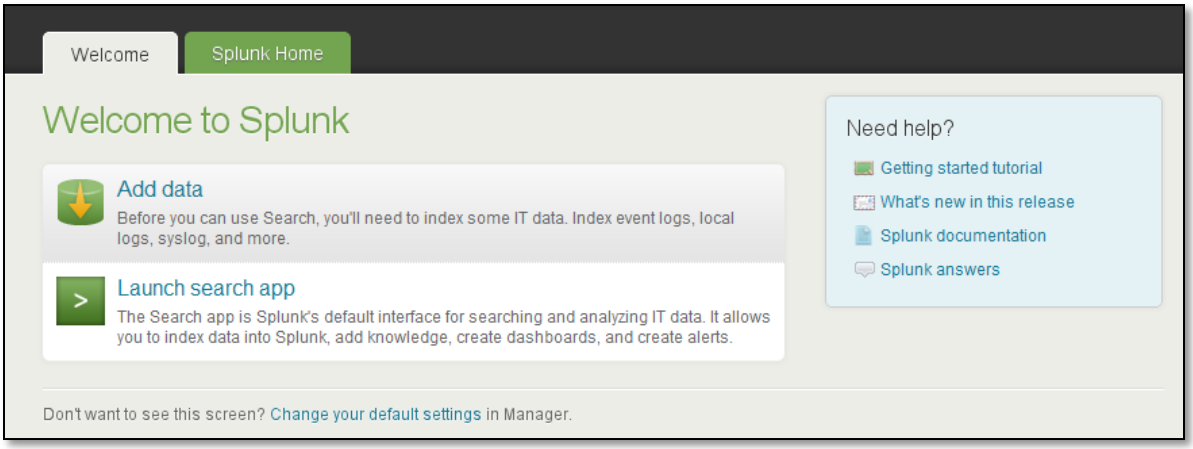

Splunk - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
splunk>
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

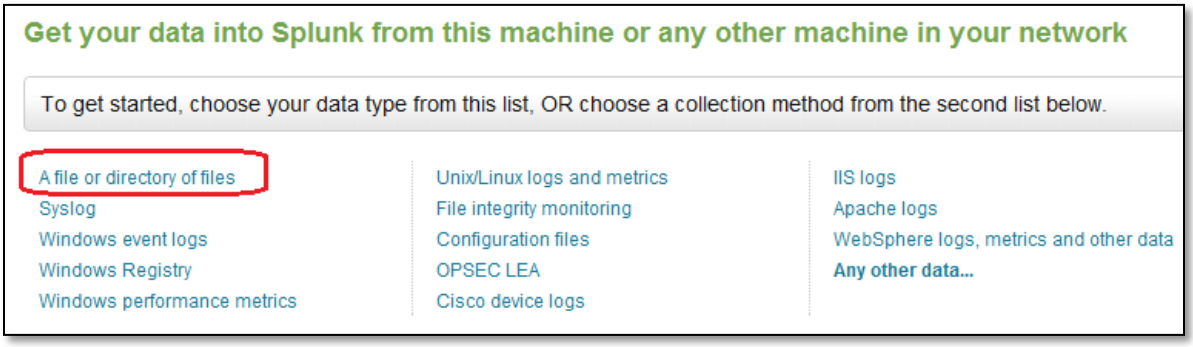

Splunk - InstallShield Wizard
Installing Splunk
The program features you selected are being installed.
splunk>
Please wait while the InstallShield Wizard installs Splunk. This may take several minutes.
Status:
Copying new files
InstallShield
< Back
Next >
Cancel
Zabdiel
Documentos
Abra su carpeta personal.
Imágenes
Música
Equipo
Panel de control

ANEXO 3

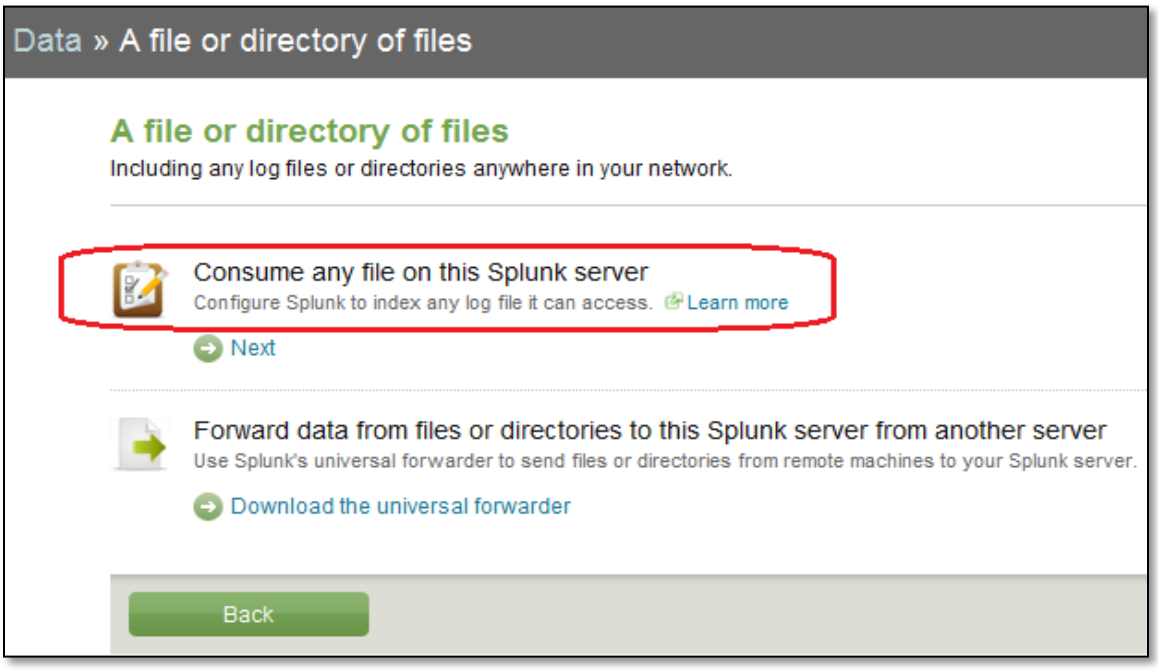
Proceso de carga del archivo log de seguridad en Splunk

Para dar inicio al proceso de carga se selecciona la opción **"ADD DATA"** y se selecciona el **archivo o directorio de archivos** donde se encuentra el log que se desea analizar.

