

“Evitando la Falsificación/ Alteración de evidencia Digital.”

Jose Moruno Cadima

Twitter: @sniferl4bs
www.sniferl4bs.blogspot.com

Que veremos

1 Introducción

- Que es la Evidencia
- Evidencia Digital
- ¿Confiar en lo electrónico?

2 Confianza Digital

- Confianza Digital
- MD5
- Firmas Digitales
- Estampa de Tiempo



3 Usando herramientas

- Que hacemos ahora
- Web Sellada
- Mail Sellado

4 Preguntas

Evidencia

- Delito.
- Proceso de investigación.



Evidencia

- Delito.
- Proceso de investigación.
- Evidencia.

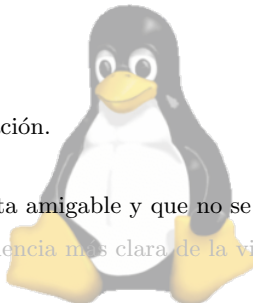


Evidencia

- Delito.
- Proceso de investigación.
- Evidencia.

Es una certeza que resulta amigable y que no se puede dudar.

- “Su rostro es la evidencia más clara de la violencia de género.”

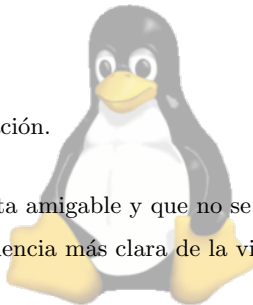


Evidencia

- Delito.
- Proceso de investigación.
- Evidencia.

Es una certeza que resulta amigable y que no se puede dudar.

- “Su rostro es la evidencia más clara de la violencia de género.”



Evidencia Digital

- Actualmente la evidencia, es presentada en medios digitales...



Evidencia Digital



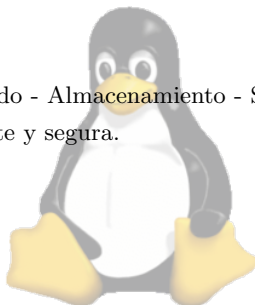
Confianza

- Archivado - Guardado - Almacenamiento - Seguridad.
- Autenticidad - Fuerte y segura.



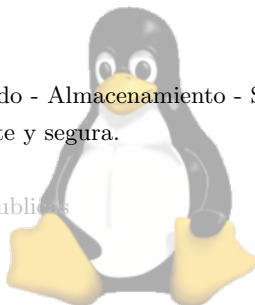
Confianza

- Archivado - Guardado - Almacenamiento - Seguridad.
- Autenticidad - Fuerte y segura.
- Certificado Digital



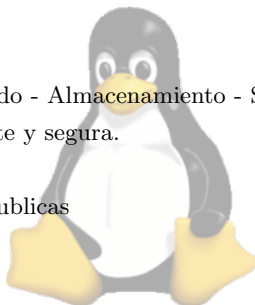
Confianza

- Archivado - Guardado - Almacenamiento - Seguridad.
- Autenticidad - Fuerte y segura.
- Certificado Digital
- Claves privadas y Públicas



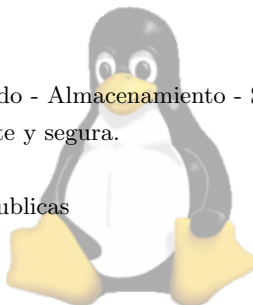
Confianza

- Archivado - Guardado - Almacenamiento - Seguridad.
- Autenticidad - Fuerte y segura.
- Certificado Digital
- Claves privadas y Publicas
- Confianza Digital



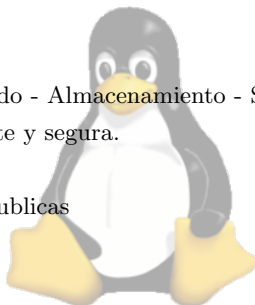
Confianza

- Archivado - Guardado - Almacenamiento - Seguridad.
- Autenticidad - Fuerte y segura.
- Certificado Digital
- Claves privadas y Publicas
- Confianza Digital



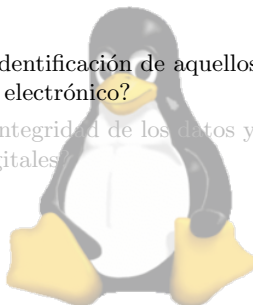
Confianza

- Archivado - Guardado - Almacenamiento - Seguridad.
- Autenticidad - Fuerte y segura.
- Certificado Digital
- Claves privadas y Publicas
- Confianza Digital



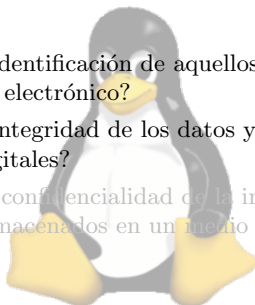
Confianza

- ¿Cómo asegurar la identificación de aquellos que están trabajando en un entorno digital o electrónico?
- ¿Cómo asegurar la integridad de los datos y documentos enviados a través de medios digitales?

