

FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

**Tema:**

Manejo de Archivos de LOG

**Autores:**

Mamani Valencia, Jeancarlos

Merino Maceta, Carlos Brayan

Morales Carlos, Jesús

Orellana Aliano, Roberto Sebastian

**Docente:**

Coronel Castillo, Eric Gustavo

**Año:**

**Año del Buen Servicio al Ciudadano**

Lima - Perú

2017

Índice

Resumen ………………………………………………………………………………………………………………………………..

Antecedentes …………………………………………………………………………………………………………………………

Desarrollo del tema ……………………………………………………………………………………………………………….

Capítulo I …………………………………………………………………………………………………………………..

1. Concepto ………………………………………………………………………………………………………
2. Tipos ……………………………………………………………………………………………………………..

Capítulo II ………………………………………………………………………………………………………………….

1. Aplicaciones ………………………………………………………………………………………………….
2. Modelo de Aplicación de los Archivos Log, en un programa de Operaciones básicas………………………………………………………………………………………………………….

Conclusiones ………………………………………………………………………………………………………………………….

Recomendaciones ………………………………………………………………………………………………………………….

Referencias …………………………………………………………………………………………………………………………….

Bibliográficas ………………………………………………………………………………………………………………………….

Anexos ……………………………………………………………………………………………………………………………………

Resumen

* Como se ha mostrado, el sistema operativo de nuestra computadora, al momento que se encuentra en pleno trabajo, comparte una gran codicia de Información acerca de los procesos que se realizan desde el momento en que iniciamos el manejo del computador hasta terminar con nuestras actividades cotidianas. Por esta razón, es de mucha importancia la ejecución de esta tarea para poder trabajar de una manera segura con nuestra computadora y evitar aquellos problemas que impiden el servicio al usuario. Aquellas informaciones que están compartidas se encuentran ubicadas en un archivo de registro, también llamados archivos log. Estos archivos son los que se encargan de cargar dichos mensajes de información enviados por el sistema operativo, lo cual son registrados y visualizados por el administrador.
* También se ha mostrado que la información que tienen los archivos log puede ayudar mucho en el aspecto de la seguridad. Ya que se pueden presentar muchos tipos de entes desconocidas que intentan alterar el sistema ya sea de una empresa o una gran organización. Por ello los archivos log tienen mucha importancia en el aspecto de la seguridad en los sistemas. Debido a ello y para controlar su administración, existen muchos tipos archivos log que permiten clasificar dichos registros. Incluso existen tipos que permiten la sincronización con otros servidores y eso también puede ayudar a brindar más seguridad en caso de que alguien intente alterar dichos archivos.
* Además de que existen varios tipos de archivos logs que se relacionan con distintos procesos, estos están presentes en acciones cotidianas, tales como mails y opciones al momento de imprimir, entre otras, siendo así que los logs registran un seguimiento, o también llamado historial, permitiendo al usuario analizar detalladamente cada movimiento que se realice.

Antecedentes

* Dada a la recopilación de información brindada por cada integrante de nuestro grupo obtuvimos un trabajo factible. Este estudio de gran contenido demostró la importancia de los archivos log (archivos de registro) con una gran cantidad de misterios lo cual fue de mucho interés y curiosidad al momento de realizar las investigaciones.
* Esta investigación está relacionada con el curso ya que es un material de conocimientos para la ilustración de procesamiento de datos a través de la recopilación de información de todos los integrantes.
* El estudio de los tipos de archivos log demuestra la importancia de cada función de cada una de estas. Dado que cada función se ha visto de importancia para el usuario, se ha visto como algo muy necesario su presentación conforme se ha avanzado esta investigación.
* Este trabajo muestra cómo se debe clasificar los archivos log y lo imprescindible que es para la solicitud de seguimientos dentro de un sistema a través de una intensa investigación y búsqueda de información de los integrantes participantes.

Desarrollo del tema

Capítulo I

1. Concepto

* **Archivo Log**

El sistema operativo es el software que me permite interactuar con mi computadora para realizar actividades, este sistema me brinda una interfaz cómoda y amigable. Por lo tanto, es el programa más importante de una computadora.