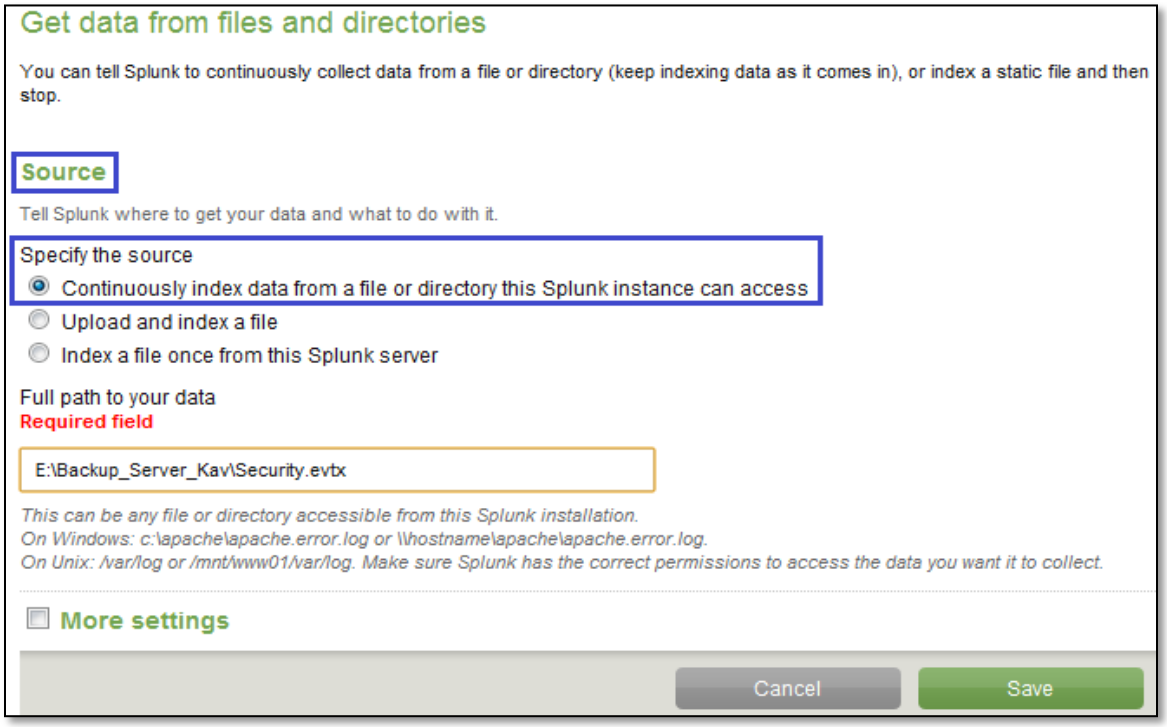




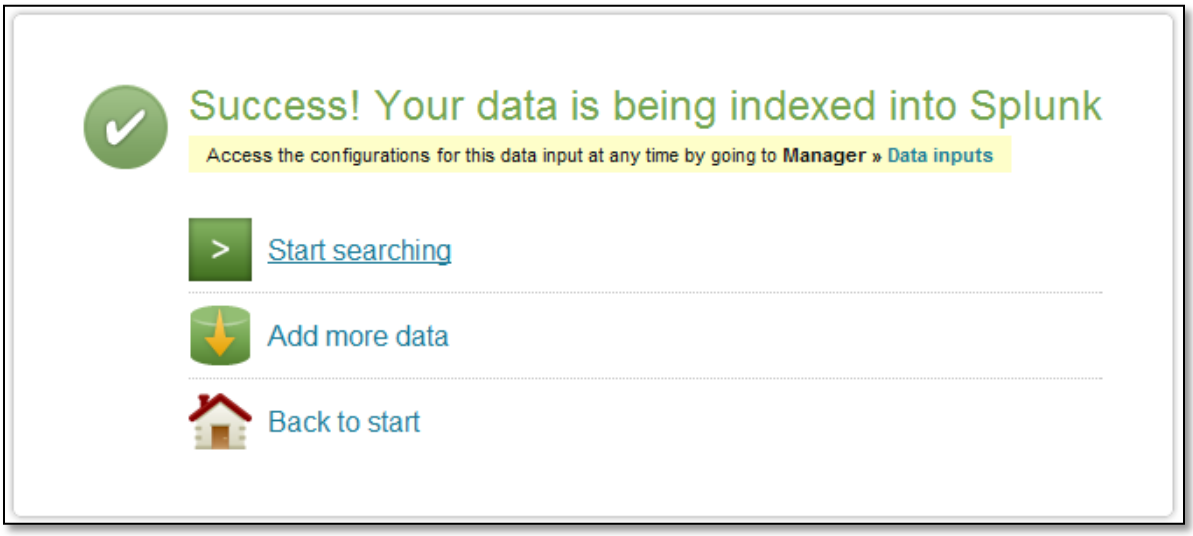
En la siguiente pantalla se especifica la opción "**Consume any file on this splunk Server**"

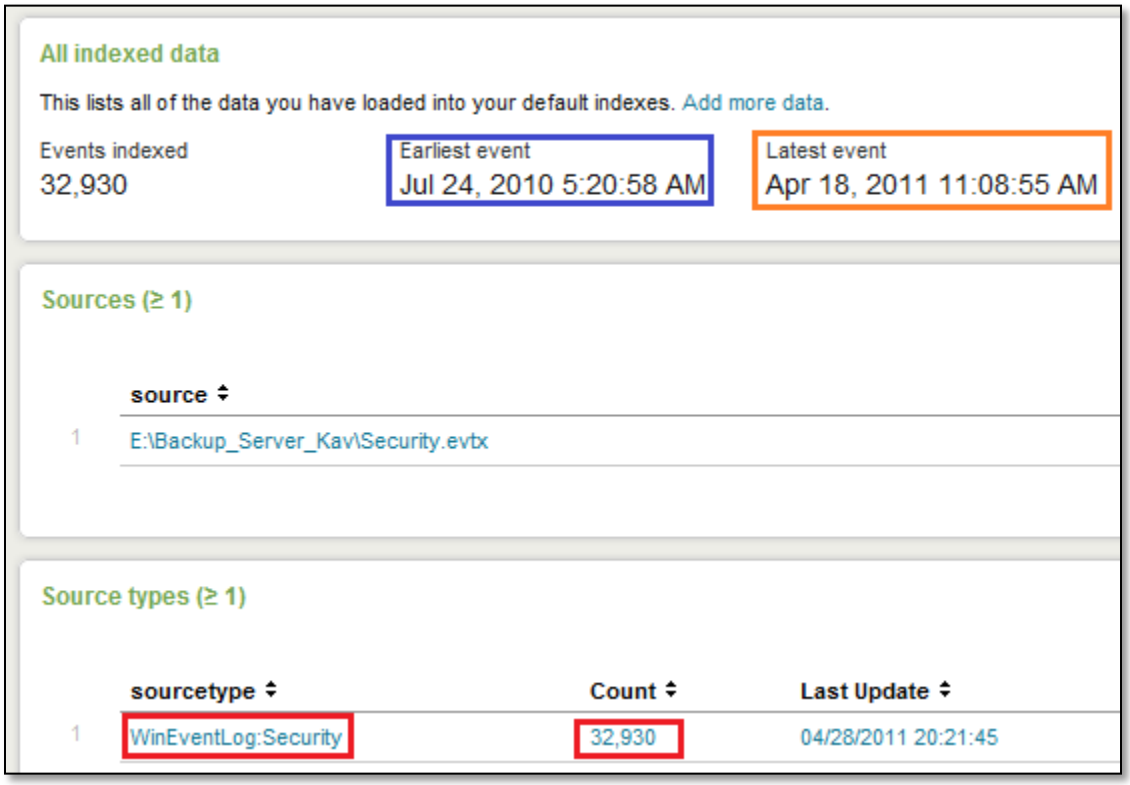


A continuación se especifica el origen del archivo log



Al guardar el origen del **logs** especificado **splunk** retorna el siguiente mensaje indicando que la data fue cargada en la aplicación **Splunk** satisfactoriamente.





Hosts (≥ 2)

	host	Count	Last Update
1	avs.unan.edu.ni	32,881	04/28/2011 20:21:45
2	avs	49	04/28/2011 20:19:54

EventCode *(numeric)*

EventCode is in 100% of results | Show only events with this field | Select/show in results

Report on: average over time | maximum value over time | minimum value over time | top values by time | top values overall

Min: 1,100 **Max**: 5,061 **Mean**: 4,643.034 **Stdev**: 235.166

Top 10 EventCodes

Value	#	%
4624	10,028	30.452%
4672	7,922	24.057%
4634	7,293	22.147%
4625	3,557	10.802%
4648	1,947	5.912%
4907	346	1.051%
5038	334	1.014%
4616	297	0.902%
5058	228	0.692%
5061	228	0.692%

ANEXO 4

Reporte de nombre de cuentas que no lograron iniciar sesión (Evento 4625)

Nombre de cuentas	Intentos	Porcentaje
-	3389	47.64
Administrador	604	8.49
William Barberena	245	3.44
Kadmin	169	2.38
AVS$	168	2.36
Angelical	104	1.46
Usuario Lapto	89	1.25
Abel MembreÃ±o	82	1.15
Martha	74	1.04
Marcia	65	0.91
Editorial	60	0.84
FISIOTERAPIA	59	0.83
Margarita Cordoba	55	0.77
Valinda	54	0.76
Interbiblio5	51	0.72
Angela Lopez	48	0.67
Maria Jose Mendoza	45	0.63
Vice Decanatura	43	0.6
UNAN	43	0.6
Norma-Martha	43	0.6
CC. Morfologica	42	0.59
Secretaria Academica	38	0.53
DIRECCION	38	0.53
Personal	36	0.51
Usuario	33	0.46
Decano	32	0.45
Administrator	31	0.44
Medicina	29	0.41
Administrator	28	0.39
PERSONAL	28	0.39

Nombre de cuentas	Intentos	Porcentaje
Ma Asuncion Morales	27	0.38
Biblioteca	27	0.38
XXXX	26	0.37
Materno Infantil	23	0.32
Raul Ruiz	22	0.31
Historia	22	0.31
Deportes	21	0.3
Usuario	20	0.28
BIOANALISIS	20	0.28
ARQ	20	0.28
USER	19	0.27
AntropologÃa	19	0.27
Picado	17	0.24
EnfermerÃa	17	0.24
REBECA SALAS	16	0.22
Miriam Castillo	16	0.22
Lidia Suarez	16	0.22
Ing. Civil	16	0.22
Henry Quintanilla	16	0.22
Ally Reyrs	16	0.22
Angela	15	0.21
SubDir Docente	15	0.21
Mario Puerto	15	0.21
Irene Landez	15	0.21
Fanny Prado	15	0.21
DELL	15	0.21
Bodega	15	0.21
LUPITA	14	0.2
ING. JULIO LOPEZ	14	0.2
Fondo Social	14	0.2
Raul	13	0.18
Morfologia	13	0.18
Margarita Baltodano	13	0.18
Kadmin	13	0.18
Contabilidad POLISAL	13	0.18

