

Redes Sociales y Adolescencia

**Jornadas de Información
sobre agresiones sexuales**

Baiona 25 de Noviembre del 2014

José Luis Rivas López
jlrvivas@laboratoriodeseguridadtelematica.com

Objetivos

- Conocer algunos de los peligros que entraña la gran red de redes, Internet, en el uso cotidiano de los adolescentes



Teléfonos móviles



Preguntas



- ¿Quién tiene smartphone?
- ¿Quién le deja a sus hijos/as un smartphone?
- ¿Quién usa redes sociales?

AGENDA

- **Datos interesantes**
- **Web 1.0 → Web 2.0**
- **Uso cotidiano del menor en las NNTT**
- **Perfil del acosador**
- **Peligros**
- **¿qué hacer para prevenir?**
- **Decálogo**

DATOS INTERESANTES

- **25% menores que navegan por Internet**
- **≈ 90% no utilizan ninguna protección**
- **44% se han sentido acosados alguna vez**
- **54% no han recibido formación**
- **28% entran en webs pornográficas**
- **38% acceden a contenidos violentos**
- **30% han facilitado su número de teléfono**
- **14% han concretado una cita real**
- **77% han colgado un perfil público**

FUENTE: QUÉ (11/II/2009) y PROTEGELES

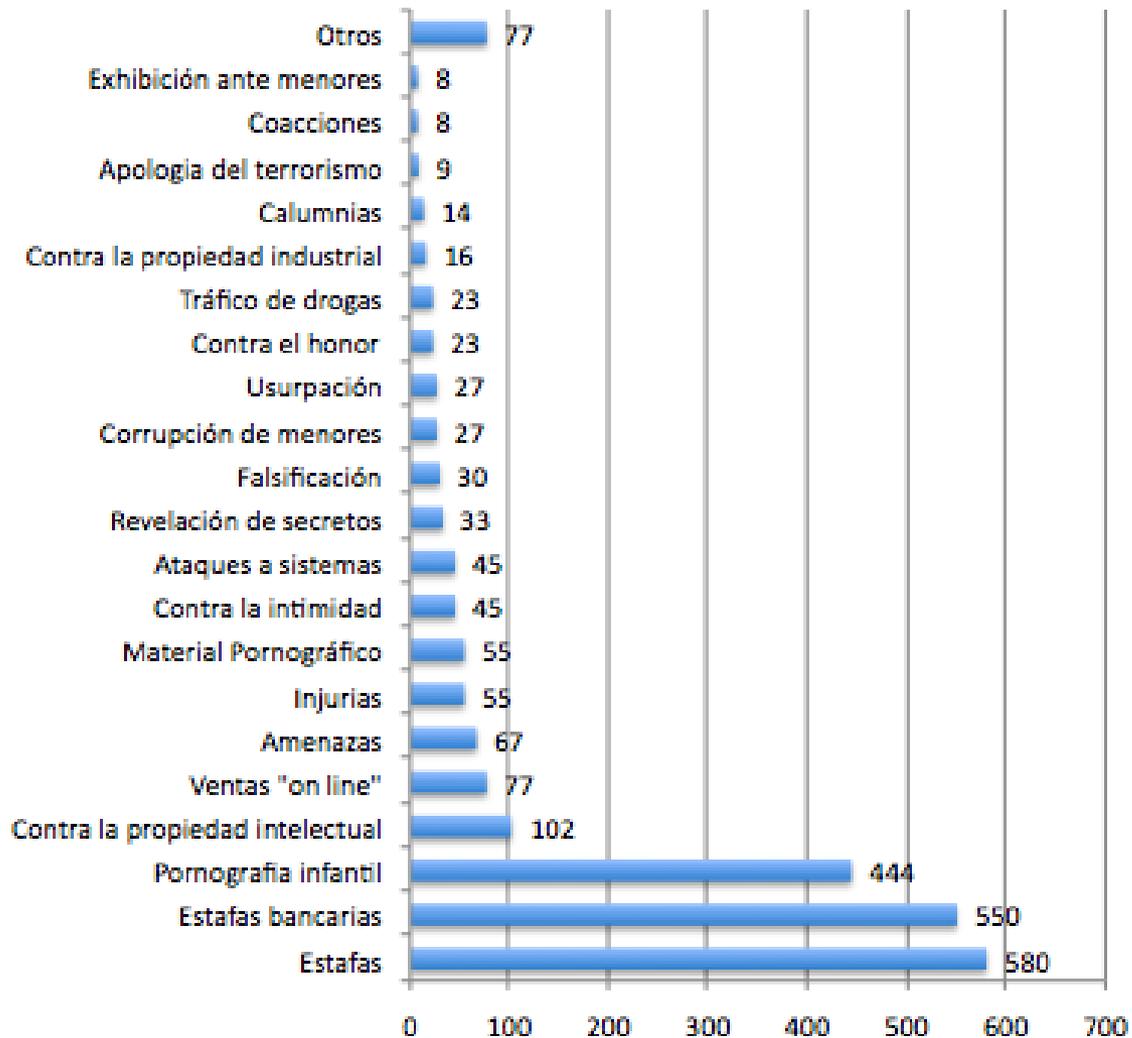
DATOS INTERESANTES II

% USO DE REDES SOCIALES

	Europa	España
Envío de mensajes	56	61
Leer mensajes	50	60
Ver fotos	43	46
Colgar fotos	31	25
Añadir amigos	24	29
Recibir alertas	23	20
Ver perfiles	15	9
Crear y colgar perfiles	13	10
Colgar videos	10	8
Participar en chats	8	6
Escribir en blogs	7	6

FUENTE: Nielsen, enero-marzo 2008 (Ciberpais 12/02/2009)

DATOS INTERESANTES III



DENUNCIAS ANTE LA P.J. FUENTE LA VOZ DE GALICIA

AGENDA

- **Introducción**
- **Datos interesantes**
- **Web 1.0 → Web 2.0**
- **Uso cotidiano del menor en las NNTT**