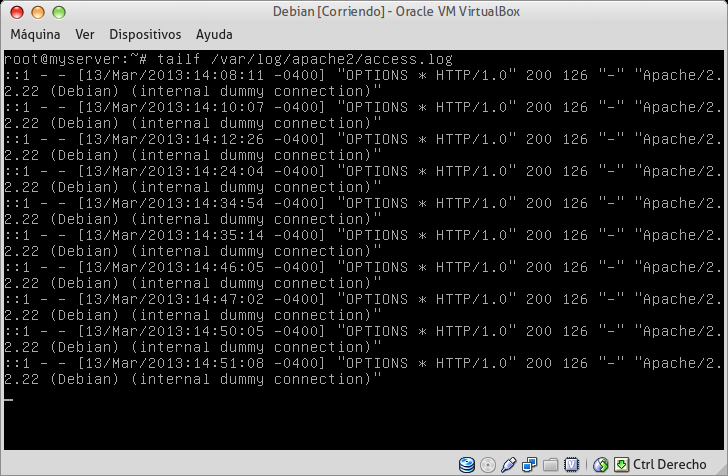
Cuando el sistema operativo está en pleno proceso comparte información con el administrador acerca de los procesos, rendimiento, detalles, servicios, historial de aplicaciones y su comportamiento de todo el sistema. Este compartimiento de información es muy importante para localizar diversos problemas a futuro y pueda seguir con aquellas actividades dirigidas por el usuario. Este informe es enviado por medio de mensajes destinados hacia los Archivos de Registro (archivo log).

Por esta razón, los registros (archivos log) son los que sujetan y/o contienen aquellos mensajes de información tratados por el sistema. Por esta razón son de mucha importancia al momento de solucionar los problemas del sistema.



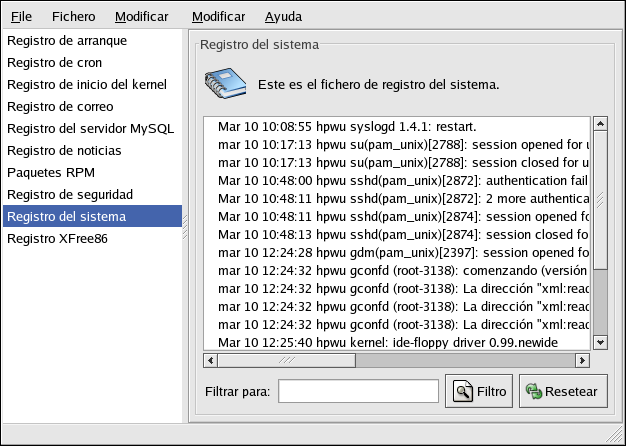
* **Localizar los archivos log**

Los archivos log se encuentran ubicados en /var/log. El “httpd” y “samba” son aplicaciones que permiten la ejecución de varios tipos de actividades ubicados en /var/log para los archivos log. Así mismo se puede observar mucha complejidad de archivos seguidos de varios números. Además, el paquete logrotate domina su tarea de, circular de archivos dependiendo de la configuración del archivo.



* **Visualizar los archivos log**

En general estos registros se encuentran en forma de contenido plano. Se puede visualizar con cualquier impresor de texto como por ejemplo Vi o Emacs. Algunos registros son visualizados y leídos por todos los administradores de su propio sistema; aunque se solicita tener privilegios como root para ser leídos por la mayoría de ellos.



1. Tipos

* **Log/Messages**

Una notificación del registro de archivos es una sucesión de texto con abundante información. Una porción de esa información es procesada por las llamadas de archivos por medio de componentes predeterminados y los demás se obtiene del sistema operativo y por último, se recopila del sistema operativo que pertenece al proceso generación.



