INFORMATICA FORENSE
PERICIAS INFORMATICAS

Ingeniero en Sistemas Informáticos

Eduardo J. Piro

Temas a desarrollar

- Aseguramiento de pruebas informáticas – Constataciones notariales y judiciales – Cómo peticionar las medidas – Cómo constatar una página WEB.
- Pruebas periciales informáticas– Obtención de evidencias y cómo resguardarlas. Técnicas de hashing – Medidas de seguridad.
- Mails – El mail como prueba – Ámbito de aplicación de la ley de delitos informáticos – Autenticación de mails.
- Políticas de uso de herramientas informáticas. Cuentas de usuarios – Contraseñas – Políticas de confidencialidad.
- Licenciamiento de Software – Intimaciones.

Pericias Informáticas - Introducción

- **El peritaje informático**, las técnicas informáticas utilizadas en la obtención de datos útiles que, potencialmente, podrían convertirse en evidencia o prueba en un proceso judicial.

- El campo de la pericias informáticas involucra la identificación, extracción, documentación y preservación de la información almacenada o transmitida de forma electrónica o magnética (o sea, evidencia digital).

- Dado que este tipo de evidencia es intangible y puede ser fácilmente modificada sin dejar rastros, la evidencia digital debe ser manejada y controlada cuidadosamente.

Informática Forense - Metodologías

Las tres A:

- **Adquirir** evidencia sin modificaciones o corrupciones
- **Autenticar** que la evidencia recuperada es la misma que la que originalmente se incauto
- **Analizar** los datos sin ninguna alteración

Proceso de investigación

- Identificación (detectar los eventos o delitos)
- Recolección (recuperar datos, recolectar evidencia)
- Preservación (almacenar/conservar, cadena de custodia, documentación)
- Examen (rastrear, filtrar, extraer datos ocultos)
- Análisis (analizar la evidencia)
- Presentación (reporte de investigación)
- Decisión (dictamen)

Pericias Informáticas

Para que una pericia informática cumpla con la finalidad por la cual fue solicitada en un juicio, los que la solicitaron, deben tener en cuenta que tienen que cumplir con algunas características específicas:

- **Tiene que derivarse de un proceso que sea válido legalmente**, la colección de datos a brindarle al perito, para que este los verifique en el proceso pericial.

- Al ser tan sofisticada y con desarrollos y modificaciones constantes, la informática, debe preverse que **los archivos necesarios para resolver el problema deben ser resguardados manteniendo determinados requisitos**, ya que de no efectuarse de ésta manera, puede quedar contaminada la evidencia.

- No siempre es verificable y se puede demostrar cabalmente una situación ocurrida por medios informáticos, por lo cual **todas las evidencias, por más insignificantes que parezcan deben resguardarse**.

Aseguramiento de pruebas

- Ante la posibilidad de desaparición de determinados elementos probatorios durante el transcurso del proceso, es necesario que éstos queden adquiridos antes de que ese riesgo se produzca.

- El hecho de que se solicite una medida cautelar, se justifica por el denominado peligro en la demora, ya que el futuro demandado **con solo apretar una tecla del equipo de sus computadoras haría desaparecer todos los archivos o mails que se encuentren almacenados en sus computadoras.**

- En caso de no efectuarse la constatación judicial -mediante una medida cautelar- podrían darse supuestos de imposibilidad y/o frustración de pruebas.

CELERIDAD en obtención de la prueba

Aseguramiento de pruebas

¿Cómo obtenemos la prueba?

Se deberá analizar cada caso en particular

Medidas cautelares judiciales (perito de oficio) o

Constataciones Notariales (perito de parte. El escribano sólo deja constancia de sus manifestaciones)

Aseguramiento de pruebas

Puntos periciales

- Terminología técnica a utilizar
- Ser muy precisos / concretos / puntuales con lo que solicita (ejemplo)
- Saber que tipo de hardware (computadoras, servidores, etc) y software (sistemas operativos, aplicaciones, etc) se utilizan
- Asesorarse por un profesional informático
- Costos de los elementos necesarios (discos rígidos, software,etc)
- Error muy común de solicitar pericial contable

Aseguramiento de pruebas: Solicita

Que a vengo solicitar que si las computadoras en las cuales constan los datos pedidos requieran algún tipo de contraseña, y la misma no fuera suministrada, o las computadoras no estuvieran funcionando o por cualquier motivo no pudiera accederse a los archivos o documentos requeridos deberá realizarse una copia completa o secuestrarse el o los discos rígidos de aquellas, previo a ser embalados y precintados, colocada una faja de seguridad firmada por el Sr. Oficial de Justicia, nombrándose un depositario judicial y se fijará día y hora para abrirla, autorizándose a la empresa XXXX a nombrar un delegado técnico que controle la pericia.

Constatación de Páginas Web

- ISP (Proveedor de Servicios de Internet)
- Dirección IP pública
- Comandos ping / tracert / nslookup
- NIC (Dominios) – Hosting (IP de la página)
- Impresión
- Grabación en medio magnético u óptico
- Código fuente
- Cuidados con los proxy server

¿Qué es una dirección IP?

- Las direcciones IP (Internet Protocol) son un número único e irrepetible con el cual se identifica un dispositivo (generalmente una computadora) conectado a una red que corre el protocolo TCP/IP.
- Una IP es un conjunto de cuatro números del 0 al 255 separados por puntos. Por ejemplo, 200.36.127.40
- Hay casi cuatro mil trescientos millones de direcciones IP posibles.

¿Qué es una dirección IP? Clasificación

- Clases: A, B o C

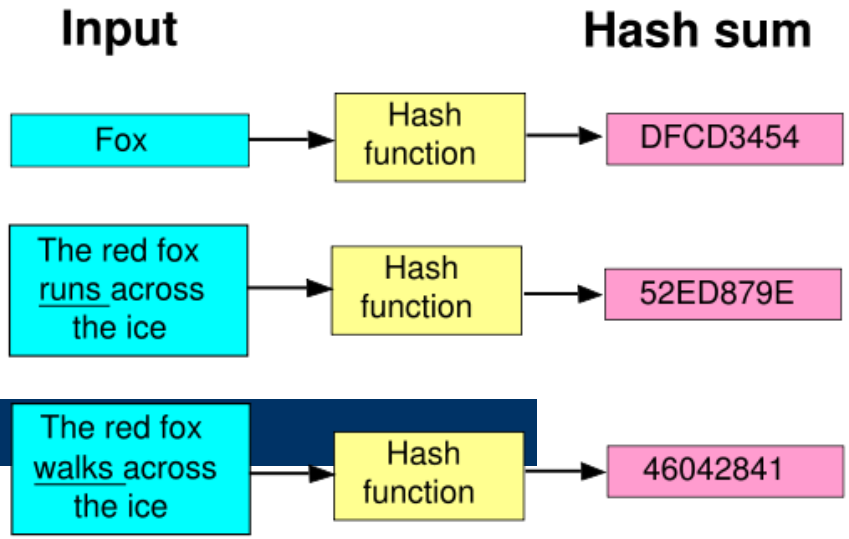
  (**10.0.0.0** / **172.16.0.0** / **192.168.0.0**)
- Públicas o Privadas
- Estáticas (Fijas) o Dinámicas

  La IP identifica a ese dispositivo unívocamente y puede permanecer invariable en el tiempo o cambiar cada vez que se reconecte a la red. Una dirección IP es estática cuando no varía, y es dirección IP dinámica cuando cambia en cada reconexión.