Nombre de cuentas	Intentos	Porcentaje
Amparito Rosales	13	0.18
Posgrado	10	0.14
Medicina	10	0.14
Maestria en Enfermer	10	0.14
Lic. Rosario Gutierr	10	0.14
Karla Solis	10	0.14
Investigacion	10	0.14
Humanidades	10	0.14
Haydee Vallejos	10	0.14
Gabi Gaitan	10	0.14
Fisioterapia	10	0.14
Editorial UNAN	10	0.14
Admin	10	0.14
Admin	9	0.13
Sergio Zamora	9	0.13
Reduc	9	0.13
Karla Aburto	9	0.13
Bibli011	9	0.13
ANATOMIA	9	0.13
w7	8	0.11
unanKadmin	8	0.11
Rectoría	8	0.11
Maestro	8	0.11
Abc	8	0.11
Vice Dec. Clinica	8	0.11
Valindacise	8	0.11
Unan Derecho	8	0.11
Semiologia	8	0.11
Prof. Elena Davila	8	0.11
OPD	8	0.11
Martha SÃ¡nchez	8	0.11
MSSR-MEDIOS	8	0.11
LIGIANA	8	0.11
HP	8	0.11
Gonzalez	8	0.11

Nombre de cuentas	Intentos	Porcentaje
Gerardo Aleman	8	0.11
Eduardo Picado	8	0.11
Dimas Delgado	8	0.11
Carlos	8	0.11
Bio A Clinico	8	0.11
123	8	0.11
Pedroza	7	0.1
Joseph Brown	7	0.1
Ecuevas	6	0.08
Akdmin	6	0.08
Dra. Reyna Martinez	6	0.08
Â¡Prohibido Ingresar!	5	0.07
Humanidades	5	0.07
franklin1981@hotmail.es	5	0.07
Cedoc	5	0.07
Anajancy	5	0.07
Xiomara Picado	5	0.07
Victor	5	0.07
VISITANTE	5	0.07
User	5	0.07
Telesalud	5	0.07
Rolando Ramirez	5	0.07
Referencia	5	0.07
Practicas Med	5	0.07
PediatrÃa	5	0.07
Pc	5	0.07
Patricia Davila	5	0.07
PREVENTIVA	5	0.07
Noel Rojas	5	0.07
Msc. Elmer Cisneros	5	0.07
Marvy	5	0.07
Marta B	5	0.07
Maria Esperanza	5	0.07
MARITZA	5	0.07
Interbibli6	5	0.07
Ing. Cuadra	5	0.07
HEWLETT	5	0.07
Gloria Argentina	5	0.07

Nombre de cuentas	Intentos	Porcentaje
Freddy Quezada	5	0.07
Erminia Alvarez	5	0.07
Elieth	5	0.07
Docentes	5	0.07
Docente	5	0.07
DivulgaciÃ³n	5	0.07
Divulgacion	5	0.07
DTN	5	0.07
Carol	5	0.07
Biblio04	5	0.07
Bethsabe Castillo	5	0.07
Auditoria	5	0.07
Amanda Collado	5	0.07
Aleyda	5	0.07
AGUSTIN	5	0.07
ADQUISICIONES	5	0.07
David	4	0.06
Rosario Gutierrez	4	0.06
Leonor	4	0.06
Johana	4	0.06
Ing. Lesther Brown	4	0.06
Enfermeria	4	0.06
Dr. Sequeira	4	0.06
Derecho	4	0.06
Darling	4	0.06
Danilo Tijerino	4	0.06
Adolfo	4	0.06
ARQUITECTURA	4	0.06
Unan	3	0.04
Kadm	3	0.04
Ramiro Sandino	3	0.04
Nutricion-POLISAL1	3	0.04
Sergio	2	0.03
kadminKa010203	2	0.03
Ka	1	0.01
ATD	1	0.01
TOTAL	7114	

ANEXO 5

Reporte de nombre de estación de trabajo que no lograron iniciar sesión (Evento 4625)

Nombre de Equipo	Intentos	Porcentaje
CONTIMPRENTA	245	6.887827
AVS	170	4.779308
PORTATIL6	89	2.502109
DIRECTORRH	86	2.417768
USODOCANESREAPO	67	1.88361
ANGELA	64	1.799269
ENRIQUEMIDIMPRE	60	1.686815
ANALISTA11	55	1.546247
VALINDACISE	54	1.518133
INTERBIBLIO05	51	1.433793
SECTESORERIA	45	1.265111
Equipo01	42	1.18077
DIRMORFOMED	42	1.18077
ARLEN	40	1.124543
VDECMED	39	1.09643
FISIOTERAPIA1	39	1.09643
TECHIGIESEGRRH	35	0.983975
HISTORIA5	35	0.983975
SECFILO	33	0.927748
DIR1POLI	33	0.927748
OPD2	32	0.899635
MARCIA	32	0.899635
DOCENFMAT1POLI	31	0.871521
ANALISTA5	30	0.843407
LAPTOP-EDISON	28	0.78718
INTERBIBLIO01	27	0.759067
MEDICINA-PC	25	0.702839
FISIOTER3POLI	25	0.702839

Nombre de Equipo	Intentos	Porcentaje
DIRREGACA	25	0.702839
VIDAE	24	0.674726
ARQUIT2	24	0.674726
ANALISTA12	24	0.674726
VIDAE3	23	0.646612
POLIREGACA2	22	0.618499
COORDINGCIV2	22	0.618499
CISEPROF1	22	0.618499
DOCENFSAL1POLI	21	0.590385
DIRDANZACOMT	21	0.590385
TECRRH	20	0.562272
MIRIAMLAPTOPGE	20	0.562272
CULTURAPROF	20	0.562272
LEONORDOCENFPOL	19	0.534158
DIRANTROPOLOGIA	19	0.534158
SECOFICPREPFIN	18	0.506044
CCOMP3MSR	18	0.506044
ANALISTA1	18	0.506044
MAYALEOPOLI	17	0.477931
SECRETARIAACAD1	16	0.449817
MIRIAMCTESORFIN	16	0.449817
INVENTFIN	16	0.449817
DIRDIRACA	16	0.449817
DIRDEPORTE	16	0.449817
BIOANALISIS	16	0.449817
ANALISTA13	16	0.449817
ADMON2POLI	16	0.449817
dirbecas	15	0.421704

Nombre de Equipo	Intentos	Porcentaje
SCARLETH	15	0.421704
INVENTARIO1	15	0.421704
BIOANAL4POLI	15	0.421704
MAESCDOCENFPO	14	0.39359
JULIOLPINGIND	14	0.39359
JORGEHHIS	14	0.39359
FONDOSOC	14	0.39359
ESPEDUBECAS	14	0.39359
TECRECLABRRH	13	0.365477
RESPROYECTOS	13	0.365477
ANALISTA9	13	0.365477
ANALISTA2	13	0.365477
AMPARITOROSALES	13	0.365477
PLANTAFISICA2	12	0.337363
MATERNO_INFANTI	12	0.337363
CORGMORFOMED	12	0.337363
UNAN-6E8F018AA9	11	0.309249
RESPCDOCMED	11	0.309249
PRESUPUESTO	11	0.309249
MARTALOPCPOLI	11	0.309249
XOLO2	10	0.281136
UNAN-379773CD91	10	0.281136
UNA-E35397406C4	10	0.281136
SECRH	10	0.281136
SECNUTRIPOLI	10	0.281136
MARTHAIMPRENTA	10	0.281136
MAESTRIA32	10	0.281136
INTERBIBLIO06	10	0.281136
HP28561136172	10	0.281136
ENFPACRIT2POLI	10	0.281136
EDUARDOPGE	10	0.281136
DIRINVES4	10	0.281136
DIRFINANZAS	10	0.281136
DIRACA	10	0.281136
DIMASANTGE	10	0.281136

Nombre de Equipo	Intentos	Porcentaje
CDOC4MED	10	0.281136
ASISADMINMSR	10	0.281136
ANALISTA4	10	0.281136
ANABELFH	10	0.281136
AGUSTINRTMED	10	0.281136
XXXXX	9	0.253022
VICEDECCLINICA1	9	0.253022
REINPROFDER	9	0.253022
REDUC4	9	0.253022
NORMA-MARTHA1	9	0.253022
LUPITA1	9	0.253022
INTERBIBLIO11	9	0.253022
ENFERMIPS	9	0.253022
DANILOTREGACA	9	0.253022
COMPU2PSICO	9	0.253022
BIOANALPOLI	9	0.253022
ANATOMIA-PC	9	0.253022
plantafisica1	8	0.224909
VALINDACISE-PC	8	0.224909
UNENEDU	8	0.224909
TECOBELE	8	0.224909
SIPDES-ATD	8	0.224909
SECCOMEDOR	8	0.224909
RECTORIA1	8	0.224909
RAUL-PC	8	0.224909
PSICOLOGIA1	8	0.224909
OPD5	8	0.224909
MSSR-MEDIOS-PC	8	0.224909
MEDPREV	8	0.224909
MAESTRO-PC	8	0.224909
MAASUNCIONMORA1	8	0.224909
LIGIAMHIS	8	0.224909
HISTORIA1	8	0.224909
ELENADAVPHIS	8	0.224909
EDUARDOPICADO	8	0.224909

