Lección 17: Datos personales. Guía de seguridad para usuarios

intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Dña. María Goretti López Deltell
goretti.lopez@madrid.org

Agencia de Protección de Datos de la Comunidad de Madrid

Algunos casos

La Policía investiga el robo de datos personales de los escoltas de Zapatero

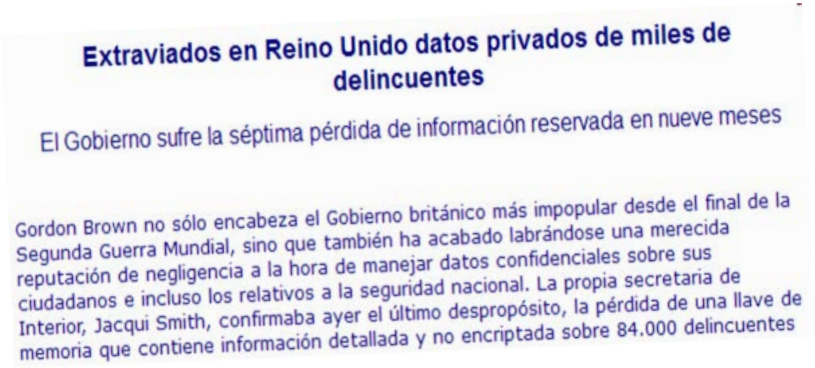
El grupo de 'hackers' Anonymus publica en la Red un archivo con las identidades de 30 guardaespaldas

16.09.11 - 01:42 - M. BALÍN | MADRID.

Detenido tras hallar contratos en un contenedor

- La pérdida de los documentos con datos personales y números de cuenta bancaria de clientes de Orange podría conllevar una sanción de hasta 300.000 euros para la tienda que los "extravió"

JOAQUÍN GIL / IGNACIO FRANCIA | | 12 ABR 2011 - 21:43 CET



Extraviados en Reino Unido datos privados de miles de delincuentes

El Gobierno sufre la séptima pérdida de información reservada en nueve meses

Gordon Brown no sólo encabeza el Gobierno británico más impopular desde el final de la Segunda Guerra Mundial, sino que también ha acabado labrándose una merecida reputación de negligencia a la hora de manejar datos confidenciales sobre sus ciudadanos e incluso los relativos a la seguridad nacional. La propia secretaria de Interior, Jacqui Smith, confirmaba ayer el último despropósito, la pérdida de una llave de memoria que contiene información detallada y no encriptada sobre 84.000 delincuentes

Gmail pierde correos, etiquetas y contactos de cientos de usuarios

28/02/2011 | Por MuyInternet | 5 comentarios

Me gusta Twittear 27 +1 0

Entre **150.000 y 500.000 clientes** de Gmail -la cifra es no se ha determinado oficialmente- se han quedado **sin correos, etiquetas, contactos** y otros datos relacionado con la configuración personal este fin de semana. Los chicos de Google están revisando este error que afecta, según la compañía, a un 0,08% de los usuarios de Gmail.

Una cantidad indeterminada de usuarios de Gmail han reportado en los blogs de soporte pérdida de datos del cliente sucedido este fin de semana. El fallo afecta a la **pérdida de correos electrónicos, carpetas, etiquetas, contactos o configuración personal de Gmail**.

Hallan en la basura datos confidenciales de afiliados del PP de Benalmádena

La caja contiene información personal de miembros del partido, cuentas bancarias y un censo electoral del municipio

05.02.10 - 01:37 - FRANCISCO JIMÉNEZ | BENALMÁDENA.

El factor humano

Ley Orgánica 15 / 1999
Artículo 9.

" El responsable del fichero . . . deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos . . . habida cuenta de los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural."

- Eslabón débil de la cadena de seguridad
- Los datos están manejados por personas
- Ninguna técnica puede proteger frente al uso malintencionado o frente a la irresponsabilidad inconsciente por parte de las personas autorizadas.
- Hay que invertir tanto o más esfuerzo y recursos en asegurar éste eslabón como en implantar las últimas técnicas de seguridad.

