



# INFRAESTRUCTURA PARA LA GESTIÓN DE LA EVIDENCIA DIGITAL EN REDES INALÁMBRICAS

---

**Pontificia Universidad Javeriana**  
Carrera de Ingeniería de Sistemas  
Bogotá, Colombia  
2007

# INFRAESTRUCTURA PARA LA GESTIÓN DE LA EVIDENCIA DIGITAL EN REDES INALÁMBRICAS

Juan David Gutiérrez Sánchez

Giovanni Zuccardi Hernández

[juan.dvd@gmail.com](mailto:juan.dvd@gmail.com)

[gzuccardi@gmail.com](mailto:gzuccardi@gmail.com)

Mayo 24 de 2007

## Resumen

El siguiente artículo presenta un proyecto el cual consiste en proponer una infraestructura para la producción de evidencia digital teniendo en cuenta el diseño para fortalecer la admisibilidad y relevancia, es decir, aporta para que la información obtenida (evidencia digital) de la infraestructura planteada sea admisible, confiable, auténtica e íntegra, de tal forma que pueda servir de utilidad para esclarecer un futuro incidente informático.

Tomando “infraestructura”, como el conjunto de elementos, servicios, políticas que se consideran necesarios para la creación y funcionamiento de la producción de evidencia digital en redes inalámbricas, se debe tener en cuenta que el diseño de los registros electrónicos o evidencia digital y la producción de la misma están enfocados hacia la forensia en redes.

## Abstract

The following article present a project that consist in a infrastructure proposal for production of digital evidence having in mind the design in order to fortify the admissibility and relevance, that is, it contributes so that the obtained data (digital evidence) of the raised infrastructure is permissible, reliable, authentic and integral, of such form that can serve as utility to clarify a future computer science incident.

Taking the meaning of “infrastructure”, as it combined of elements, services, policies that are necessary for the creation and operation of the production of digital

evidence in wireless networks, it must consider that the design of the electronic registries or digital evidence and the production of the evidence are focused towards networks forensics.

## Palabras clave:

Infraestructura, redes inalámbricas, evidencia digital, registros de eventos (logs), IEEE 802.11.

## 1. Introducción

La seguridad en las redes inalámbricas es un aspecto crítico que no se puede descuidar. Debido a que las transmisiones viajan por un medio abierto (el radio frecuencias, al cual tiene acceso cualquiera), se requieren mecanismos que aseguren la confidencialidad de los datos así como su integridad y autenticidad.

Los importantes avances en el campo de la conexión inalámbrica lleva a la pregunta sobre que tan preparados estamos para obtener la información necesaria como evidencia digital con un resultado que beneficie a todos los usuarios de esta tecnología, las autoridades, entre otros; teniendo en cuenta un aspecto fundamental como la seguridad, por esto el interés en el tema de seguridad informática de redes inalámbricas.

También hay que tener en cuenta que la evidencias digital es fácil de manipular ya que la evidencia digital posee la característica fundamental de ser frágil (volátil) y además se puede copiar fácilmente, lo cual permite robo de

información. Por ello este tipo de evidencias pierde credibilidad y es de vital importancia buscar un mecanismo que brinde la confianza y autenticidad necesaria para que dichas evidencias puedan ser llevadas a un tribunal y cumplan con un papel importante dentro de la investigación y procesamiento de los cibercriminales.

En las redes inalámbricas actualmente encontramos un problema al intentar administrar la evidencia digital; debido a que es difícil definir, producir, obtener y analizar la evidencia en una red inalámbrica. La imposibilidad de tener disponible el dispositivo desde el cual se realizó la conexión a la red inalámbrica y analizarlo, obliga a relacionar directamente este problema con lo que llamamos *network forensics* o forensia en redes, puesto que esta parte del tema forense, específica que la evidencia deben ser eventos de la red como tal.

El diseño y producción de los registros electrónicos es de vital importancia en la gestión de evidencia digital, de estos pasos depende que la evidencia digital exista de forma coherente y luego pueda ser recolectada y utilizada como prueba incriminatoria o registro valido.