¿Qué es una dirección IP? Clasificación

Por lo general los servidores (computadoras) que alojan sitios web poseen direcciones IP fijas, de esta manera son identificables en todo momento, con facilidad y, especialmente, de forma única. Por ejemplo, nosotros podríamos acceder a un sitio web específico con cualquier navegador sabiendo su dirección IP, pero recordar tantos números es complicado y difícil de manejarlos; por lo tanto se usan direcciones más sencillas como podría ser "miempresa.com.ar". Dicha dirección está asociada a una dirección IP y permite así identificar qué servidor es el encargado de mostrarnos este sitio.

Hashing



¿Qué es hashing? El hashing es una técnica que consta de datos de entrada, una función hash y un código de salida.

Esta función calcula un código específico para los datos de entrada (ejemplo toda la información contenida en el disco rígido). El valor calculado puede parecer aleatorio, pero no lo es, ya que las operaciones para obtener el código de salida son siempre las mismas.

La función hash asocia siempre la misma salida para una entrada determinada. Por consiguiente cualquier variación realizada en los datos del disco sería detectada porque el código hash resultaría diferente.

Hashing

- **hash(“María”) = 1082358727484**
- **Ejemplo de herramientas: md5** **prueba**
- El hash es la única manera de preservar la **integridad** de la información para saber si el contenido fue modificado.

Secuestros de equipos o discos

Los equipos secuestrados pueden contener información o datos trascendentales o muy importantes. Su pérdida o modificación puede causar daños irreparables al dueño de los equipos. Además no es necesario secuestrar todo el equipo, con solo hacer una copia de los discos rígidos de los mismos se obtiene la evidencia para su posterior análisis y se evita posibles roturas de los equipos.

Como se debe realizar un secuestro de un equipo, PC o notebook:

- Realizar una copia bit-stream del o los discos rígidos que contienen los equipos. De esta manera se preserva la información contenida por una posible pérdida o daño provocado por el traslado de los mismos.
- Se debería obtener de cada disco el hash. De esta manera se preserva la integridad de la información contenida para saber si el contenido fue modificado.
- Cuidados en el embalaje y precintado.

Secuestros de CDs / DVDs

Acta. "También se procede al secuestro de diecinueve (19) CD-R conteniendo programas apócrifos de Microsoft y dos (02) leyendas con Nro de Series de Windows".

- NO se constató el contenido o los datos almacenados en los CDs. No se realizaron impresiones del contenido. No sabemos como determinan que contienen programas apócrifos.
- NO se deja constancia ni de la marca ni de los números de serie de los CDs secuestrados.
- NO se realizó el hash de cada CD.
- NO se tuvieron cuidados en el embalaje y precintado.

Resguardo físico de la prueba

Consideraciones a tener en cuenta en el momento de un aseguramiento de pruebas

- Cuando se van a realizar grabaciones se deben utilizar dispositivos nuevos (embalaje original cerrado). CDs, pendrives, rígidos, etc.
- Se deben separar las personas que trabajen sobre los equipos informáticos lo antes posible y no permitirles volver a utilizarlos. Desconectar equipos de la red.
- Fotografiar la pantalla / equipo / ubicación. Fotografiar una toma completa del lugar donde se encuentren los equipos informáticos.
- Hacer una imagen de los discos del equipo para preservar la integridad de los originales y comprobar la integridad de la imagen para asegurarse de que la misma sea exacta.

Resguardo físico de la prueba

Consideraciones a tener en cuenta en el momento de un aseguramiento de pruebas

- Apagar el sistema de una forma segura, de acuerdo con el sistema operativo que utilice. Para evitar la destrucción de archivos se recomienda que se desenchufe el equipo directamente, sin realizar la operación de cierre. También para evitar programas de autodestrucción o borrado. Si son notebooks es necesario quitarles la o las baterías.

- Transportar las piezas sensibles en una bolsa antiestática y asegurarse de mantenerlas alejadas de fuentes de calor y electromagnéticas. Si no se cuenta, pueden utilizarse bolsas de papel madera. Evitar el uso de bolsas plásticas, ya que pueden causar una descarga de electricidad estática que puede destruir los datos.

- Los elementos informáticos son frágiles y deben manipularse con cautela.