Nombre de Equipo	Intentos	Porcentaje
DIRDER	8	0.224909
CONTABPOLI	8	0.224909
CCOMP4MSR	8	0.224909
BODEGA1	8	0.224909
AUDITMAGCONF2	8	0.224909
ATD-CONTAB	8	0.224909
ASTRALIADER	8	0.224909
ANESREARACAPOLI	8	0.224909
ADS1-2	8	0.224909
ADMINIPS	8	0.224909
ABC-PC	8	0.224909
123-PC	8	0.224909
PEDROZA	7	0.196795
MEDPREV4	7	0.196795
MARIO	7	0.196795
LESTHER	7	0.196795
CCOMP5MSR	7	0.196795
BODEGA	7	0.196795
ATD2	7	0.196795
HUMANIDADES	6	0.168681
CDOC11MED	6	0.168681
asistbecas	5	0.140568
VICTORREYES	5	0.140568
VICE-DECANA	5	0.140568
VDECACLINMED	5	0.140568
USER	5	0.140568
UNENMED	5	0.140568
UNENCIEN	5	0.140568
UNAN-FD8042CF3F	5	0.140568
UNAN-D0FB1E5E18	5	0.140568
UNAN-AD2656215F	5	0.140568
UNAN-7BA2FFED59	5	0.140568
UNAN-60165C8A01	5	0.140568
UNAN	5	0.140568
UDOCBIOACPOLI	5	0.140568

Nombre de Equipo	Intentos	Porcentaje
UDOC2BIOACPOLI	5	0.140568
SUBDIRDOCPOLI	5	0.140568
SOCALVGE	5	0.140568
SERGIO	5	0.140568
SEMIOMED	5	0.140568
SECRETARIA	5	0.140568
SECCONTAB	5	0.140568
SECAUD	5	0.140568
SECATD	5	0.140568
SANDRARENFPOLI	5	0.140568
SALAMEDHIS	5	0.140568
ROSAAGFISIOPOLI	5	0.140568
RESPROYECTO	5	0.140568
RESPCLINMSR	5	0.140568
RENEIGPSICO	5	0.140568
RECTORIA2010	5	0.140568
PROFISIOIPS	5	0.140568
PLANTAFISICA1	5	0.140568
PERSONAL-BA3C28	5	0.140568
PEDIATRIA01	5	0.140568
ORIENTACION	5	0.140568
NORGMEDPREV	5	0.140568
NOEL	5	0.140568
MEDPRE	5	0.140568
MCARMENDAVFH	5	0.140568
MARVY-PC	5	0.140568
MARITZA	5	0.140568
MARINITA	5	0.140568
MAESTRIA26	5	0.140568
MAESTENFPOLI	5	0.140568
LUZSECDECAFH	5	0.140568
LESSAGE	5	0.140568
KABURTOTRRHH	5	0.140568
JUANAESTADFACH	5	0.140568
IVANCFILO	5	0.140568

Nombre de Equipo	Intentos	Porcentaje
INTERBIBLIO09	5	0.140568
INTERBIBLIO07	5	0.140568
INTERBIBLIO04	5	0.140568
HP32694348505	5	0.140568
HEMEROTECA	5	0.140568
GLADJDESMED	5	0.140568
FREDQFILOLO	5	0.140568
FISIOLAB1	5	0.140568
ESPRECLAB	5	0.140568
EQUIPO03MSSR	5	0.140568
ENFSALPUB1POLI	5	0.140568
ENF-SANREYES	5	0.140568
DOCENCIA1MED	5	0.140568
DIVULGA2	5	0.140568
DIVULGA	5	0.140568
DIRFISIO	5	0.140568
DIRECCION1	5	0.140568
DESKTOP	5	0.140568
D1T5YML1	5	0.140568
CULTURADIR	5	0.140568
CULTURA	5	0.140568
CORELAB6	5	0.140568
CORELAB22	5	0.140568
CORELAB20	5	0.140568
COORESTMEDKAR	5	0.140568
COORDARQFARACH	5	0.140568
COORD	5	0.140568
CONTADOR	5	0.140568
COLOSSUS	5	0.140568
CISEPROF2	5	0.140568
CISE	5	0.140568
CIENBASMED	5	0.140568
CDOC3MED	5	0.140568
CCOMP8MSR	5	0.140568
CCOMP7MSR	5	0.140568
CAROLINA	5	0.140568
CAJA2TESORERIA	5	0.140568

Nombre de Equipo	Intentos	Porcentaje
BIOANAL2POLI	5	0.140568
BERTAGE	5	0.140568
AULAMAGMED	5	0.140568
AUDITMAGCONFIG1	5	0.140568
ATM3	5	0.140568
ATD-1	5	0.140568
ASISTEDITREC	5	0.140568
ARQDIRSAFACH	5	0.140568
ANALISTA8	5	0.140568
ANALISTA3	5	0.140568
AMPBRENGE	5	0.140568
AMANDANOMINA	5	0.140568
ALIMENTPOLISAL	5	0.140568
ADMONSEC	5	0.140568
ADMONMED2	5	0.140568
UNENRECINTO3	4	0.112454
SECSDIRDOCIPS	4	0.112454
SECRELINT	4	0.112454
SALAPROF1DER	4	0.112454
PROFBIOAPOLI	4	0.112454
LAPTOPDIRACA	4	0.112454
LAPTOPADMONMED	4	0.112454
IVANMARIN2	4	0.112454
IVANMARIN	4	0.112454
EXTCULTURAL	4	0.112454
ENFTELESA12POLI	4	0.112454
DRSEQUEIRA-PC	4	0.112454
DOCENFPOLIAURA	4	0.112454
DIRIPS	4	0.112454
DIRACA2	4	0.112454
DARSECSACADFH	4	0.112454
COORDINGIND2	4	0.112454
ADMINMED1	4	0.112454
SERGIOZFINLAPTO	3	0.084341
RAMIRO	3	0.084341
LAPTOP	3	0.084341
DEPTONUTRIPOLI	3	0.084341

ANEXO 6

INFORME DE HALLAZGO

A solicitud del **Proyecto de Tecnología de Comunicación e Información**, se ha procedido a levantar un proceso de análisis e investigación del servidor kaspersky con el objetivo de determinar posibles intentos de conexión y uso de recursos no autorizados, así como también modificación, y eliminación de información.

Nombre del equipo:AVS

Sistema Operativo: Windows Server 2008 R2

Funcionalidad: Servidor de Kaspersky Administration Kit

Fecha y hora de inicio: 18 de abril de 2010

Institución: Oficinas **del Proyecto TIC, UNAN – Managua, Pabellón -14**

Descripción del Incidente: El servidor presenta lentitud en el servicio, y se apaga constantemente debido al crecimiento en los logs, la consola del antivirus pierde conexión a la red, no hay una buena sincronización entre los equipos que están registrados en la consola, debido a que el DNS tiene problemas con la resolución de nombre y debido a esto el estado de los equipos físicamente, no es el que se refleja en la consola.

Metodología de investigación: El proceso de investigación se llevo a cabo de acuerdo a la siguiente metodología que se plantea a continuación:

1. **Recolección de datos:** Para obtener información del caso se realizó entrevistas al personal de informática del Proyecto de Tecnología de Comunicación e Información**(TIC)**:

   En base a las entrevistas realizas se determinó que el servidor de kaspersky presenta las siguientes debilidades en cuanto a seguridad:

   1. No presenta un plan de configuración de auditorías de seguridad, que permita controlar a mayor escala los registros de eventualidades ocurridos en el servidor por usuarios no autorizados. Actualmente el servidor dispone únicamente de las auditorias que por default habilita el sistema operativo al momento de su instalación.

   2. No dispone de un Sistema de Detección de Intrusos (IDS)

   3. No se tiene control (dominio) de las cuentas de usuario, ya que no todos los usuarios están bajo el dominio del Active Directory, por tal razón los equipos no están siendo actualizados correctamente por la consola de administración de Kaspersky Anti Virus, dando lugar a posibles infecciones en los equipos clientes, lo cual puede aumentar el intento de acceso no autorizado.