## 2. Definiciones

### 2.1 Registros de eventos.

Un evento es un suceso o cambio de estado que puede ocurrir en un sistema o red. Un registro de eventos, es un repositorio de eventos almacenados. [Casey04]

De ésta manera se tiene que la función principal de un registro de eventos es proporcionar información a los administradores a cerca de los cambios sucedidos en los sistemas. Es aquí donde se ve la importancia de monitorear y revisar los registros de eventos continuamente. Siendo así, si un evento es atendido oportunamente, se pueden corregir errores en el funcionamiento de los sistemas así como tomar acciones frente a un incidente de seguridad.

## 2.2 Evidencia digital

Casey define la evidencia de digital como “cualquier dato que puede establecer que un crimen se ha ejecutado o puede proporcionar una enlace entre un crimen y su víctima o un crimen y su autor”. [Casey04]

Otra definición a tener en cuenta es “Cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático” [HBIT03] [Acis06]

La evidencia digital debe cumplir con 4 criterios de admisibilidad, los cuales son:

**Autenticidad:** Una evidencia digital será autentica siempre y cuando se pueda demostrar que dicha evidencia ha sido generada y registrada en el lugar de los hechos. También se debe mostrar que los medios originales no han sido modificados.

**Confiabilidad:** Se dice que los registros de eventos de seguridad son confiables si provienen de fuentes que son “creíbles y verificable” [AdmEvi03]. Una prueba digital es confiable si el “sistema que lo produjo no ha sido violado y estaba en correcto funcionamiento al momento de recibir, almacenar o generar la prueba” [EviDig05].

**Suficiencia o completitud de las pruebas:** Para cumplir con este criterio la prueba debe estar completa. Para asegurar esto es necesario “contar con mecanismos que proporcionen integridad, sincronización y centralización” [AdmEvi03] para lograr tener una vista completa de la situación.

**Apogeo y respeto por las leyes y reglas del poder judicial:** Este criterio se refiere a que la evidencia digital debe cumplir con los códigos de procedimientos y disposiciones legales del ordenamiento del país. Es decir, debe respetar y cumplir las normas legales vigentes en el sistema jurídico.

El ciclo de administración de la evidencia digital esta compuesto por:



Figura 1: Ciclo de vide de la administración de la evidencia digital. [BueAdm06]

Para este trabajo se contemplaran la fase 1 y 2 del ciclo, es decir, el diseño y la producción de evidencia digital. El diseño ayuda a fortalecer la admisibilidad y relevancia de la evidencia producida por las tecnologías de información. La producción ayuda a que el sistema o tecnología de información produzca los registros electrónicos, verificando la completitud de los registros generados.

Por ello la infraestructura debe cumplir con algunos de los siguientes requisitos:

Para el Diseño:

- Asegúrese de que se ha determinado la relevancia de los registros electrónicos, que éstos se han identificado, están disponibles y son utilizables.
- Los registros electrónicos tienen un autor claramente identificado.
- Los registros electrónicos cuentan con una fecha y hora de creación o alteración.
- Los registros electrónicos cuentan con elementos que permiten validar su autenticidad. (integridad (hash, firmas digitales,), autenticación (tiene, posee, es) y autorización (certificados digitales)).
- Se debe verificar la confiabilidad (nivel de calidad del servicio ofrecido teniendo en cuenta disponibilidad y seguridad (integridad y confidencialidad)) de la producción o generación de los registros electrónicos por parte del sistema de información.

Para la Producción:

- Que el sistema o tecnología de información produzca los registros electrónicos.
- Identificar el autor de los registros electrónicos almacenados.
- Identificar la fecha y hora de creación.
- Verificar que la aplicación está operando correctamente en el momento de la generación de los registros, bien sea en su creación o modificación.
- Verificar la completitud de los registros generados.

## 2.3 IEEE 802.11i

El estándar 802.11i introdujo varios cambios fundamentales, como la separación de la autenticación de usuario (802.1X/EAP) de la integridad y privacidad de los mensajes (AES-CCMP), proporcionando una arquitectura robusta y escalable, que sirve igualmente para las redes locales domésticas como para los grandes entornos de red corporativos. [SEGWF] Esta consta básicamente de 3 elementos: Estaciones (STA), Puntos de Acceso (AP) y Servidor de Autenticación (AS).