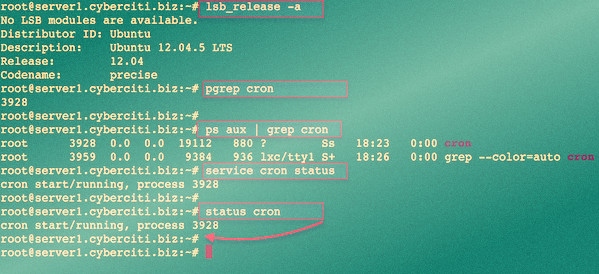
* **Log/Secure**

Registro de seguridad es un archivo de registro para las notificaciones de seguridad contienen información secreta que no puede ser revelado debido a su privacidad puesto que lo hace muy vulnerable la seguridad del propio sistema. Por esa razón es de mucha importancia cuidar y/o proteger la privacidad de la información.



* **Log/Cron**

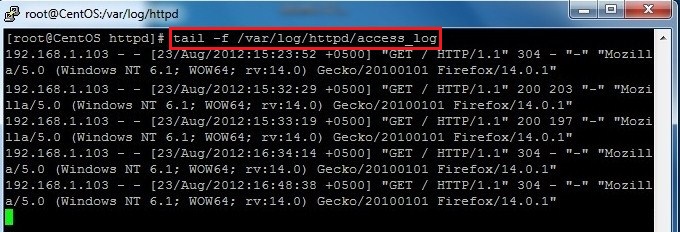
Se encarga de las tareas de crond que es el programa que permite a usuarios Linux/Unix ejecutar comandos a hora y fecha específica.



* **Log/httpd**

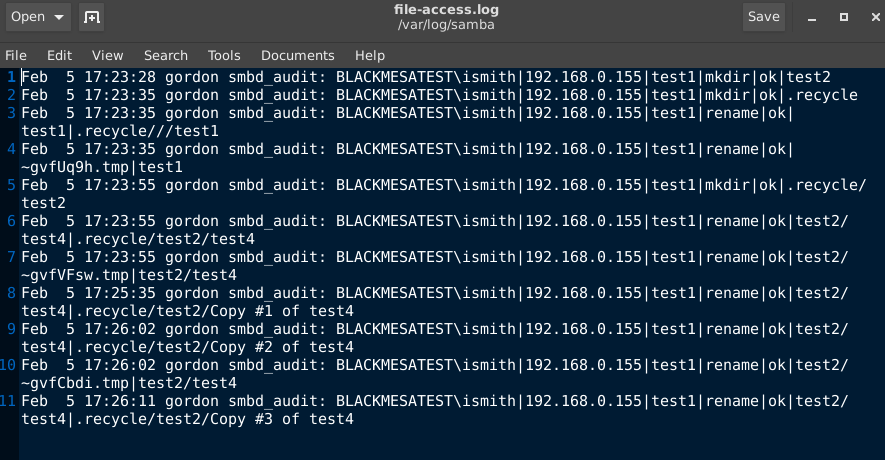
Se ocupa de los errores y accesos de apache los cuales son:

* **Error Log**
* Es el más importante de todos los registros. Apache enviará cualquier información de evaluación y reconocerá cualquier error que encuentre al tratar peticiones al archivo de registro seleccionado.
* El formato del registro de errores es relativamente libre y descriptivo. Pero, hay cierta información que se incluye en algunas de las entradas de un registro de errores.
* **Access Log**
* El servidor acopla en el registro de acceso información acerca de todas las peticiones que trata. Este formato del registro es altamente configurable.
* Esto solo resulta ser el primer paso, ya que después de esto se analiza la información obtenida para procesar estadísticas que resulten útiles.