Resguardo físico de la prueba

Consideraciones a tener en cuenta en el momento de un aseguramiento de pruebas

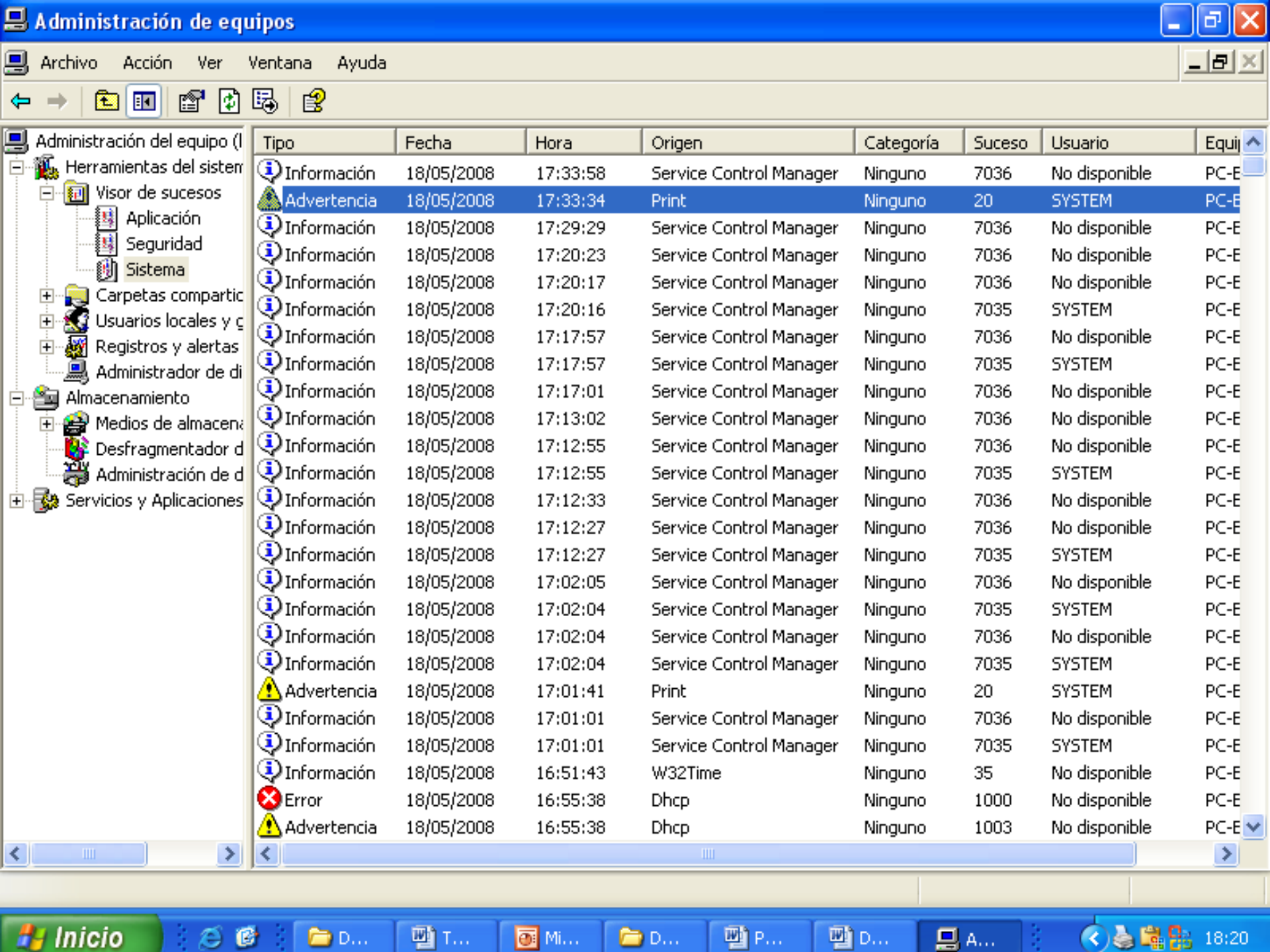
- Tomar las medidas necesarias para resguardar la información volátil (la contenida en almacenamientos temporales, tales como memoria RAM, memoria caché,etc.) Una vez que el equipo o dispositivo se apaga la información contenida en este tipo de almacenamiento se destruye.

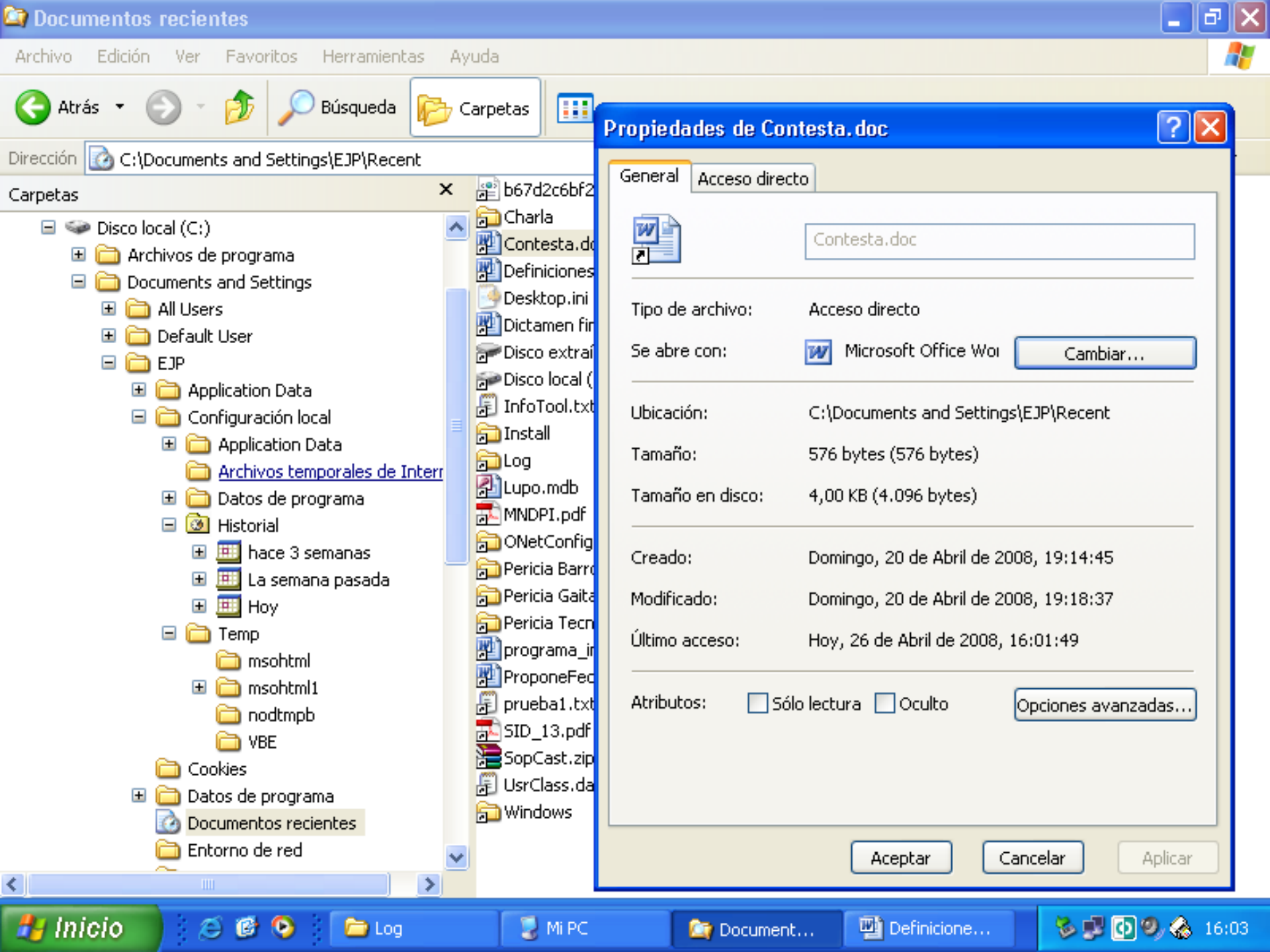
- Precintar cada equipo informático en todas sus entradas eléctricas y todas las partes que puedan ser abiertas o removidas.