**AP:** Los puntos de acceso varían según el fabricante, sin embargo por lo general manejan los logs de actividad del sistema, información debug, ataques, paquetes perdidos y otras notificaciones.

**AS:** El servidor de autenticación permite el uso de métodos avanzados de autenticación y de cifrado. Los registros generados por éste serán más relevantes en cuanto a que los clientes han sido plenamente identificados.

**STA:** Las estaciones son los dispositivos inalámbricos utilizados por los usuarios. Estos no tendrán una gran influencia dentro del modelo planteado, ya que estas pueden no estar disponibles después de una intrusión y se convierte en un recurso con el cual no se puede contar. Sin embargo la infraestructura esta diseñada para autenticar los clientes y poder tener información de ellos.

## 2.4 Definición de la Infraestructura.

Para lograr una definición exitosa de la infraestructura se deberá tener en cuenta varios aspectos, los cuales serán enunciados a continuación.

Lo primero que se debe tener en cuenta es identificar los registros electrónicos, como esta infraestructura se centra en Network Forensics los logs son nuestra principal fuente de evidencia.

La administración de logs ayuda a que los registros de eventos tengan autenticidad, exactitud y suficiencia. La técnica de rotación de logs permite limitar el volumen de datos que se tienen disponibles, se basa principalmente en cambiar la ubicación de los logs y renombrarlos de esta manera podrá reflejar la rotación.

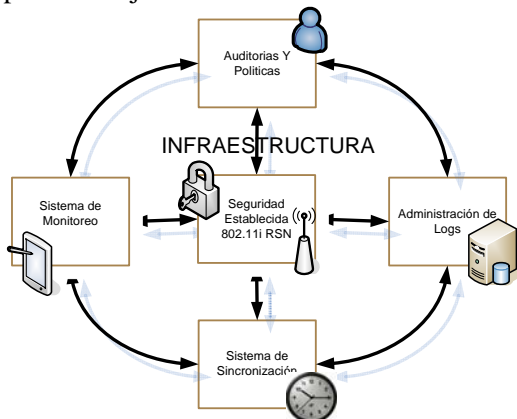


Figura 2: Infraestructura Planteada.

Para generar mayor exactitud y tener la posibilidad de correlacionar logs, los dispositivos que producen los logs deben manejar una alta exactitud en el tiempo, para ello se puede utilizar el servicio Network Time protocol (NTP).

Las auditorías de sistemas por su parte son muy buena práctica para controlar, analizar, verificar y revisar como se producen los registros y que tan relevantes o valiosos pueden llegar a ser.

El uso del estándar IEEE 802.11i, es un gran aporte a la infraestructura, ya que ayuda a mejorar la integridad, autenticación y confidencialidad de los datos

La implementación de un dispositivo o sistema de monitoreo para la captura de tráfico 802.11, genera información valiosa y que con el debido manejo puede ser de gran utilidad como evidencia digital.

Por ultimo, la utilización de mecanismos de cifrado y algoritmos de hashing como (MD5 y GPG) permite aumentar la integridad, confiabilidad y autenticidad de los registros electrónicos, incrementando la admisibilidad de estos como evidencia.

## 3. Resultados.

- En el sistema de monitoreo para los casos planteados fue posible la captura de paquetes con el software usado. Haciendo un análisis detallado de la captura se pudo identificar la presencia de un ataque como también los diferentes intercambios de mensajes necesarios para la asociación y autenticación.
- En el servidor se registraron los eventos generados por las pruebas y ataques realizados. Cada dispositivo y servicio generó correctamente su registro para luego centralizarlo y unificarlo obteniendo así una producción de logs acorde con lo planeado. Los registros generados tienen el formato establecido y diseñado en la configuración de syslog aportando a la unificación de estos y ayudando a la identificación del evento registrado.
- Se puede concluir que el uso de estándares de seguridad como 802.11i aumenta notablemente la seguridad de la red, haciéndola más robusta y generando registros de mayor calidad.
- La existencia de mas dispositivos generando registros ayuda a aumentar el peso de los registros obtenidos, ya la mayoría de las veces un evento queda registrado en mas de un archivo de registro y estos pueden ser correlacionados confirmando el suceso.
- Se pudo establecer que los registros no fueron modificados desde su producción hasta su centralización

garantizando su integridad, además luego del cifrado aumenta su disponibilidad y confiabilidad por lo que es posible decir que se aporta a la admisibilidad de los registros generados.