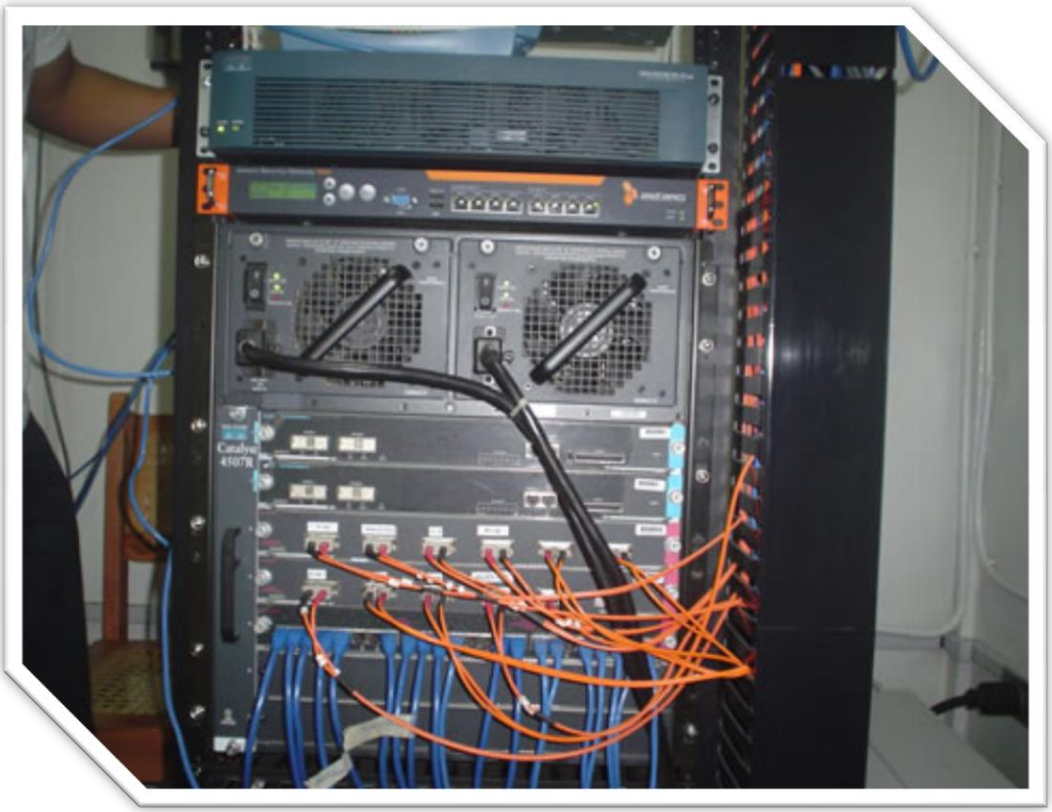
   4. Los logs del Antivirus están siendo almacenados en la unidad de disco donde se encuentra instalado el sistema operativo.

   5. La red local no dispone de políticas de seguridad que ayuden a disminuir el riesgo de la información digital.

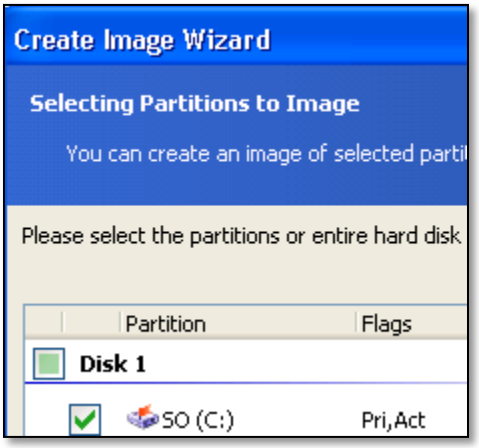
2. **Resguardo de la escena:** Se verificaron los grupos y cuentas de usuarios existentes en el servidor de Kaspersky, para descartar que otro usuario que no fuese empleado del Proyecto TIC tuviese acceso al servidor mientras se hace el proceso de investigación, ya que de acuerdo a la funcionalidad del servidor no se puede realizar confiscación de equipo, ni desconectar por completo ya que se estaría afectando la seguridad de la red.

   Fecha de resguardo: 18 de abril de 2011
   Hora: 08:15 a.m.

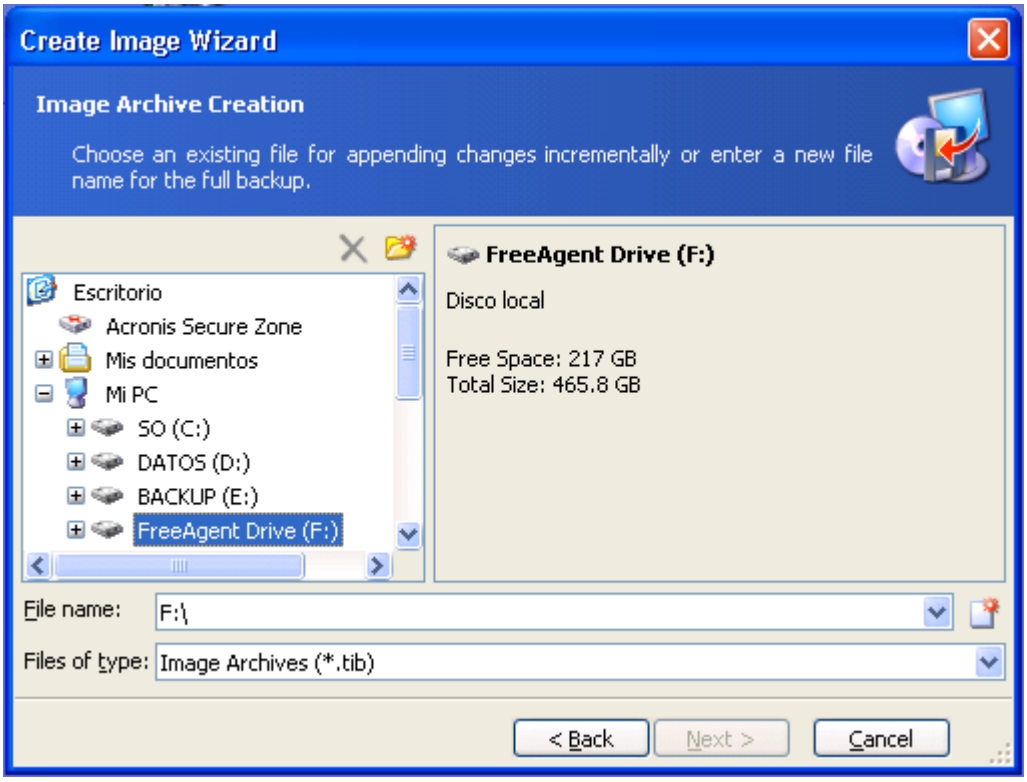
   Fotografías del servidor



3. **Capturar la escena:** Se procedió a realizar la captura de información mediante la herramienta **ACRONIS TRUE IMAGE SERVER V.8.0.**, la cual permite obtener una imagen exacta de la información **(Partición Disk1 - Disco Local C:)**



La imagen fue extraída en un disco externo de **500 GB** de almacenamiento (marca Seagate).



4. **Custodia:** Se encripto la imagen realizada con la herramienta ACRONIS TRUE IMAGE SERVER V.8.0. con el propósito de asegurar la confidencialidad de la información en caso de extravío.

Información de custodia

Ubicación del equipo:	**Oficinas del Proyecto TIC – Pabellón 14 (UNAN – Managua, RURD)**		
Encargado de custodia	Zabdiel José Zepeda Vega		
Identificación:	XXX-XXXXXX-XXXXX		
Ocupación:	Estudiante de computación		
Fecha de inicio custodia:	18 de abril, 2011	**Hora:**	11:08:55 a.m.
Tiempo de custodia:	12 días		
Fecha finaliza custodia:	30 de Abril, 2011	**Hora:**	03:05:00 p.m.
Tipo de Almacenamiento:	En disco externo		