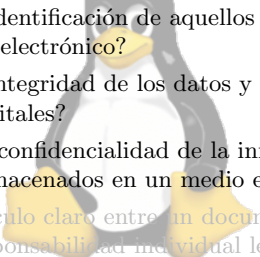


Confianza

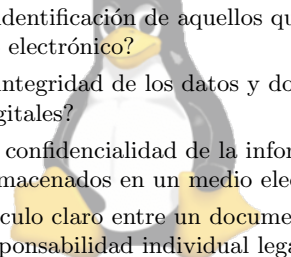
- ¿Cómo asegurar la identificación de aquellos que están trabajando en un entorno digital o electrónico?
- ¿Cómo asegurar la integridad de los datos y documentos enviados a través de medios digitales?
- ¿Cómo conservar la confidencialidad de la información y los datos intercambiados o almacenados en un medio electrónico?



Confianza

- 
- ¿Cómo asegurar la identificación de aquellos que están trabajando en un entorno digital o electrónico?
 - ¿Cómo asegurar la integridad de los datos y documentos enviados a través de medios digitales?
 - ¿Cómo conservar la confidencialidad de la información y los datos intercambiados o almacenados en un medio electrónico?
 - ¿Cómo crear un vínculo claro entre un documento o una acción electrónicos y la responsabilidad individual legal?

Confianza

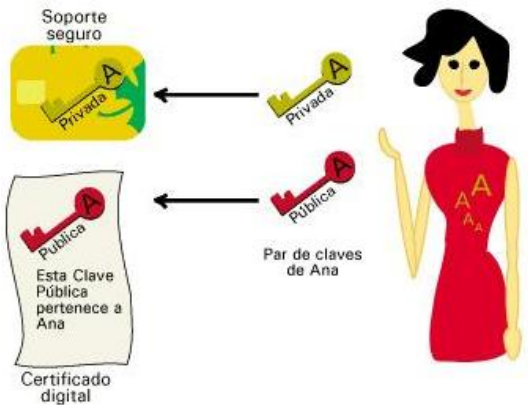
- 
- ¿Cómo asegurar la identificación de aquellos que están trabajando en un entorno digital o electrónico?
 - ¿Cómo asegurar la integridad de los datos y documentos enviados a través de medios digitales?
 - ¿Cómo conservar la confidencialidad de la información y los datos intercambiados o almacenados en un medio electrónico?
 - ¿Cómo crear un vínculo claro entre un documento o una acción electrónicos y la responsabilidad individual legal?

MD5



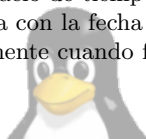
- MD5 (abreviatura de Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits.

Certificado Digital



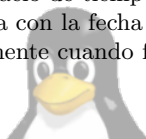
Time Stamp

- Marca de tiempo ó Timestamping consiste en certificar mediante una secuencia de caracteres que un conjunto de datos ha existido y no ha sido modificado en un espacio de tiempo determinado. La secuencia de caracteres está relacionada con la fecha y el momento en que ocurre dicho evento y específicamente cuando fue creado en un sistema de cómputo.



Time Stamp

- Marca de tiempo ó Timestamping consiste en certificar mediante una secuencia de caracteres que un conjunto de datos ha existido y no ha sido modificado en un espacio de tiempo determinado. La secuencia de caracteres está relacionada con la fecha y el momento en que ocurre dicho evento y específicamente cuando fue creado en un sistema de cómputo.



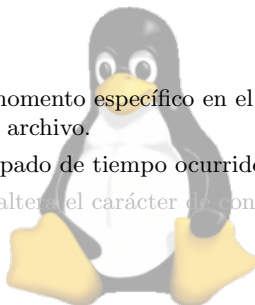
Características

- Certifica la hora y momento específico en el que se lleva a cabo un suceso o se firma un archivo.
- Registra todo estampado de tiempo ocurrido, en una base de datos.