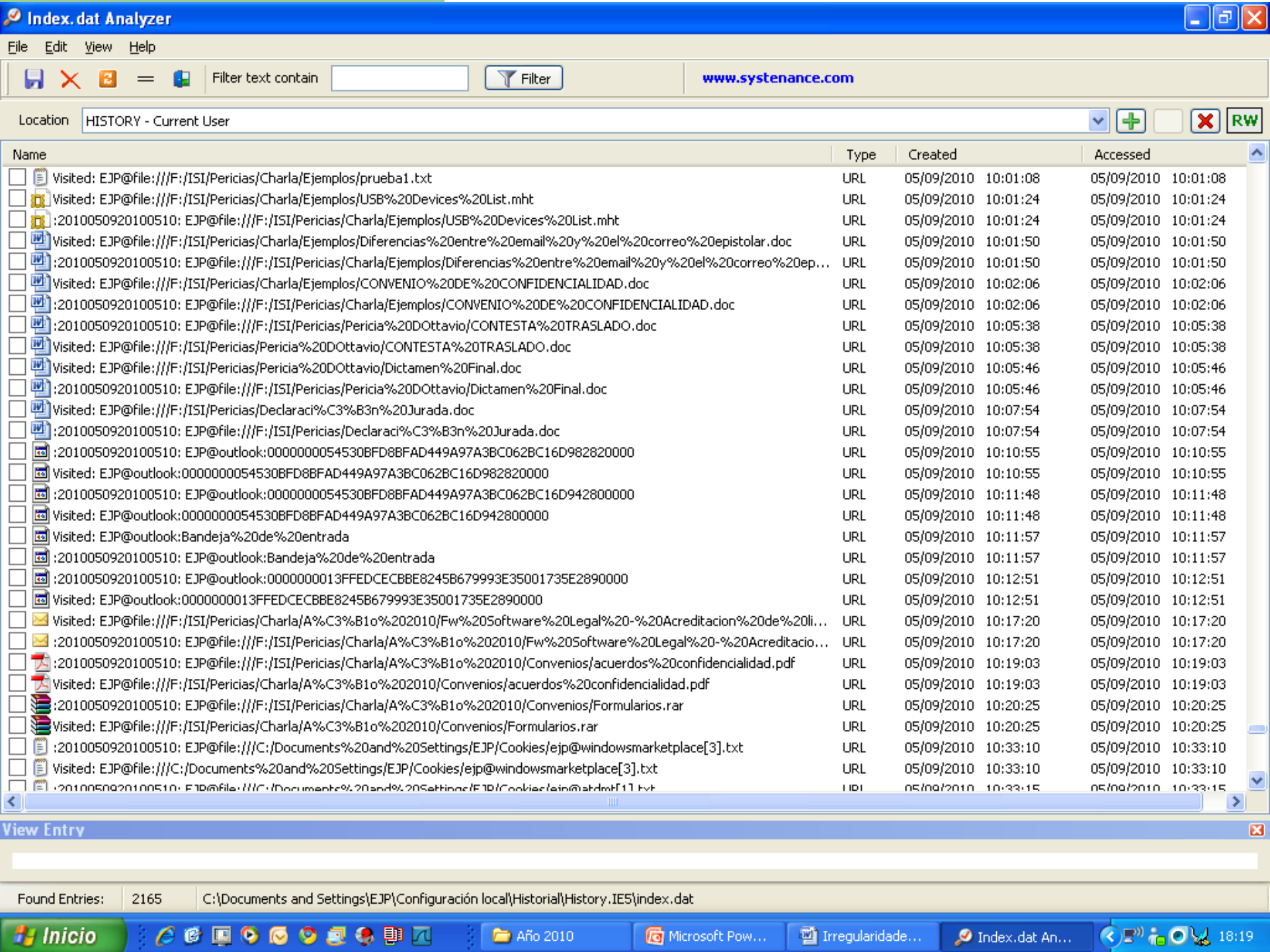
- Identificar correctamente toda la evidencia. Rotular el hardware con los siguientes datos:
  - Para computadoras, notebooks, palms, celulares, etc.: N° del Expediente Judicial, Fecha y Hora, Número de Serie, Fabricante, Modelo.
  - Para DVDs, CDs, Diskettes, discos Zip, etc: almacenarlos en conjunto en un sobre antiestático, indicando N° del Expediente Judicial, Tipo (DVDs, CDs, Diskettes, discos Zip, etc.) y Cantidad, marca y nro de serie.

LOG

¿Que es un log? Es un archivo que registra movimientos y actividades de un determinado programa y es utilizado como mecanismo de control y estadística. Es un registro de eventos durante un periodo de tiempo en particular. Es usado para registrar datos o información sobre quien, que, cuando, donde y por que un evento ocurre para un dispositivo en particular o aplicación.


Administración de equipos
Archivo Acción Ver Ventana Ayuda
Administración del equipo (l
Herramientas del sistem
Visor de sucesos
Aplicación
Seguridad
Sistema
Carpetas compartic
Usuarios locales y g
Registros y alertas
Administrador de di
Almacenamiento
Medios de almacena
Desfragmentador d
Administración de d
Servicios y Aplicaciones
Tipo Fecha Hora Origen Categoría Suceso Usuario Equi
Información 18/05/2008 17:33:58 Service Control Manager Ninguno 7036 No disponible PC-E
Advertencia 18/05/2008 17:33:34 Print Ninguno 20 SYSTEM PC-E
Información 18/05/2008 17:29:29 Service Control Manager Ninguno 7036 No disponible PC-E
Información 18/05/2008 17:20:23 Service Control Manager Ninguno 7036 No disponible PC-E
Información 18/05/2008 17:20:17 Service Control Manager Ninguno 7036 No disponible PC-E
Información 18/05/2008 17:20:16 Service Control Manager Ninguno 7035 SYSTEM PC-E
Información 18/05/2008 17:17:57 Service Control Manager Ninguno 7036 No disponible PC-E
Información 18/05/2008 17:17:57 Service Control Manager Ninguno 7035 SYSTEM PC-E
Información 18/05/2008 17:17:01 Service Control Manager Ninguno 7036 No disponible PC-E
Información 18/05/2008 17:13:02 Service Control Manager Ninguno 7036 No disponible PC-E
Información 18/05/2008 17:12:55 Service Control Manager Ninguno 7036 No disponible PC-E
Información 18/05/2008 17:12:55 Service Control Manager Ninguno 7035 SYSTEM PC-E
Información 18/05/2008 17:12:33 Service Control Manager Ninguno 7036 No disponible PC-E
Información 18/05/2008 17:12:27 Service Control Manager Ninguno 7036 No disponible PC-E
Información 18/05/2008 17:12:27 Service Control Manager Ninguno 7035 SYSTEM PC-E
Información 18/05/2008 17:02:05 Service Control Manager Ninguno 7036 No disponible PC-E
Información 18/05/2008 17:02:04 Service Control Manager Ninguno 7035 SYSTEM PC-E
Información 18/05/2008 17:02:04 Service Control Manager Ninguno 7036 No disponible PC-E
Información 18/05/2008 17:02:04 Service Control Manager Ninguno 7035 SYSTEM PC-E
Advertencia 18/05/2008 17:01:41 Print Ninguno 20 SYSTEM PC-E
Información 18/05/2008 17:01:01 Service Control Manager Ninguno 7036 No disponible PC-E
Información 18/05/2008 17:01:01 Service Control Manager Ninguno 7035 SYSTEM PC-E
Información 18/05/2008 16:51:43 W32Time Ninguno 35 No disponible PC-E
Error 18/05/2008 16:55:38 Dhcp Ninguno 1000 No disponible PC-E
Advertencia 18/05/2008 16:55:38 Dhcp Ninguno 1003 No disponible PC-E
Inicio
D...
T...
Mi...
D...
P...
D...
A...
18:20