El engaño para la obtención de datos

Social engineering

- No hace falta ser un hacker informático para obtener fraudulentamente datos protegidos. Esto lo saben muy bien los detectives profesionales y los periodistas.
- A veces el simple y clásico “engaño” a un empleado puede ser más efectivo.
- Es tan importante este método que los anglosajones también han inventado un término para él, el “*social engineering*”.
- Este método, a veces primitivo, puede presentar muchas formas:
  - El “*phishing*”, que consiste en enviar emails falsos en donde simulando que se emiten desde la central se piden las claves de acceso con la excusa de que se han perdido.
  - Suplantación de identidad de un técnico de la central
  - Suplantación de identidad por teléfono de la secretaria de un director que pide urgentemente sus claves de acceso

Los listados

- Es muy fácil imprimir. Diariamente se producen miles de páginas fallidas que acaban en la basura.
- En las organizaciones con cierta conciencia ecológica ese papel se recicla. ¡Pero eso no impide que antes caigan en manos inapropiadas que puedan hacer mal uso de esa información!
- Los contenedores de papel, o las empresas de reciclaje son una de las principales fuentes de información para los que quieren acceder a datos confidenciales.

¿Qué hacer con los listados?

1. Imprimir lo menos posible. La vida de muchos documentos puede y debe ser meramente electrónica. Se escribe en un ordenador, se envía por email a otro, se lee, y se archiva o se borra. Sin papel.
2. En las empresas u organizaciones, tener una máquina destructora de documentos para eliminar al menos los documentos más confidenciales.
3. Exigir a las empresas de reciclado una garantía de destrucción de nuestros impresos, y una garantía de custodia hasta su destrucción. Ya hay muchas compañías que ofrecen este tipo de contratos.

Los soportes removibles: CDs y DVDs

- En un CD caben ¡200.000 folios! (600 Mb a 3Kb por folio).
- Con frecuencia se utilizan para hacer copias de seguridad, lo que hace que sus contenidos sean más peligrosos.
- La popularización de las grabadoras de CDs o DVDs hace que cada vez proliferen más estos soportes en los cubos de basura.

¿Qué hacer con los CDs y DVDs?

- Es importante etiquetarlos para conocer su contenido
- A los desechados se les debe dar un tratamiento similar al de las pilas y baterías.
- Como ocupan poco se pueden ir acumulando en algún lugar seguro de la oficina, y periódicamente entregarlos a una empresa de reciclaje que garantice su destrucción.
- Toda organización debe tener un protocolo sobre como deshacerse de forma segura de estos peligrosísimos soportes.

Los ordenadores obsoletos

- Se calcula que la vida media de un ordenador es actualmente de unos tres años.
- Cada año se retiran a reciclaje o reventa millones de ordenadores.
- Todos ellos llevan uno o varios discos duros con, como mínimo, varias decenas de gigabytes de información.

¿Qué hacer con los ordenadores obsoletos?

- NUNCA deben entregarse para ser donados o revendidos, sin haber sido previamente "sanitizados".
- "Sanitizar" un ordenador es borrar los datos de sus discos duros.
- Pero no basta con hacer un borrado lógico con un comando del sistema operativo.
- Un formateado del disco puede hacer más difícil la recuperación de los datos a un principiante pero no a un experto.
- Existen programas que literalmente machacan los bits de los discos con sucesivas reescrituras de ceros o unos, para hacerlos ilegibles a cualquiera.

Borrado de discos y soportes

- El mejor método de borrado de discos y soportes informáticos es su destrucción física cuando eso sea posible.
- Si no es posible, o se quiere respetar el soporte para su uso posterior, se debe proceder al borrado de sus datos.
- Por eso existen programas de borrado que sobreescriben los datos para impedir su recuperación.
- Para obtener programas de borrado basta con entrar en Google y buscar por “disc eraser”.