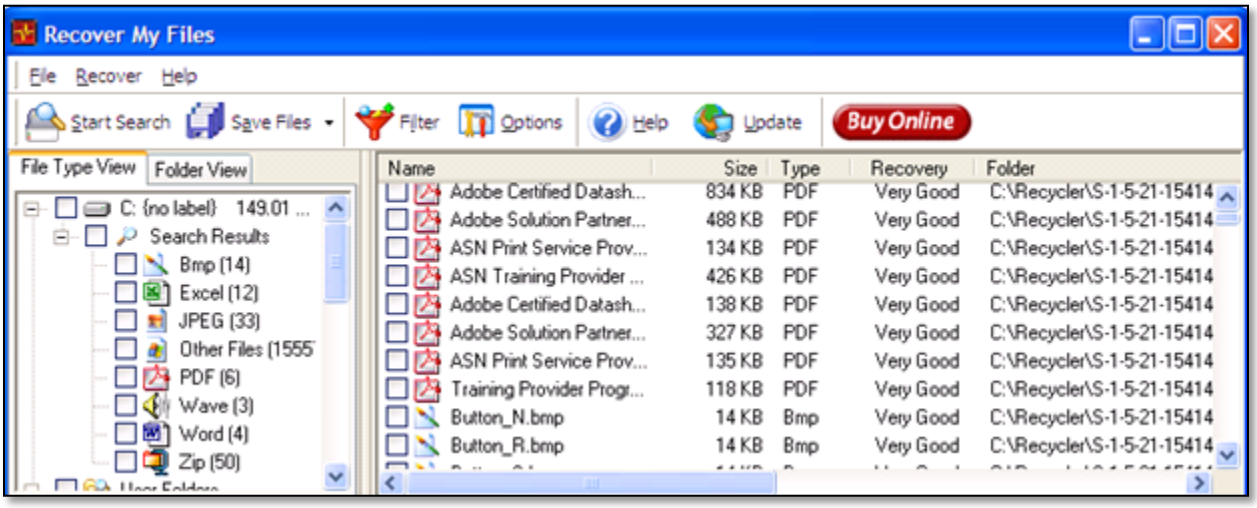
5. **Análisis de información:** Para el análisis de la investigación realizada fue necesario instalar **ACRONIS TRUE IMAGE SERVER V.8.0.**en una laptop **Sony Vaio** con sistema Operativo **Windows 7** y anti virus **Kaspersky v.6.0.** la cual será asignada para el análisis de evidencias de la información respaldada.

Para la búsqueda de evidencias registradas en el servidor se ejecutaron las siguientes acciones:

Búsqueda de archivos eliminados: Se escaneó la imagen realizada con la herramienta **GetData Recover My Files,** permitiendo hacer una búsqueda completa de archivos borrados. No se encontró información sospechosa que sirva como evidencia de un posible delito cometido en el servidor o realizado a través del servidor como puente de conexión hacia otro destino de interés para usuarios no autorizados.

El escaneo realizado por Recover My Files permitió recuperar e identificar 1,677 archivos borrados, entre ellos los siguientes tipos de datos:

Tipo Archivos	Encontrados
*.pdf (Acrobat PDF)	6
*.doc (Word)	4
*.xls (Excel)	12
*.txt	15
*.bmp (imagen)	14
*.jpeg (imagen)	33
*.zip (compreso)	50
Otros	1555

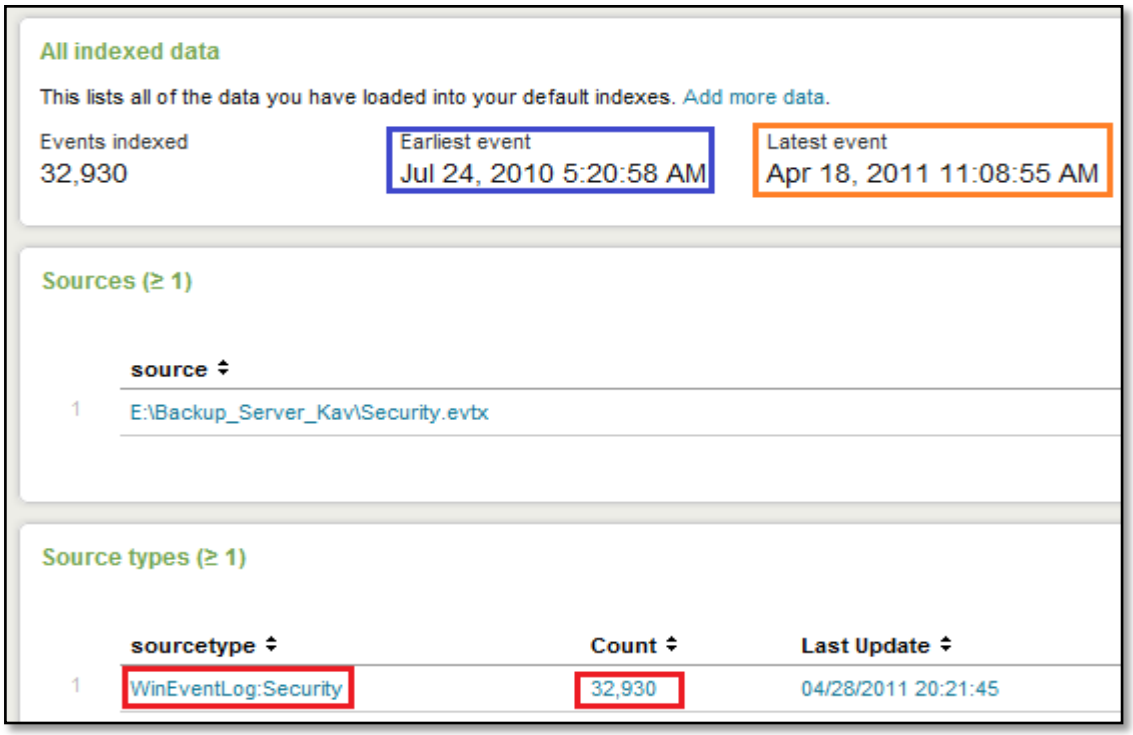


Los archivos recuperados deberán ser revisados por los administradores de servidores del Proyecto TIC en supervisión del jefe inmediato o delegado, quienes establecerán parámetros para determinar si la información recuperada hace referencia a las funciones realizadas por ellos mismos en el servidor y si existe justificación del porque fue eliminada.

Análisis de Registros generados por el Servidor: Estos registros son generados como efecto de la programación del servidor, y son inalterables por una persona, los mismo son llamados registros de eventos de seguridad (Logs)

La revisión del Logs de seguridad del servidor fue realizada con la aplicación **Splunk**, servicio en línea que permite buscar, alertar e informar sobre datos online, o datos históricos de Tecnología de la información.

El archivo log de seguridad analizado contiene información de eventos registrados en el servidor kaspersky del Proyecto TIC desde el 24 de julio de 2010 a las 05:20:58 a.m. hasta el 18 de Abril de 2011 a las 11:08:55 a.m. en el cual se identificaron 23 eventos con diferentes acciones, entre ellos se analizaron los más importantes.



Detalle de eventos ocurridos en el servidor:

Código de evento	Frecuencia	Porcentaje	Descripción
4624	10028	30,45 %	Una cuenta ha iniciado sesión correctamente.
4672	7922	24,06 %	Privilegios especiales asignados al nuevo inicio de sesión
4634	7293	22,15 %	Una cuenta ha cerrado la sesión
4625	3557	10,8 %	Una cuenta no pudo iniciar sesión
4648	1947	5,91 %	Se ha intentado un inicio de sesión mediante credenciales explícitas
4907	346	1,05 %	Se han cambiado la configuración de auditoría en objeto
5038	334	1,01 %	Integridad de código determinó que el hash de imagen de un archivo no es válido. El archivo podría estar dañado debido a modificación no autorizada o no es válido el valor de hash podría indicar un posible error de dispositivo de disco
4616	297	0,9 %	Se cambió la hora del sistema
5061	228	0,69 %	Operación criptográfica
5058	228	0,69 %	Operación de archivo de clave
5033	129	0,39 %	El controlador de Firewall de Windows se ha iniciado correctamente
5024	129	0,39 %	El servicio Firewall de Windows se ha iniciado correctamente
4902	129	0,39 %	Se creó la tabla de directivas de auditoría por usuario
4608	129	0,39 %	Windows se está iniciando
4647	93	0,28 %	Cierre de sesión del usuario iniciado
1101	88	0,27 %	Los sucesos de auditoría se han caído por el transporte
1100	40	0,12 %	El servicio de registro de eventos se ha apagado