- **Perfil del acosador**
- **Peligros**
- **Ejemplo práctico**
- **¿qué hacer para prevenir?**
- **Decálogo**



WEB 1.0 → WEB 2.0

• **RED DE DOCUMENTOS**

• LEER

- Contenidos generado por expertos
- Comunicación unidireccional
- Sitios de información estática

• **RED SOCIAL**

• LEER Y ESCRIBIR

- Contenidos generado por los usuarios
- Comunicación multidireccional
- Sitios de información cambiante

WEB 1.0 → WEB 2.0

- Una filosofía caracterizada por:
 - Acceso libre a la información
 - Compartir conocimiento
 - Fácil publicación y libertad de expresión
 - El usuario como emisor de información y no sólo consumidor
- Muchas herramientas o recursos:
 - Publicación archivos audiovisuales (youtube, google video...)
 - Publicación de archivos de imagen (flickr, picasa)
 - Publicación de presentaciones (slideshare)
 - Publicación de espacios web personales (blogs)
 - Publicación compartida (wikis)
 - Compartición de software, musica, videos (Emule, etc)

AGENDA

- **Introducción**
- **Datos interesantes**
- **Web 1.0 → Web 2.0**
- **Uso cotidiano del menor en las NNTT**
- **Perfil del acosador**
- **Peligros**
- **¿qué hacer para prevenir?**
- **Decálogo**



USO COTIDIANO DEL MENOR EN LAS NNTT I

Jose Luis Rivas Lopez WebSite - Seguridad Telematica
http://webs.uvigo.es/jlrvivas/

JOSÉ LUIS RIVAS LÓPEZ : SEGURIDAD TELEMÁTICA

INICIO | PUBLICACIONES | I+D+i | CURSOS y CONFERENCIAS | RECURSOS | PREMIOS | PRENSA | CONTACTAR

PRÓLOGO

José Luis Rivas
INFORMÁTICO

La Universidad de Vigo organiza esta semana un curso sobre seguridad informática en el que se analizan las herramientas de protección de datos e información. José Luis Rivas dirige estas jornadas.