Empresas de destrucción de soportes y documentación

- Existen centenares de empresas en España.
- Se debe exigir un contrato que garantice la destrucción confidencial de los datos. Estos contratos deben de cumplir el Artículo 12 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (LOPD).
- La destrucción puede ser in situ o mediante recogida en contenedores metálicos sellados.
- Deben entregar un certificado que garantice la destrucción de la documentación según las normas acordadas.

Dispositivos portátiles y de almacenamiento

		Factor binario
Bytes	B	$2^0 = 1$
KiloBytes	Kb	$2^{10} = 1024$
MegaBytes	Mb	$2^{20} = 1\,048\,576$
GigaBytes	Gb	$2^{30} = 1\,073\,741\,824$
TeraBytes	Tb	$2^{40} = 1\,099\,511\,627\,776$
PetaBytes	Pb	$2^{50} = 1\,125\,899\,906\,842\,624$
ExaBytes	Eb	$2^{60} = 1\,152\,921\,504\,606\,846\,976$
ZettaBytes	Zb	$2^{70} = 1180591620717411303424$
YottaBytes	Yb	$2^{80} = 1208925819614629174706176$

- Un pendrive, un DVD o un portátil puede almacenar decenas de Gigabytes, es decir decenas de miles de millones de caracteres.
- En cualquiera de esos dispositivos cabría una información de mil caracteres (1 página) de los 47 millones de españoles.

- SON UN PELIGRO. Por su pequeñez, facilidad de pérdida o hurto y enorme capacidad.
- NUNCA se debe almacenar datos protegidos en esos dispositivos si no están cifrados.
- Los DVDs que se utilicen como copias de respaldo son aún más peligrosos porque contienen TODA la información de un servidor o PC.

La solución: el cifrado

El cifrado de datos es un proceso sencillo e inmediato en cualquier ordenador actual.

En Windows:

- **Botón derecho sobre el archivo**
- **Propiedades avanzadas**
- **Cifrar**

En un servidor u otro sistema consultar con el soporte técnico

Impide la lectura de los datos desde cualquier otro ordenador que no contenga su clave secreta de cifrado.

- Es la garantía de que si nos roban o perdemos el dispositivo o portátil, nadie podrá acceder a los datos protegidos.
- ¡CÍFRALO!, si lo pierdes o te lo roban sólo perderás el hardware, no tu cuenta corriente o tu intimidad.

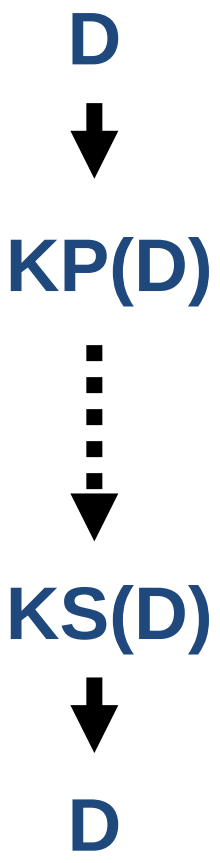
Protección física de dispositivos portátiles

- Evitar la proliferación de copias de datos personales en dispositivos portátiles.
- Como norma se debe prohibir el trabajo con datos personales en ordenadores portátiles.
- Aun así es usual que existan copias parciales de datos personales en portátiles, bien por la realización de determinados procesos, bien porque inadvertidamente se graban en ficheros temporales.
- Las memorias removibles portátiles, especialmente los pendrives sólo deben ser utilizadas bajo estricto control, dada su enorme peligrosidad dado su pequeño tamaño y facilidad de pérdida.
- Por eso la protección física es necesaria pero no suficiente.

Protección lógica de los dispositivos portátiles

- La protección lógica es la única realmente fiable
- El cifrado de datos y ficheros, correctamente utilizada, proporciona un método invulnerable para proteger la confidencialidad de los datos.
- Los sistemas actuales facilitan ese cifrado de forma que su uso es simple, sencillo, rápido y utilizable por cualquiera sin ningún conocimiento técnico específico.
- Por ejemplo, en Windows, basta con registrar un fichero como cifrado (botón derecho del ratón, propiedades avanzadas), para que todo lo que se grabe en él quede cifrado y sólo visible por el usuario indicado.