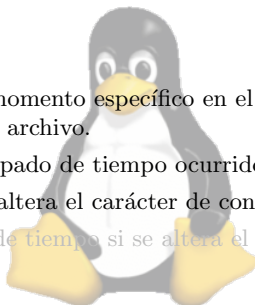
Características

- Certifica la hora y momento específico en el que se lleva a cabo un suceso o se firma un archivo.
- Registra todo estampado de tiempo ocurrido, en una base de datos.
- Asegurar que no se altera el carácter de confidencialidad del archivo



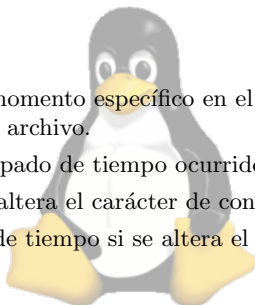
Características

- Certifica la hora y momento específico en el que se lleva a cabo un suceso o se firma un archivo.
- Registra todo estampado de tiempo ocurrido, en una base de datos.
- Asegurar que no se altera el carácter de confidencialidad del archivo
- Invalidar el sellado de tiempo si se altera el documento.



Características

- Certifica la hora y momento específico en el que se lleva a cabo un suceso o se firma un archivo.
- Registra todo estampado de tiempo ocurrido, en una base de datos.
- Asegurar que no se altera el carácter de confidencialidad del archivo
- Invalidar el sellado de tiempo si se altera el documento.



Beneficios

- Minimiza el riesgo de modificación de la información.
- Alteración.



Beneficios

- Minimiza el riesgo de modificación de la información.
- Alteración.
- Se eliminan factores de duda respecto del momento en que suceden acciones.



Beneficios

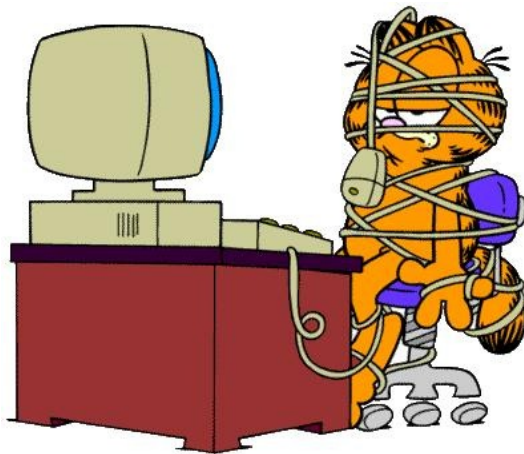
- Minimiza el riesgo de modificación de la información.
- Alteración.
- Se eliminan factores de duda respecto del momento en que suceden acciones.



Y ahora todo eso de que me sirve?



A ponerlo en práctica



Web Sellada



Acuse de Recibo Sello de tiempo en WEB



Recibidos x



websellada@securitybydefault.com



para mí ▾



chino ▾



español ▾

[Traducir mensaje](#)

Adjuntado PDF, contenido web, firma digital y el sello de tiempo

Status info:

Status: Granted.

Status description: unspecified

Failure info: unspecified

TST info:

Version: 1

Policy OID: 1.3.6.1.4.1.8149.3.2.1.1.0

Hash Algorithm: sha1

Message data:

0000 · 2f 52 42 5d ee 5f 1e ef-65 b9 82 7e 7b ed 9d b1 /RB]_...e...~{...

0010 · 38 5c 88 99 8\...

Serial number: 0xD422C0

Time stamp: Jun 18 00:06:02 2012 GMT

Accuracy: unspecified

Ordering: yes

Nonce: 0x3E65AFE7EAFC97E7

TSA: DirName:/C=ES/O=Generalitat Valenciana/OU=PKIGVA/CN=TSA1 ACCV

Extensions:

3 archivos adjuntos — [Descargar todos los archivos adjuntos](#)**727801348931.614.pdf**33 kb [Ver](#) [Descargar](#)**727801348931.614.pdf.asc**1 kb [Ver](#) [Descargar](#)**727801348931.614.tsr**4 kb [Descargar](#)

Como se usa

- Enviar un mail a websellada@securitybydefault.com
- url

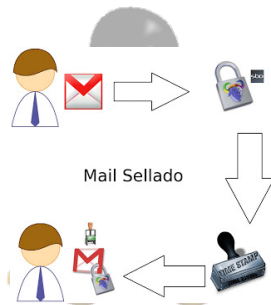


Como se usa

- Enviar un mail a websellada@securitybydefault.com
- url



Mail Sellado



Como se usa

- Enviar un mail a websellada@securitybydefault.com
- url



Como se usa

- Enviar un mail a websellada@securitybydefault.com
- url



Preguntas!