- Los registros de un evento generados por las partes del sistema se pueden relacionar gracias a la exactitud del sistema NTP, además la concordancia de los registros generados en el sistema de monitoreo y el RADIUS por ejemplo, colaboran con la completitud de los registros dando la posibilidad de correlacionar eventos.

#### 4. Conclusiones.

La infraestructura fue generada a modo general, ya que en el mercado existen muchos fabricantes y software que puede ser usado para implementarla, esto con el objetivo de no limitar al usuario y adaptarse a los equipos que tenga en el momento y a las capacidades de obtención de dispositivos, hardware y software.

La propuesta de la infraestructura presentada no pretende ser un modelo de cómo manifestar conceptos de gestión de evidencia en una arquitectura de computadores, sino plantear consideraciones básicas para un estudio futuro.

La autenticidad, exactitud y suficiencia de los registros son características importantes a la hora de dar relevancia a una evidencia, la infraestructura planteada tiene como objetivo aumentar la admisibilidad y relevancia de los registros, para el cual se puede realizar varios aportes pero no logrando cumplirlo en su totalidad. Es importante resaltar que la alternativa de seguridad 802.11i no aporta mucho por sí sola en la búsqueda de este objetivo por eso se cuenta con varios elementos que complementan la solución.

Dentro del proceso de gestión de evidencia se deben tener en cuenta varias recomendaciones establecidas para no invalidar la evidencia o que pierda valor probatorio por establecer malas prácticas o

algunos otros factores. El factor humano, se requiere de un profesional capacitado para llevar a cabo este proceso de gestión y aun así existe la posibilidad que se falle en algún punto. Los procedimientos de recolección y análisis aunque no son tema de esta infraestructura.

Es importante tener en cuenta las técnicas antiforenses que pueden ser usadas en contra de los sistemas de monitoreo y gestión de evidencia. Con el fin de evadir un posterior análisis forense, algunos métodos usados son el uso de canales ilegales y cifrado fuerte. Es recomendable estudiar a profundidad estos casos para en un futuro tener herramientas que permitan un análisis forense completo.

#### 5. Referencias

[Acis06] Cano Martines Jeimy José. Introducción a la informática forense. Revista ACIS Junio de 2006 Disponible en: [http://www.acis.org.co/fileadmin/Revista\\_9/dos.pdf](http://www.acis.org.co/fileadmin/Revista_9/dos.pdf)

[AdmEvi03] Cano Martines Jeimy José. Admisibilidad de la Evidencia Digital: Algunos Elementos de Revisión y Análisis. Agosto de 2003. <http://www.alfa-redi.org/rdi-articulo.shtml?x=1304>

[BueAdm06] Cano Martines Jeimy José. (2006) Buenas prácticas en la administración de la evidencia digital. Consultado: Mayo de 2006. Disponible: <http://gecti.uniandes.edu.co/docs/buenas%20Opractica%20evidencia%20digital%20jcano.pdf>

[Casey04] CASEY, Eoghan. "Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet". 2004

[EviDig05] Cano Martines Jeimy José, Mosquera González José Alejandro, Certain Jaramillo Andrés Felipe. Evidencia Digital: contexto, situación e implicaciones nacionales. Abril de 2005. Disponible en: <http://derecho.uniandes.edu.co/derecho1/export/derecho/descargas/texto/NasTecnologias6.pdf>

[HBIT03] HB171:2003 Handbook  
Guidelines for the management of IT  
evidence Disponible en:

<http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN016411.pdf>

[SEGWF] Lehembre, Guillaume. Seguridad  
Wi-Fi – WEP, WPA y WPA2. Recuperado  
el 9/10/2006 de

[http://www.hsc.fr/ressources/articles/hakin9\\_wifi/hakin9\\_wifi\\_ES.pdf](http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_ES.pdf)