Documentos recientes
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás
Búsqueda
Carpetas
Dirección C:\Documents and Settings\EJP\Recent
Carpetas
Disco local (C:)
Archivos de programa
Documents and Settings
All Users
Default User
EJP
Application Data
Configuración local
Application Data
Archivos temporales de Interr
Datos de programa
Historial
hace 3 semanas
La semana pasada
Hoy
Temp
msohtml
msohtml1
nodtmpb
VBE
Cookies
Datos de programa
Documentos recientes
Entorno de red
b67d2c6bf2
Charla
Contesta.dc
Definiciones
Desktop.ini
Dictamen fir
Disco extraí
Disco local (
InfoTool.txt
Install
Log
Lupo.mdb
MNDPI.pdf
ONetConfig
Pericia Barr
Pericia Gaita
Pericia Tecn
programa_ir
ProponeFec
prueba1.txt
SID_13.pdf
SopCast.zip
UsrClass.da
Windows
Propiedades de Contesta.doc
General
Acceso directo
Contesta.doc
Tipo de archivo: Acceso directo
Se abre con: Microsoft Office Wor
Cambiar...
Ubicación: C:\Documents and Settings\EJP\Recent
Tamaño: 576 bytes (576 bytes)
Tamaño en disco: 4,00 KB (4.096 bytes)
Creado: Domingo, 20 de Abril de 2008, 19:14:45
Modificado: Domingo, 20 de Abril de 2008, 19:18:37
Último acceso: Hoy, 26 de Abril de 2008, 16:01:49
Atributos: Sólo lectura Oculto
Opciones avanzadas...
Aceptar
Cancelar
Aplicar
Inicio
Log
Mi PC
Document...
Definicione...
16:03


Index.dat Analyzer
File Edit View Help
Filter text contain
Filter
www.systenance.com
Location
HISTORY - Current User
RW
Name Type Created Accessed
Visited: EJP@file:///F:/ISI/Pericias/Charla/Ejemplos/prueba1.txt URL 05/09/2010 10:01:08 05/09/2010 10:01:08
Visited: EJP@file:///F:/ISI/Pericias/Charla/Ejemplos/USB%20Devices%20List.mht URL 05/09/2010 10:01:24 05/09/2010 10:01:24
:2010050920100510: EJP@file:///F:/ISI/Pericias/Charla/Ejemplos/USB%20Devices%20List.mht URL 05/09/2010 10:01:24 05/09/2010 10:01:24
Visited: EJP@file:///F:/ISI/Pericias/Charla/Ejemplos/Diferencias%20entre%20email%20y%20el%20correo%20epistolar.doc URL 05/09/2010 10:01:50 05/09/2010 10:01:50
:2010050920100510: EJP@file:///F:/ISI/Pericias/Charla/Ejemplos/Diferencias%20entre%20email%20y%20el%20correo%20ep... URL 05/09/2010 10:01:50 05/09/2010 10:01:50
Visited: EJP@file:///F:/ISI/Pericias/Charla/Ejemplos/CONVENIO%20DE%20CONFIDENCIALIDAD.doc URL 05/09/2010 10:02:06 05/09/2010 10:02:06
:2010050920100510: EJP@file:///F:/ISI/Pericias/Charla/Ejemplos/CONVENIO%20DE%20CONFIDENCIALIDAD.doc URL 05/09/2010 10:02:06 05/09/2010 10:02:06
:2010050920100510: EJP@file:///F:/ISI/Pericias/Pericia%20DOttavio/CONTESTA%20TRASLADO.doc URL 05/09/2010 10:05:38 05/09/2010 10:05:38
Visited: EJP@file:///F:/ISI/Pericias/Pericia%20DOttavio/CONTESTA%20TRASLADO.doc URL 05/09/2010 10:05:38 05/09/2010 10:05:38
Visited: EJP@file:///F:/ISI/Pericias/Pericia%20DOttavio/Dictamen%20Final.doc URL 05/09/2010 10:05:46 05/09/2010 10:05:46
:2010050920100510: EJP@file:///F:/ISI/Pericias/Pericia%20DOttavio/Dictamen%20Final.doc URL 05/09/2010 10:05:46 05/09/2010 10:05:46
Visited: EJP@file:///F:/ISI/Pericias/Declaraci%C3%B3n%20Jurada.doc URL 05/09/2010 10:07:54 05/09/2010 10:07:54
:2010050920100510: EJP@file:///F:/ISI/Pericias/Declaraci%C3%B3n%20Jurada.doc URL 05/09/2010 10:07:54 05/09/2010 10:07:54
:2010050920100510: EJP@outlook:0000000054530BFD8BFAD449A97A3BC062BC16D982820000 URL 05/09/2010 10:10:55 05/09/2010 10:10:55
Visited: EJP@outlook:0000000054530BFD8BFAD449A97A3BC062BC16D982820000 URL 05/09/2010 10:10:55 05/09/2010 10:10:55
:2010050920100510: EJP@outlook:0000000054530BFD8BFAD449A97A3BC062BC16D942800000 URL 05/09/2010 10:11:48 05/09/2010 10:11:48
Visited: EJP@outlook:0000000054530BFD8BFAD449A97A3BC062BC16D942800000 URL 05/09/2010 10:11:48 05/09/2010 10:11:48
Visited: EJP@outlook:Bandeja%20de%20entrada URL 05/09/2010 10:11:57 05/09/2010 10:11:57
:2010050920100510: EJP@outlook:Bandeja%20de%20entrada URL 05/09/2010 10:11:57 05/09/2010 10:11:57
:2010050920100510: EJP@outlook:0000000013FFEDCECBBE8245B679993E35001735E2890000 URL 05/09/2010 10:12:51 05/09/2010 10:12:51
Visited: EJP@outlook:0000000013FFEDCECBBE8245B679993E35001735E2890000 URL 05/09/2010 10:12:51 05/09/2010 10:12:51
Visited: EJP@file:///F:/ISI/Pericias/Charla/A%C3%B1o%202010/Fw%20Software%20Legal%20-%20Acreditacion%20de%20li... URL 05/09/2010 10:17:20 05/09/2010 10:17:20
:2010050920100510: EJP@file:///F:/ISI/Pericias/Charla/A%C3%B1o%202010/Fw%20Software%20Legal%20-%20Acreditacio... URL 05/09/2010 10:17:20 05/09/2010 10:17:20
:2010050920100510: EJP@file:///F:/ISI/Pericias/Charla/A%C3%B1o%202010/Convenios/acuerdos%20confidencialidad.pdf URL 05/09/2010 10:19:03 05/09/2010 10:19:03
Visited: EJP@file:///F:/ISI/Pericias/Charla/A%C3%B1o%202010/Convenios/acuerdos%20confidencialidad.pdf URL 05/09/2010 10:19:03 05/09/2010 10:19:03
:2010050920100510: EJP@file:///F:/ISI/Pericias/Charla/A%C3%B1o%202010/Convenios/Formularios.rar URL 05/09/2010 10:20:25 05/09/2010 10:20:25
Visited: EJP@file:///F:/ISI/Pericias/Charla/A%C3%B1o%202010/Convenios/Formularios.rar URL 05/09/2010 10:20:25 05/09/2010 10:20:25
:2010050920100510: EJP@file:///C:/Documents%20and%20Settings/EJP/Cookies/ejp@windowsmarketplace[3].txt URL 05/09/2010 10:33:10 05/09/2010 10:33:10
Visited: EJP@file:///C:/Documents%20and%20Settings/EJP/Cookies/ejp@windowsmarketplace[3].txt URL 05/09/2010 10:33:10 05/09/2010 10:33:10
View Entry
Found Entries: 2165
C:\Documents and Settings\EJP\Configuración local\Historial\History.IE5\index.dat
Inicio
Año 2010
Microsoft Pow...
Irregularidade...
Index.dat An...
18:19