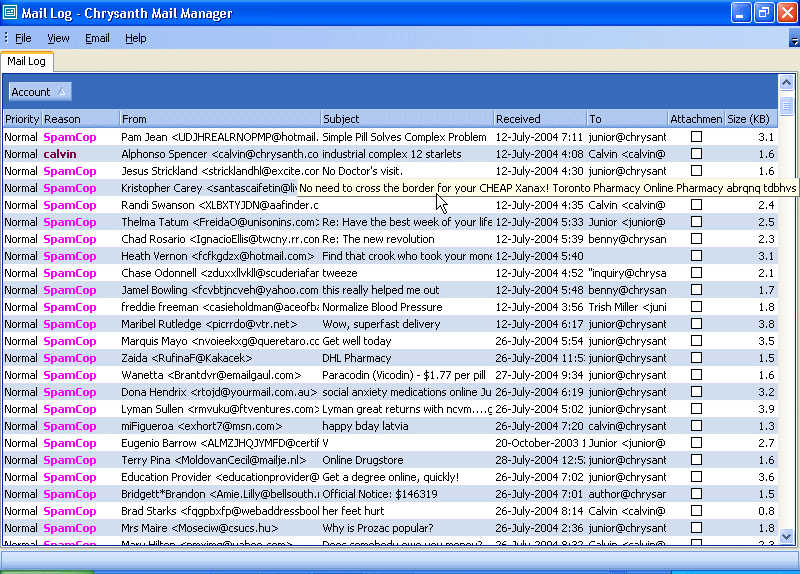
* **Log/Samba**

En este directorio se guardan los logs relacionados con el servicio samba, el cual permite conectar equipo Windows con Linux.



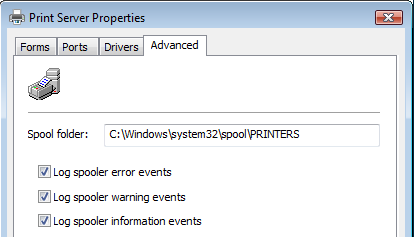
* **Log/Maillog**

Se encargan del seguimiento de registros del servidor de mails.



* **Log/Spooler**

Se encarga del seguimiento del registro de todas las actividades referentes a la impresora siendo esta la cola de impresión la principal.



* **Log/boot.log**

Registra eventos y servicios que empiezan cuando se inicia el sistema. Sirve para ayudar a diagnosticar acerca de cualquier problema durante el proceso de inicio.

* **Log/dmesg**

Proporciona mensajes del kernel (núcleo), así como también información sobre el hardware de un sistema y puede ser muy útil en la solución de problemas de esta.

* **Var/run/utmp**

Mantiene una contabilidad completa del estado actual del sistema, por ello lista a los usuarios que están actualmente dentro del sistema.

* **Var/log/wtmp**

Este actúa como un historial, ya que registra quiénes estuvieron en el sistema y cuándo lo estuvieron.

* **Var/log/lastlog**

Este formatea y solo muestra, para cada usuario, el último archivo de registro de inicio de sesión en el sistema, es decir, cuándo fue la última vez que entró al sistema.

* **Var/log/btmp**
* Se encarga de registrar aquellos intentos fallidos de inicio de sesión para poder monitorear a intrusos que puedan tratar de alterar el sistema.
* Tanto utmp, wtmp y btmp son los que mantienen registrados todos los inicios y cierres de sesión en el sistema. Ayudan a mantener la seguridad del sistema mostrando el seguimiento de los usuarios e incluso de terceros que tratan de ingresar al sistema.
* **Var/log/daemon.log**

Mensajes acerca de los servicios o permisos corriendo en el sistema.

* **Var/log/auth.log**

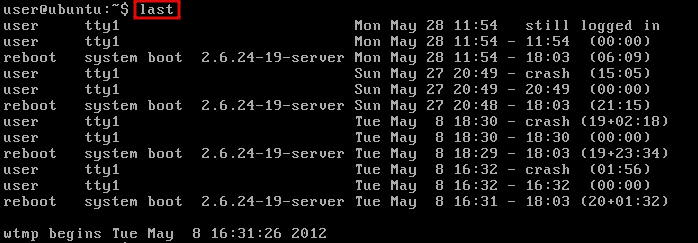
Autenticación de permisos y de usuarios.

* **Var/log/syslog.log**

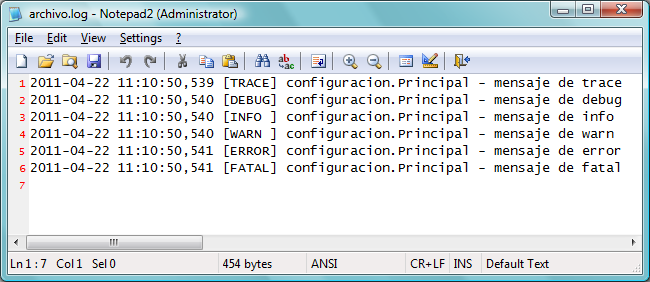
Registro del sistema de registro.