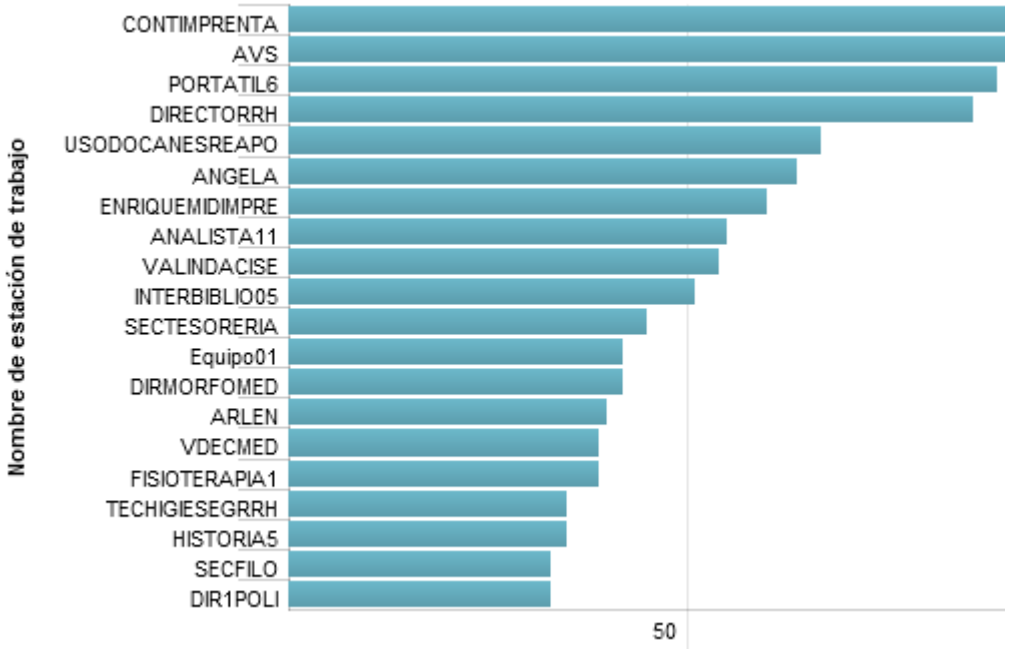
Código de evento	Frecuencia	Porcentaje	Descripción
4776	4	0,01 %	El controlador de dominio intentaba validar las credenciales para una cuenta
4732	3	0,01 %	Se agregó un miembro a una seguridad habilitada grupo local
4739	2	0,01 %	Se cambió la directiva de dominio
4733	2	0,01 %	Se ha quitado un miembro de un grupo local con seguridad habilitada
4738	1	0 %	Se ha modificado una cuenta de usuario
4724	1	0 %	Se intentó restablecer la contraseña de una cuenta

Evento 4625 –"Una cuenta no pudo iniciar sesión" porque el **usuario es desconocido o la contraseña es incorrecta:** El evento retorno 123 nombre de cuentas utilizadas.

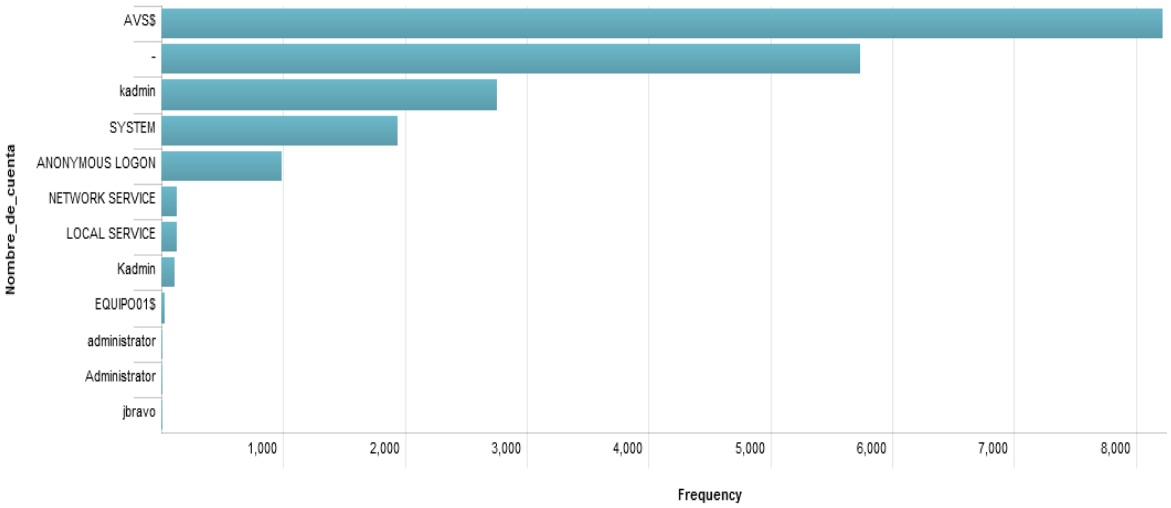
Cuentas de usuarios que presentaron intentos fallidos elevados

Nombre_de_cuenta	Intentos	percentaje
- (Administrador)	3389	47.64 %
Administrador	604	8.49 %
William Barberena	245	3.44 %
Kadmin	169	2.38 %
AVS$	168	2.36 %
Angelical	104	1.46 %
Usuario Lapto	89	1.25 %
Abel MembreÃ±o	82	1.15 %
Martha	74	1.04 %
Marcia	65	0.91%

Gráfica de los equipos que intentaron conectarse y generaron el evento 4625



Evento4624–"Una cuenta ha iniciado sesión correctamente"



El evento 4624 muestra la siguiente información:

Campos de red, indican dónde se originó una solicitud de inicio de sesión remota (información del equipo que realizo algún tipo de conexión en algunos casos podría ser el atacante), no siempre es posible disponer del nombre del usuario y dirección IP.

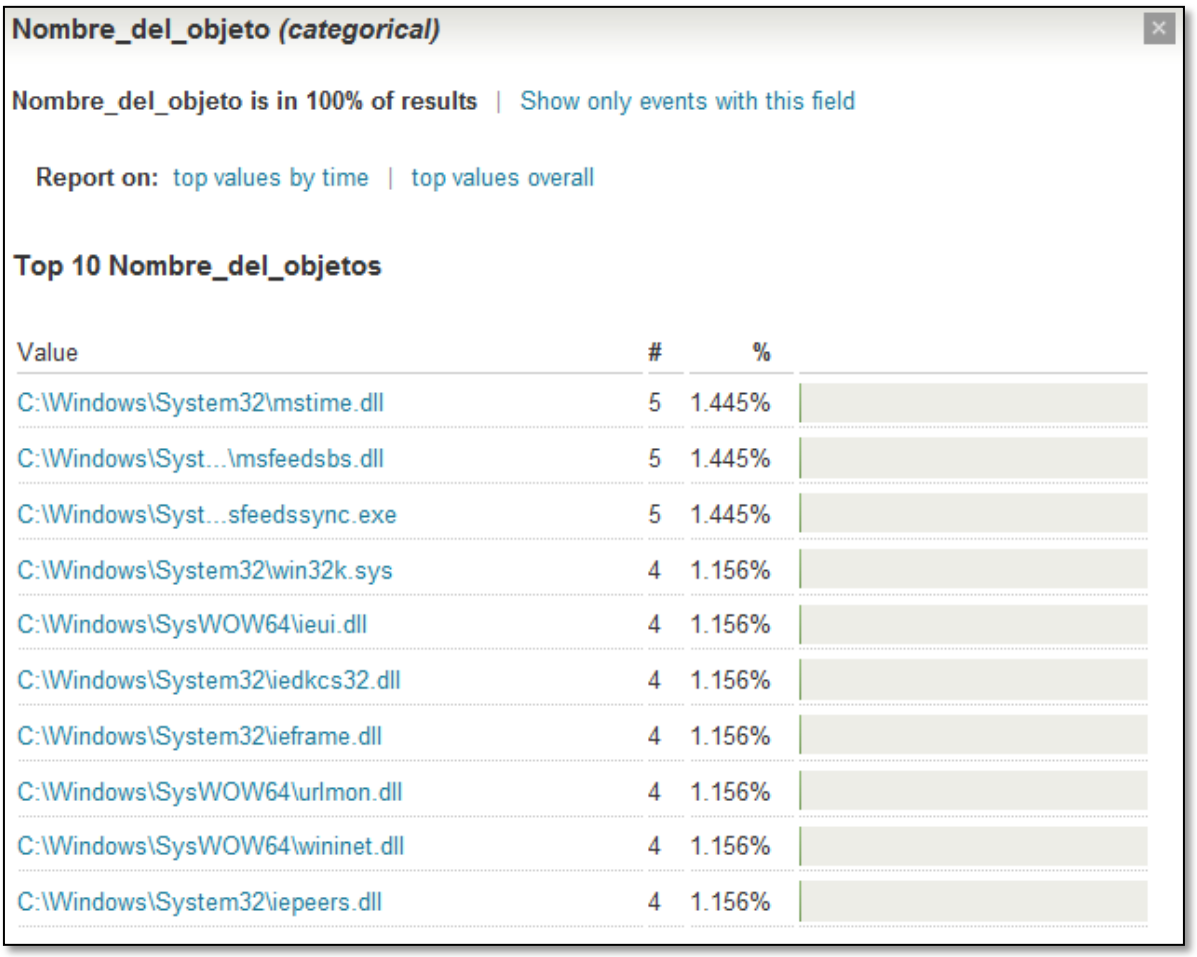
```
Información de red:
Nombre de estación de trabajo: AVS
Dirección de red de origen: 10.1.120.30
Puerto de origen: 59022

Información de autenticación detallada:
Proceso de inicio de sesión: User32
Paquete de autenticación: Negotiate
Servicios transitados: -
Nombre de paquete (sólo NTLM): -
Longitud de clave: 0
```

Se logro detectar que la mayor frecuencia de conexión realizada hacia el servidor fue mediante el tipo de inicio 3, este tipo de inicio se refiere a conexiones a carpetas compartidas en el servidor de Kaspersky, en este caso se logro detectar que la carpeta compartida a la que se está accediendo es la **carpeta de actualización de bases de datos del antivirus**. La otra forma de conexión utilizada al servidor fue el tipo de conexión 5 por conexión remota o terminal services.