¿Qué se puede hacer para evitar virus informáticos? Lo más importante es instalar un antivirus, que se actualiza a diario y automáticamente siempre que el ordenador esté conectado a Internet. ¿Y si no lo está? No cabe duda que la mejor

Soy consultor, auditor y profesor de seguridad especializado en soluciones avanzadas de seguridad telemática y servicios de prevención, detección y respuesta frente a las diferentes amenazas e incidentes de seguridad que existen.

La experiencia que tengo viene avalada por el trabajo realizado durante muchos años englobando múltiples sectores (defensa, telecomunicaciones, industria, gobierno, financiero, etc) incluyendo el diseño y la revisión de arquitecturas de seguridad, realización de las políticas de uso y de seguridad, pruebas de intrusión, respuesta ante incidentes, análisis forenses, auditorías y securización de diversos y diferentes sistemas. Todo ello desde las perspectivas técnica y jurídica.

Entre mi currículum se encuentran diversas cartas de felicitación por el trabajo realizado. También he sido varias veces **jurado del reto internacional de análisis forense** realizado por los CERTS españoles y mexicano. Además de haber desarrollado las políticas de uso de RedIRIS entre otras junto a Jesus Sanz de las Heras (de RedIRIS)

Para terminar os recomiendo si estáis interesados en el análisis forense de ordenadores que os subscribáis a la lista **ANAFON** de RedIRIS de la cual soy uno de los administradores junto a Francisco Monserrat (de RedIRIS).

protección es no conectarse a Internet. Una persona que tenga su ordenador sólo para trabajar personalmente, no tiene riesgo. Sólo le podría entrar un virus por vía externa, es decir, a través de disquete, CD o un dispositivo de transporte de datos similar. Por eso, para evitar cualquier ataque lo mejor es un antivirus.

¿Padece Vigo los proble...

1.6 METODOLOGÍA Y FASES DE UN ANALISIS FORENSE

En el análisis forense nos vamos a encontrar con 3 fases bien diferenciadas a pesar que dependiendo del enfoque y del tipo que sea dicho análisis se podrá dividir en más fases.

```

graph LR
    A[Adquisición de datos] --> B[Análisis e Investigación]
    B --> C[Redacción del Informe]
    
```

Fases de un análisis forense. FIGURA 5

1.6.1 ADQUISICIÓN DE DATOS

La adquisición de datos es una de las actividades más críticas en el análisis forense. Dicha criticidad es debida a que si se realizase mal, todo el análisis e investigación posterior no sería valido debido a que estaría la información con impurezas es decir, la información que creemos que es del origen no lo es realmente.

Una vez que se ha detectado un incidente de seguridad uno de los primeros problemas del analista en la recogida de datos se resume en decir si el equipo hay que apagarlo o no. Esta decisión, aunque pueda parecer trivial, no lo es tanto, porque las consecuencias pueden ser varias: perder evidencias que estén en la memoria volátil, ver los usuarios conectados, ver los procesos en ejecución, conocer las conexiones existentes, etc.

Vista Diseño de impresión | Páginas: 20 de 35 | Palabras: 0 de 7569 | MCA

USO COTIDIANO DEL MENOR EN LAS NNTT II

The screenshot displays a desktop environment with several applications open:

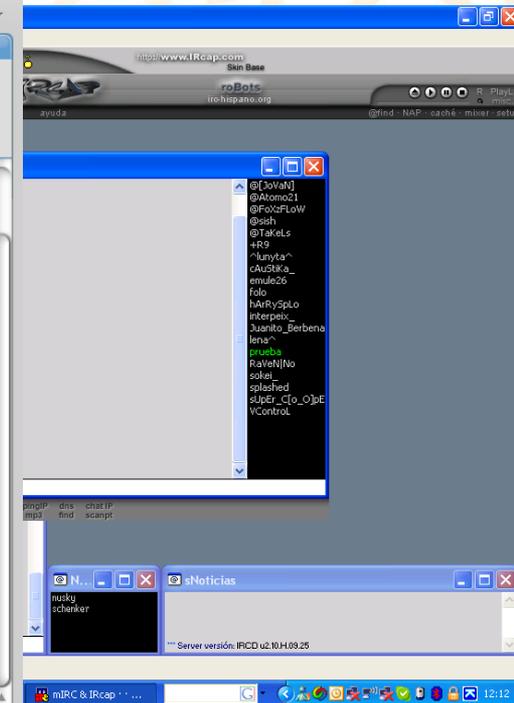
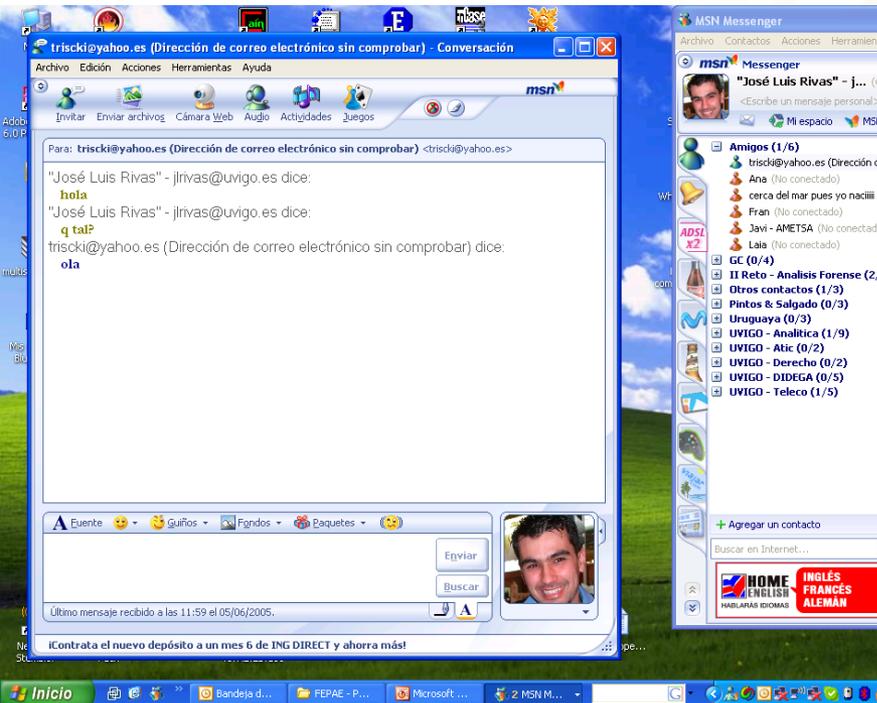
- eMule Plus v1.1d:** Shows a list of files being downloaded. The table below summarizes the data:

Nombre	Tamaño	Transfe...	Comple...	Velocidad	Fuentes	Estado	Progreso	Restante
[Au]Hikaru No Gol - 19 [Rg].avi	173,69 MB	152,45 MB	155,14 MB		9/16 (0)	Esperando	89,3%	18,55 MB
[Au]Hikaru No Gol - 20 [Rg].avi	173,69 MB	36,7 MB	37,18 MB		16/17 (0)	Esperando	21,4%	136,51 MB
[Au]Hikaru No Gol - 21 [Rg].avi	173,51 MB	0 Bytes	0 Bytes		9/10 (0)	Esperando	0%	173,51 MB
[Au]Hikaru No Gol - 22 [Rg].avi	173,69 MB	261 KB	262 KB		2 (0)	Esperando	0,1%	173,43 MB
[Au]Hikaru No Gol - 23 [Rg].avi	173,57 MB	22,33 MB	22,48 MB		4/5 (0)	Esperando	12,9%	151,09 MB