* **Var/log/user.log**

Información sobre los procesos realizados por el usuario.



* Los archivos log también se pueden presentar y mostrar por prioridades
* **Debug**. Mensaje de depuración.
* **Info**. Mensaje informativo.
* **Notice**. Condición normal, pero significativa.
* **Warning**. Hay condiciones de advertencia.
* **Err**. Hay condiciones de error.
* **Crit**. Cuando las condiciones llegan a ser críticas.
* **Alert**. Se debe tomar inmediatamente una acción correctora.
* **Emerg**. El sistema está inutilizable.



Capítulo II

1. Aplicaciones

* En los sistemas operativos por defecto se crea muchos archivos de registro(LOG) de distintos procesos realizados, Eventos del sistema, eventos de seguridad, evento de aplicaciones, evento de configuración, evento de entrada y salida. Estor archivos son importantes para el sistema de información, debido a que si hay un error en el sistema se puede recuperar mediante los archivos log.



* En los correos electrónicos los archivos se almacenan de los mensajes, notificaciones y notas. Usado luego para recuperar datos del usuario.



* En los softwares instalados almacena todos los datos que puedan afectar al sistema, por si algún momento hay un fallo en el sistema se podrá solucionar fácilmente.



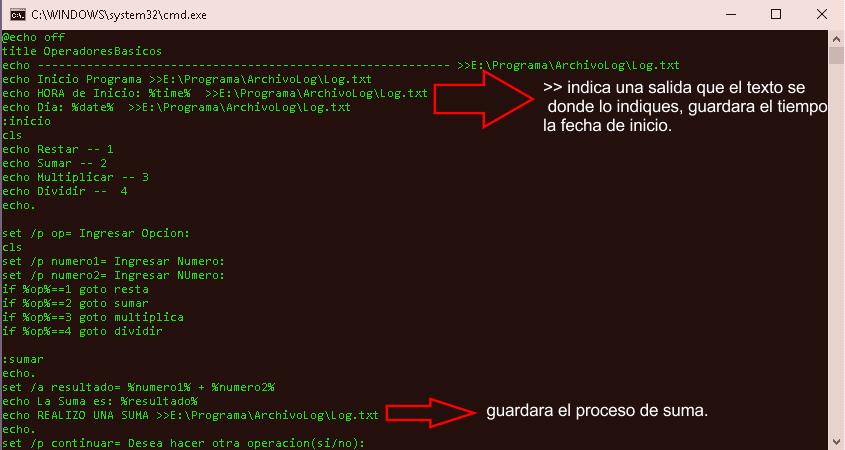
* Servidores web una gran información brinda información útil de cada usuario la cual es almacenada en una base de datos, los cuales también son guardadas en archivo log por si sucede un fallo en el sistema y puedan recuperar los datos. También son usados los archivos log para saber cuánto tiempo el usuario para en el sitio web, cuál es su dirección IP, a que hora se conectó, cuando se desconectó, cualquier evento que pueda realizar el usuario en la página web.