Correo electrónico – Tipos de servidores

- El SMTP (Simple Mail Transfer Protocol) es el proceso de transferencia de archivos más usado y utiliza TCP/IP como medio de transporte, abre una conexión con el destino, le informa al otro servidor para quién es el mensaje y lo transfiere. Es el servidor de correo saliente.

- El POP es un protocolo que está diseñado para permitir al usuario, de manera personalizada, leer el correo electrónico almacenado en un servidor.

- Con las cuentas POP3, el usuario tiene control físico de sus archivos de correo y puede bajar ese correo a través de un cliente del tipo Outlook. También suelen tener asociado un servicio de webmail, que permite chequear la casilla de correo desde cualquier computadora. Hay incluso sitios que permiten hacer esto desde el browser, ingresando la dirección de e-mail y la contraseña para acceder a ella.

- Esto es diferente de las cuentas IMAP (Interactive Mail Access Protocol), en donde su correo siempre permanece en el servidor. Un ejemplo de IMAP. sería algo como el Hotmail, donde el usuario se conecta a través de un buscador. La diferencia con las POP3 es que los mensajes se almacenan en las unidades del servidor y no en las del usuario.

Correo electrónico - Clasificación

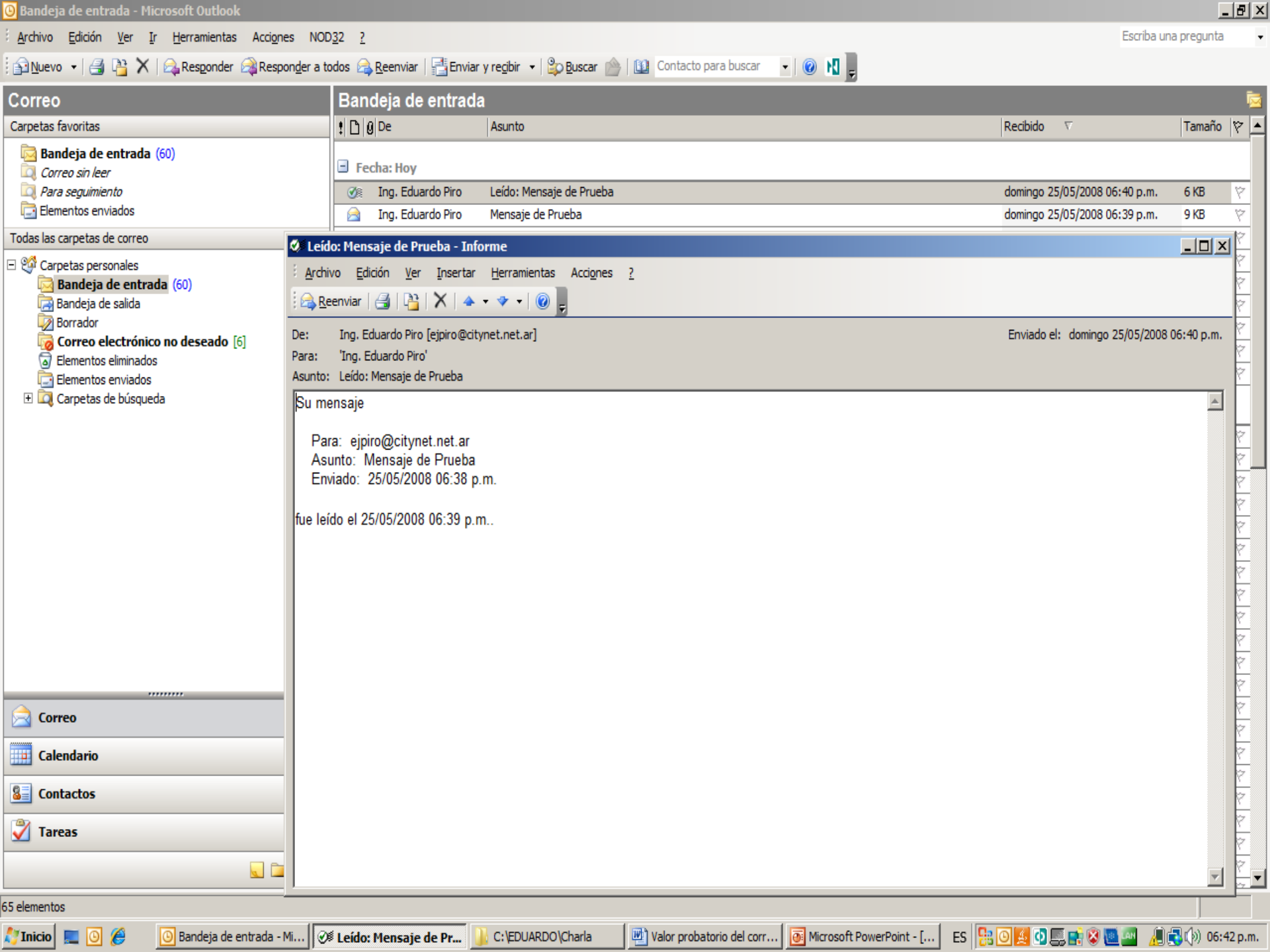
- Mails pagos y gratuitos
- Mails POP3 y Webmail (IMAP)
- Mails con dominio propio y sin dominio propio
- Clientes de correo
  - Outlook (.pst)
  - Outlook Express (.dbx)
  - Windows Live Mail