La criptografía asimétrica o de clave púbica



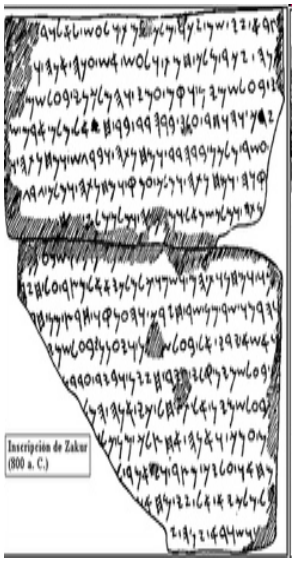
- Toda el cifrado de datos hoy en día se realiza mediante criptografía asimétrica.
- La criptografía asimétrica o de clave pública es uno de los inventos más útiles de los últimos 30 años. Sin ella no sería posible el comercio electrónico en Internet.
- Un rápido proceso, basado en el manejo de grandes números primos (hasta 1024 bits o centenares de cifras decimales), genera en pocos milisegundos dos claves emparejadas, la clave pública y la clave privada.
- La característica especial del algoritmo de cifrado (RSA o similar) asimétrico es que:

  Todo lo que se cifra con la clave pública sólo puede ser descifrado con la clave secreta asociada y ni siquiera puede descifrarse con la misma clave pública.
- Es materialmente imposible descifrar un fichero que ha sido cifrado con una clave pública sin conocer su clave privada pareja. Se calcula que harían falta millones de años de cómputo para descubrir la clave secreta correspondiente a una clave pública.

Cifrado de datos y ficheros

- Si se pierde un portátil o un pendrive que tenga sus ficheros cifrados por éste método, nadie que no tenga la clave secreta podrá acceder a los datos.
- Los ordenadores de terroristas cifrados con estos algoritmos han sido imposibles de descifrar. Desgraciadamente esta es la otra cara de la moneda.
- La clave secreta está almacenada en el propio PC pero protegida de forma que sólo el usuario autorizado tiene acceso a ella mediante una clave nemotécnica.
- Hay que tener mucho cuidado con la elección de esas claves, para que no puedan ser deducidas a partir de nuestros datos personales.

¡Hay que utilizar ficheros cifrados!



- En cualquier portátil o pendrive los ficheros deben estar cifrados.
- Es conveniente incluso cifrar todo el disco duro (mismo procedimiento, botón derecho etc..)
- El cifrado no perjudica en absoluto el rendimiento. Es simple y transparente de utilizar.
- Es la garantía de que si nos roban o perdemos el dispositivo o portátil, nadie podrá acceder a los datos protegidos.
- ¡CÍFRALO!, si lo pierdes o te lo roban sólo perderás el hardware, no tu cuenta corriente o tu intimidad.

Borrado de discos y soportes

- El mejor método de borrado de discos y soportes informáticos es su destrucción física cuando eso sea posible.
- Si no es posible, o se quiere respetar el soporte para su uso posterior, se debe proceder al borrado de sus datos.
- Por eso existen programas de borrado que sobreescriben los datos para impedir su recuperación.
- Para obtener programas de borrado basta con entrar en Google y buscar por “disc eraser”.

El Documento de Seguridad

- De obligado cumplimiento para el personal con acceso a los datos y a los sistemas de información
- Contenido:
  - Ámbito de aplicación detallando recursos protegidos
  - Medidas, normas, procedimientos, reglas y estándares
  - Funciones y obligaciones del personal
  - Estructura de los ficheros y sistemas que los tratan
  - Procedimiento de notificación, gestión y respuesta de incidencias
  - Procedimientos de realización de copias de respaldo y recuperación de datos
  - Medidas para el transporte de soportes y documentos, así como para la destrucción y reutilización.
- Continua revisión y actualización del documento
- Adecuación a la normativa vigente en cada momento
- Designación de un responsable de seguridad
- Controles periódicos a realizar para verificar su cumplimiento

intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Contacto: info@intypedia.com