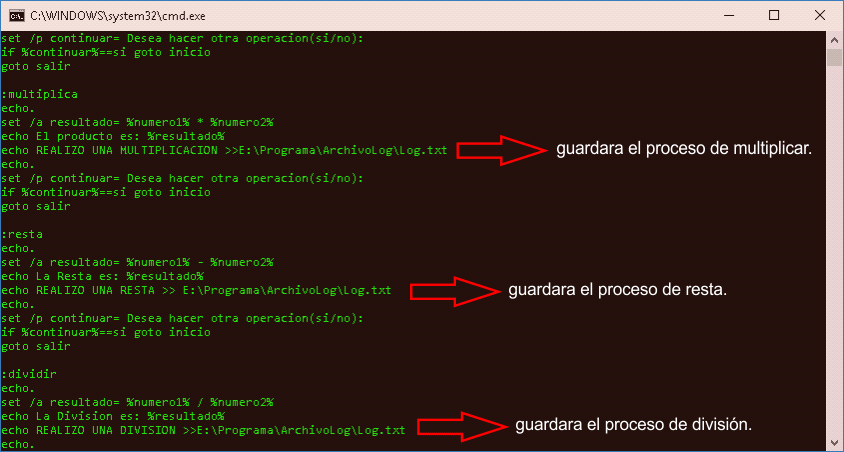


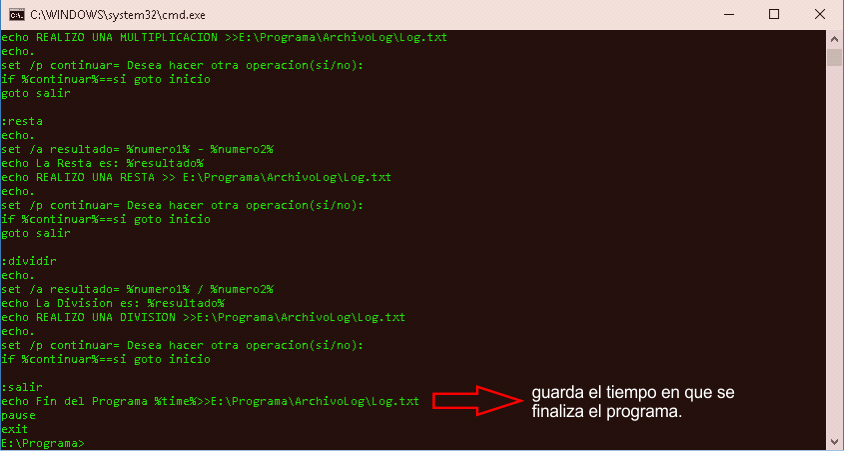
1. Modelo de Aplicación de los Archivos Log, en un programa de Operaciones básicas

* En esta pequeña aplicación desarrollada en el lenguaje "BAt", archivo de procesamiento por lotes
* En el archivo registraremos la hora de Inicio del programa, las operaciones que realiza el usuario y el fin del programa.
* **Pasos**

1.



2. 

3. 

Conclusiones

* En conclusión, los archivos log (archivos de registro) son los que registran la información brindada por el sistema operativo, lo cual podemos ubicar aquellos problemas que se presenten por delante. Por esta razón son de mucha importancia al momento de solucionar problemas. Por otro lado, existen dichas dificultades que, al momento de eliminarlos, la recopilación de la información brindada no es suficiente para poder obtener una solución.
* El grupo concluye que los tipos de archivos log brindan una mejor facilidad para la impresión de los registros hechos por los usuarios y con ello genera una mejor facilidad para la administración de estas. Incluyendo la muestra de mensajes con prioridades por problemas que se puedan presentar.
* Finalmente se puede apreciar que estos archivos están presentes en diversos procesos que se relacionan con nuestro entorno, haciéndonos obtener un mayor conocimiento de las acciones que estos realizan.

Recomendaciones

* El grupo recomienda, estar actualizados con la información servida por el sistema operativo y poder visualizarlo constantemente para poder evitarnos de aquellos problemas dados en momentos inesperados. Sin embargo, no se deben satisfacer con la información que se le es brindada al usuario, se debe seguir investigando más para una mayor seguridad tanto la computadora como el usuario.
* Nuestro equipo recomienda que para mantener seguro un sistema, se debe administrar adecuadamente los archivos log, conocer cada tipo y emplearlos para un seguimiento adecuado de las operaciones de los usuarios.
* Estos procesos se pueden aplicar a diversos entornos, por lo tanto, la recomendación es estar atentos a lo que surja en un futuro, ya que esto simplifica bastante el seguimiento de las acciones que realizamos.

Referencias Bibliográficas

* ALEGRE DEZ, Alonso, BEGOÑA, María. Gestión de Logs [en línea]. febrero de 2016. [Fecha de consulta: 12 de septiembre de 2017].