Como Preconstituir pruebas con correo electrónico

La mejor prueba de que se envío un mail, es que el destinatario nos conteste el mismo mail, en el cual recibimos por lo general el texto original en la parte inferior del mismo en nuestra bandeja de entrada constituyéndose en una especie de acuse de recibo.

Configurar el programa de correo para que solicite confirmación de la recepción del mensaje, para lo cual deberíamos archivar con fines probatorios, tanto el mensaje enviado, como la confirmación de recepción y lectura del mensaje, que son dos mails diferentes.

La Parte negativa de este método, es que la solicitud de confirmación de correo puede no ser aceptada a propósito por el receptor del mail


Bandeja de entrada - Microsoft Outlook
Archivo Edición Ver Ir Herramientas Acciones NOD32 ?
Escriba una pregunta
Nuevo Responder Responder a todos Reenviar Enviar y recibir Buscar Contacto para buscar
Correo
Carpetas favoritas
Bandeja de entrada (60)
Correo sin leer
Para seguimiento
Elementos enviados
Todas las carpetas de correo
Carpetas personales
Bandeja de entrada (60)
Bandeja de salida
Borrador
Correo electrónico no deseado [6]
Elementos eliminados
Elementos enviados
Carpetas de búsqueda
Correo
Calendario
Contactos
Tareas
Bandeja de entrada
De Asunto Recibido Tamaño
Fecha: Hoy
Ing. Eduardo Piro Leído: Mensaje de Prueba domingo 25/05/2008 06:40 p.m. 6 KB
Ing. Eduardo Piro Mensaje de Prueba domingo 25/05/2008 06:39 p.m. 9 KB
Leído: Mensaje de Prueba - Informe
Archivo Edición Ver Insertar Herramientas Acciones ?
Reenviar
De: Ing. Eduardo Piro [ejpiro@citynet.net.ar]
Enviado el: domingo 25/05/2008 06:40 p.m.
Para: 'Ing. Eduardo Piro'
Asunto: Leído: Mensaje de Prueba
Su mensaje
Para: ejpiro@citynet.net.ar
Asunto: Mensaje de Prueba
Enviado: 25/05/2008 06:38 p.m.
fue leído el 25/05/2008 06:39 p.m..
65 elementos
Inicio
Bandeja de entrada - Mi...
Leído: Mensaje de Pr...
C:\EDUARDO\Charla
Valor probatorio del corr...
Microsoft PowerPoint - [...
ES
06:42 p.m.

Como Preconstituir pruebas con correo electrónico

Si existen otros mensajes de datos, esto podrá ser utilizado para indicar autoría y uso de una cuenta determinada.

Incluir en los contratos la validez de notificaciones vía correo electrónico identificando las cuentas de correo determinadas para que contractualmente se reconozca la identidad del usuario de la cuenta de correo.

Autenticidad de un mail

Debemos analizar cada caso en particular

¿Cómo podemos saber si un mail es auténtico o desde que PC fue enviado?

Por medio de los llamados

"encabezados de Internet"

Correo electrónico – Encabezados de Internet

Return-Path: <ingenieriainformatica@hotmail.com>
Delivered-To: data-k87557@datamarkets.com.ar
Received: (qmail 16943 invoked from network); 25 May 2008 23:23:58 -0000
Received: from unknown (HELO postino2.prima.com.ar) (200.42.0.133)
  by cumeil14.prima.com.ar with SMTP; 25 May 2008 23:23:58 -0000
Received: (qmail 31787 invoked by alias); 25 May 2008 23:23:58 -0000
Delivered-To: CITYNET-ejpiro@citynet.net.ar
Received: (qmail 31778 invoked from network); 25 May 2008 23:23:57 -0000
Received: from blu0-omc1-s14.blu0.hotmail.com (65.55.116.25)
  by postino2.prima.com.ar with SMTP; 25 May 2008 23:23:57 -0000
Received: from BLU134-W16 ([65.55.116.9]) by blu0-omc1-s14.blu0.hotmail.com with Microsoft
      SMTPSVC(6.0.3790.3959); Sun, 25 May 2008 16:23:55 -0700
Message-ID: <BLU134-W16E0C393E1CC6CC08C3819BDC30@phx.gbl>
Return-Path: ingenieriainformatica@hotmail.com
Content-Type: multipart/alternative;
      boundary="_c86d9dff-9a67-4ff8-8763-8ec1614119c6_"
X-Originating-IP: [190.189.0.140]
From: "Ing. Eduardo Piro" <ingenieriainformatica@hotmail.com>
To: Eduardo Piro <ejpiro@citynet.net.ar>
Subject: Esto es una prueba
Date: Sun, 25 May 2008 23:23:55 +0000
Importance: Normal
MIME-Version: 1.0
X-OriginalArrivalTime: 25 May 2008 23:23:56.0034 (UTC) FILETIME=[66F33E20:01C8BEBE]

Características necesarias para la admisibilidad y eficacia probatoria del documento electrónico

- Inalterabilidad. Debe revestir el carácter de permanente. El temor sobre la posibilidad de reutilización de los soportes informáticos disminuye su seguridad y confiabilidad.