Evento 4907 –"Se ha cambiado la configuración de auditoría en objeto"

En el analisis del **evento 4907** se detectaron 346 registros por cambio en la configuración de auditoría de 184 objetos ubicados en 2 carpetas con auditorias de seguridad, **archivos de programas (Internet explorer, Windows mail, Worpad.exe) y en la carpeta Windows y System32 del sistema operativo, (librerías dll)**



Nombre_del_objeto *(categorical)*

Nombre_del_objeto is in 100% of results | Show only events with this field

Report on: top values by time | top values overall

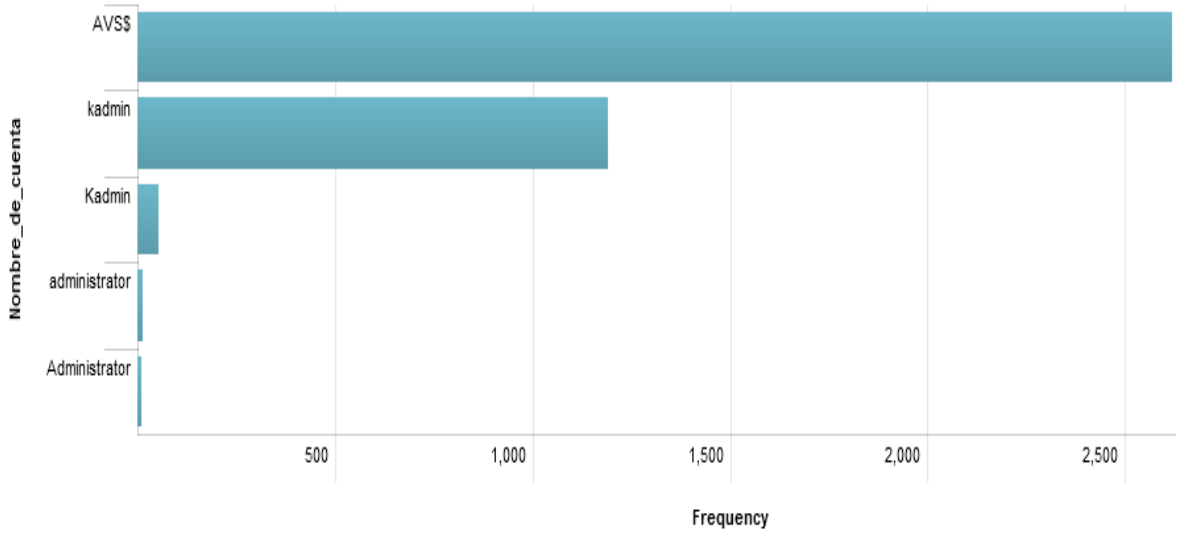
Top 10 Nombre_del_objetos

Value	#	%
C:\Windows\System32\mstime.dll	5	1.445%
C:\Windows\Syst...\msfeedsbs.dll	5	1.445%
C:\Windows\Syst...sfeedssync.exe	5	1.445%
C:\Windows\System32\win32k.sys	4	1.156%
C:\Windows\SysWOW64\ieui.dll	4	1.156%
C:\Windows\System32\iedkcs32.dll	4	1.156%
C:\Windows\System32\ieframe.dll	4	1.156%
C:\Windows\SysWOW64\urlmon.dll	4	1.156%
C:\Windows\SysWOW64\wininet.dll	4	1.156%
C:\Windows\System32\iepeers.dll	4	1.156%

Evento 4648 –"Se ha intentado un inicio de sesión mediante credenciales explícitas"

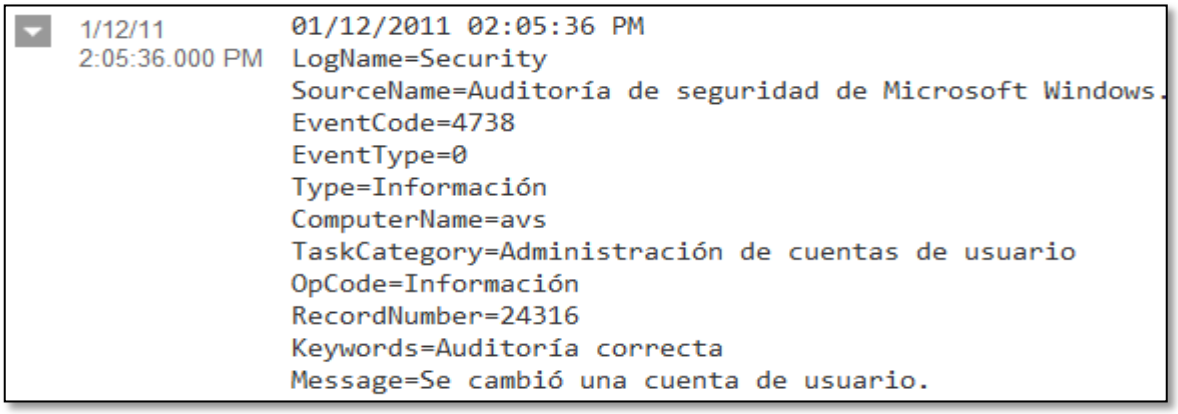
Este evento se genera cuando un proceso intenta iniciar sesión en una cuenta especificando explícitamente las credenciales de la cuenta. Suele producirse en configuraciones de tipo de lote como tareas programadas, o cuando se usa el comando RUNAS (Opción click derecho sobre el ejecutable y luego se selecciona la opción ejecutar como).

Gráfica de cuentas que generaron el evento 4648



Evento 4738 –"Se ha modificado una cuenta de usuario

De este evento se encontró un único cambio de cuenta de usuario, el cual no representa ninguna anomalía.



```
Atributos cambiados:
Nombre de cuenta SAM: Administrator
Nombre para mostrar: <valor no establecido>
Nombre principal de usuario: -
Directorio principal: <valor no establecido>
Unidad principal: <valor no establecido>
Ruta de acceso de script: <valor no establecido>
Ruta de acceso de perfil: <valor no establecido>
Estaciones de trabajo de usuario: <valor no establecido>
Última contraseña establecida: 1/12/2011 2:05:36 PM
Expiración de cuenta: <nunca>
Id. de grupo primario: 513
Se permite delegación a: -
Valor de UAC anterior: 0x10
Nuevo valor de UAC: 0x10
Control de cuentas de usuario: -
Parámetros de usuario: -
Historial de SID: -
Horas de inicio de sesión: Todo
```

En el análisis de logs realizado no se logro determinar ningún delito informático realizado en el servidor de Kaspersky, sin embargo se recomienda al personal de seguridad del Proyecto TIC realizar lo siguiente para reforzar la seguridad en dicho servidor:

1- Hacer una revisión en la configuración del agente de Kaspersky anti virus, para solventar el problema de actualización de las bases de datos del anti virus en los equipos clientes, ya que esto es lo que provoca se registre gran cantidad de conexión hacia la carpeta compartida de actualización.
2- Instalar actualizaciones y parches de seguridad de Microsoft Windows Server 2008 R2
3- Habilitar auditorias de seguridad (Localmente).
4- Revisar periódicamente los logs del servidor kaspersky.
5- Limitar el grupo de administrador **KLADMINS** a los usuarios que requieran el privilegio de administración del servidor.
6- Configurar alertas **(en los eventos)** que se consideren importantes **(críticos)** para que puedan ser almacenados y visualizados desde el visor de sucesos.

7- Crear configuración de seguridad personalizadas según la necesidad de los grupos de trabajo de la institución.

8- Configurar el envío de alertas por correo electrónico a los eventos críticos que se describen a continuación:

- Detección de objetos infectados
- Detección de ataques de red

9- Configurar contraseñas seguras para evitar modificaciones en la aplicación de anti virus por parte de los usuarios finales.

10- Crear proceso de revisión de reportes de protección de anti virus con el objetivo de detectar, corregir y prevenir infecciones por virus en la institución.