Disponible en:

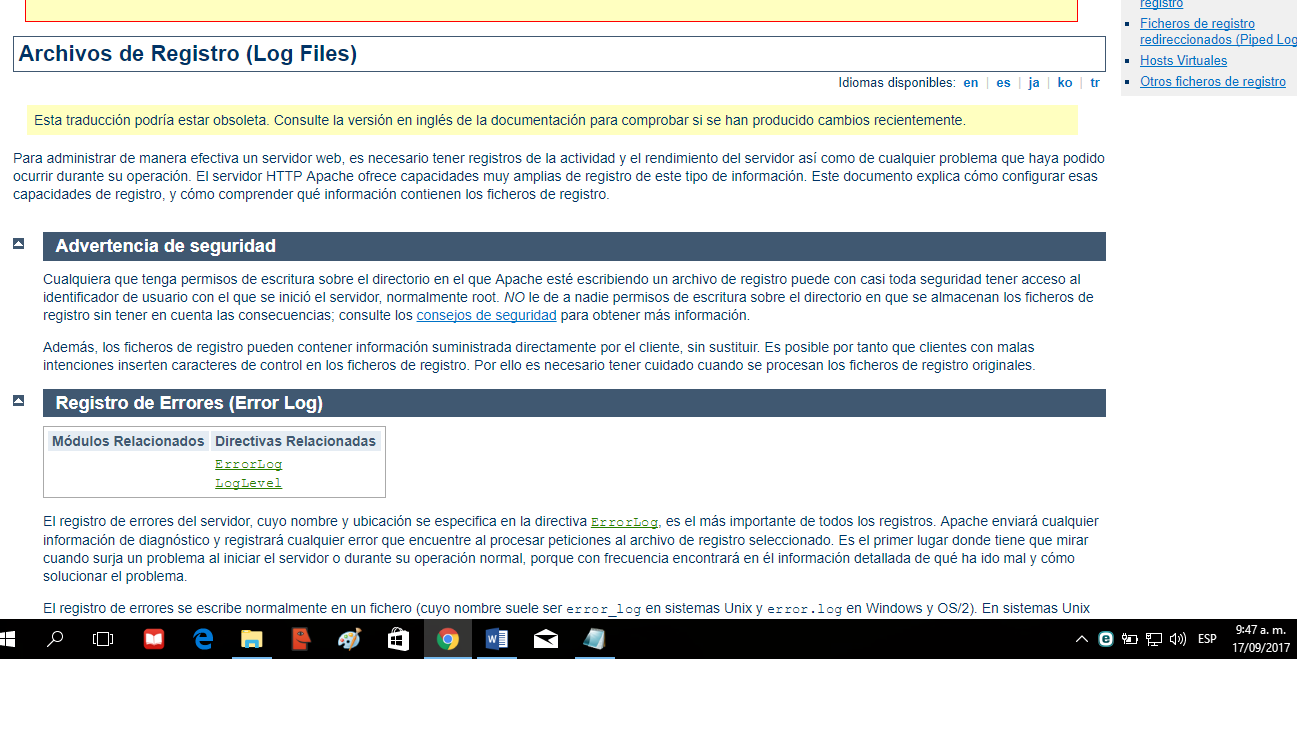
<http://reunir.unir.net/bitstream/handle/123456789/3618/ALONSO-ALEGRE%20DIEZ%2c%20MARIA%20BEGO%C3%91A.pdf?sequence=1&isAllowed=y>

* Archivos de Registro (Log Files) - Servidor HTTP Apache [en línea]. [Fecha de consulta: 12 de septiembre de 2017].

Disponible en:

<https://httpd.apache.org/docs/2.0/es/logs.html>

* CHICANO, Ester. Gestión de incidentes de seguridad informática. IFCT0109: IC Editorial, 2015. ISBN: 9788416351701
* Red Hat. Manual de administración del sistema [en línea]. Estados Unidos: 2003. Disponible en: <http://web.mit.edu/rhel-doc/3/pdf/rhel-sag-es.pdf>

Anexos