- Autenticidad e integridad. Un documento es auténtico cuando no ha sufrido alteraciones tales que varíen su contenido.

- Durabilidad. Se refiere al soporte. Que sea estable en el tiempo, y que no pueda ser alterada por una intervención externa sin dejar huella.

- Identidad de las partes autoras de los mensajes. La firma como elemento de seguridad documental.
  - Ley de firma digital, firma electrónica y documento digital. Se sancionó la ley 25506 de Firma Digital, necesaria para validar la autenticidad, integridad y el no repudio del llamado documento electrónico, reglamentada en decreto 2628/2002.
  - Uno de los aspectos más trascendentes es la equiparación entre "firma manuscrita" y "firma digital". El art. 3 reza textualmente: "Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia".

Vinculación a lo Laboral – Seguridad Informática

QUE ES SEGURIDAD DE LA INFORMACION

La seguridad informática consiste en asegurar todos los recursos informáticos (material físico e informáticos, programas, etc.) de una organización de la manera que se decidió en las políticas y que el acceso a la información solo sea posible a las personas que se encuentre acreditadas y que estén dentro de los limites de autorización.

No es lo mismo seguridad, auditoria o pericias informáticas.
Un experto en seguridad no lo es en pericias.

Vinculación al Derecho Laboral – Factores de control

1) **Disponibilidad de la información:** La disponibilidad implica que la información debe ser accesible en todo momento para aquellos que están expresamente autorizados. Los controles que aseguran la disponibilidad de la información son políticas y procedimientos de respaldo, planes de contingencia, tecnologías de redundancia y alta disponibilidad.

2) **Integridad de la información:** La información debe mantenerse protegida de modificaciones no autorizadas tanto de usuarios como procesos autorizados como no autorizados, de tal manera que sea consistente tanto externa como internamente. Los controles que permiten mantener la integridad de la información son sistemas antivirus, registros de auditoría (logs), softwares de encripción y desencripción, etc.

3) **Confidencialidad de la información:** Implica que solo aquellos usuarios o procesos explícitamente autorizados acceden a los activos de información cuando ellos lo requieran. Algunos controles y tecnologías que se pueden mencionar son: firewalls, listas de control de acceso, etc.

Ley 26388: Delitos Informáticos

Ahora, el Código Penal contempla los siguientes tipos de delitos:

- Distribución y tenencia con fines de pornografía infantil
- Violación de correo electrónico
- Acceso ilegítimo a sistemas informáticos
- Daño informático y distribución de virus
- Daño informático agravado
- Interrupción de comunicaciones
- Esta Ley NO regula el Spam que ya era ilegal bajo el art. 27 de la Ley 25.326 de Habeas Data. Eventualmente un envío masivo de correos que obstruya un sistema informático podría llegar a ser considerado como delito (interrupción de comunicaciones).

Ley 26388: Delitos Informáticos

- Será reprimido con prisión de quince (15) días a seis (6) meses **el que abriere o accediere indebidamente a una comunicación electrónica**, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; **o se apoderare indebidamente de una comunicación electrónica**, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; **o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida**. En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

Vinculación al Derecho Laboral - Login

Cada usuario de un sistema se identifica con un nombre o palabra único. Esta palabra o nombre desde el punto de vista técnico es denominado "*Login*", el cual, es como una especie de pseudónimo electrónico.

La asignación de logins para cada usuario, tiene la finalidad de poder identificar quien, como, donde y cuando se realizaron actividades en un sistema, lo cual es fundamental a la hora de establecer responsabilidades sobre hechos jurídicos informáticos

El reconocimiento por escrito de la asignación de logins de usuario, establece la conexión entre la identidad legal del usuario y la identidad electrónica o virtual, facilitando las demás pruebas de los hechos jurídicos informáticos.

Vinculación al Derecho Laboral

- Acuerdos de confidencialidad
  - Login (responsabilidades sobre el uso de mi cuenta de usuario)
  - No divulgar cualquier información, guardar absoluta reserva
  - Toda información a la que se acceda es de propiedad de la Organización
  - Se considera información confidencial (procedimientos, rutinas, códigos fuentes, e-mail, archivos electrónicos, programas, sistemas, software, documentos en cualquier soporte, etc.)
- Normativa sobre la utilización de los recursos
  - Correo electrónico (mensajes con sexo, racismo, creencias, etc., correos masivos, cadenas, etc.)
  - USB o Diskettes (infectar con virus, copia de información, etc)
  - Internet (descargas, virus, navegación excesiva, páginas desconocidas, juegos, facebook, msn, etc.)
  - Telefonía fija y móvil (duración conversaciones, mensajes de texto, etc)

Vinculación al Derecho Laboral – Recomendaciones

- Utilizar los recursos únicamente para fines laborales.
- Toda información almacenada y/o transmitida utilizando los equipos u otros medios provistos por la Empresa, es propiedad de ésta y está sujeta a revisión y/o control en cualquier momento.
- El correo electrónico podrá ser archivado para futuras referencias o destruido a discreción del administrador.
- Dejar en claro que todas las actividades de los usuarios en los sistemas pueden ser monitoreadas y auditadas.
- Se recomienda utilizar cuentas de correo por funciones o sectores: compras@miempresa.com.ar, info, ventas, administración, etc.
- Las funciones de cada dependiente en el área de informática (como en el resto de las áreas), deben estar claramente estipuladas y definidas, y los equipos deben ser de uso restringido a uno solo, por período de tiempo, de forma tal que quede evidente quien es el responsable cuando ocurre un incidente.

Constataciones de Software

- Software legal

  Intimaciones:

  - Mail
  - Telefónicas
  - Correo
  - Auditorías
- BSA (Business Software Alliance)
  - Aseguramiento de pruebas / Orden de allanamiento
- Microsoft
  - Ámbito penal y civil

Licenciamiento de software

- Tener adquiridas licencias no implica de tener en regla o licenciados los equipos
- Evitar multas por desinstalación de software
- Realizar una auditoría de los equipos / servidores
- Asesorarse por especialistas en licenciamiento
  - Que tipo de licencias conviene adquirir (OEM / OLP / etc)
  - Utilización de software libre (Linux / OpenOffice / etc)
  - Limpieza de los equipos (temporales, log, registro de windows)
  - Busqueda de instaladores, cracks, keygen, seriales, etc.
  - Papelería en orden

INFORMATICA FORENSE
PERICIAS INFORMATICAS

Ing en Sistemas Informáticos
Eduardo J. Piro
www.ejpinformatica.com.ar
ejpiro@overnetsa.com.ar
Cel: 156911550

Preguntas