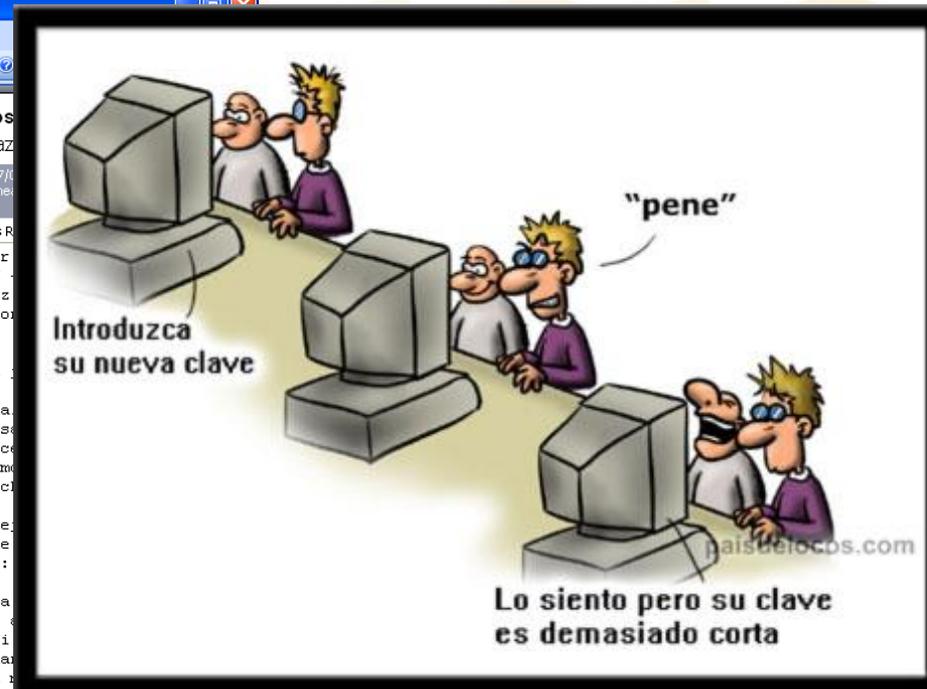
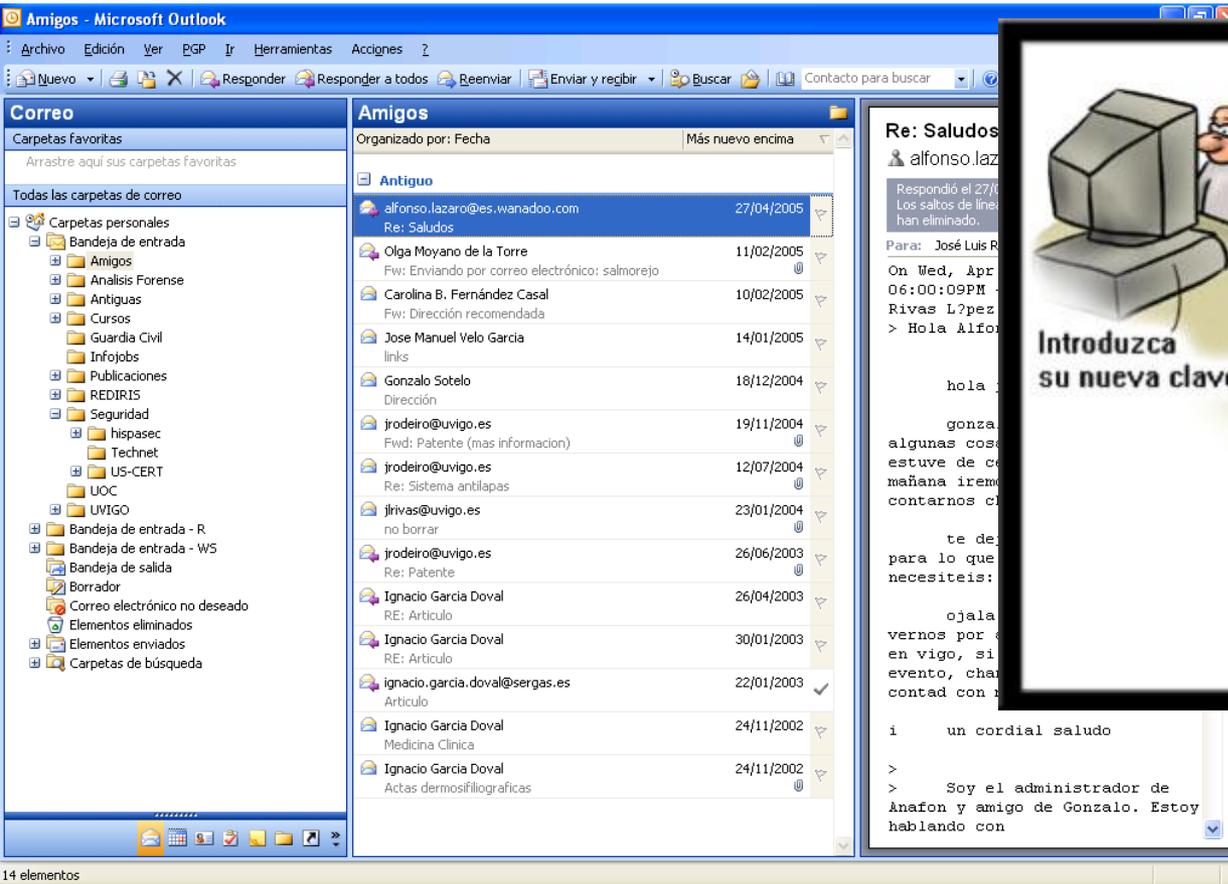
- Spotify:** Shows a social playlist titled "Lista social" with tracks like "Bailando - Spanish Version", "Come Home", "The Sound of Goodbye - Radio Edit", "How Did You Know - Radio Edit", "Blood I Bled", and "Everybody's Talkin'".
- File Manager:** Shows a list of files with their sizes and sources. The table below summarizes the data:

Tamaño	Fuentes
4,88 MB	2950 (2950)
4,88 MB	2225 (2225)
60,06 MB	2013 (1856)
59,19 MB	909 (723)
4,88 MB	695 (695)
51,8 MB	596 (541)
4,89 MB	568 (568)
4,88 MB	507 (507)
55,54 MB	476 (361)
4,35 MB	441 (441)
4,88 MB	405 (405)
55,15 MB	401 (356)
4,35 MB	381 (381)
83,88 MB	364 (0)
470,85 MB	352 (227)
3,4 MB	350 (350)
4,88 MB	325 (325)
3,58 MB	320 (320)
37,71 MB	309 (276)
81,06 MB	306 (267)
3,59 MB	294 (294)
4,89 MB	286 (286)
3,39 MB	270 (270)

USO COTIDIANO DEL MENOR EN LAS NNTT III



USO COTIDIANO DEL MENOR EN LAS NNTT IV



Shockwave Flash Object

AGENDA

- **Introducción**
- **Datos interesantes**
- **Web 1.0 → Web 2.0**
- **Uso cotidiano del menor en las NNTT**
- **Perfil de acosador**
- **Peligros**
- **¿qué hacer para prevenir?**
- **Decálogo**



Perfil del acosador I

- **Acosadores circunstanciales**
 - **No tienen preferencia por un menor**
- **Acosadores preferenciales**
 - **Únicamente le interesan los menores**

Perfil del acosador II

Acosadores preferenciales

CARACTERÍSTICAS:

- Modelo de comportamiento muy previsible
- Habilidad en las relaciones interpersonales con menores
- Técnica bien desarrollada para alcanzar víctimas
- Utilizan con facilidad las tecnologías modernas

Perfil del acosador III

Acosadores preferenciales

CARACTERÍSTICAS:

- Estimulador de fantasías
- Técnicas bien desarrollada de localización y conversación con menores
- Miente y manipula diestramente
- Transforma las fantasías en realidad

Perfil del acosador IV

Acosadores preferenciales

- Utiliza el ordenador en el trabajo
- La mayoría de las veces casado
- Envía fotografías suyas
- Utiliza el teléfono del trabajo o el móvil
- Posee una colección de pornografía infantil y/o erotismo infantil
- De forma activa solicita fotos

Perfil del acosador V

Acosadores preferenciales

TÉCNICAS:

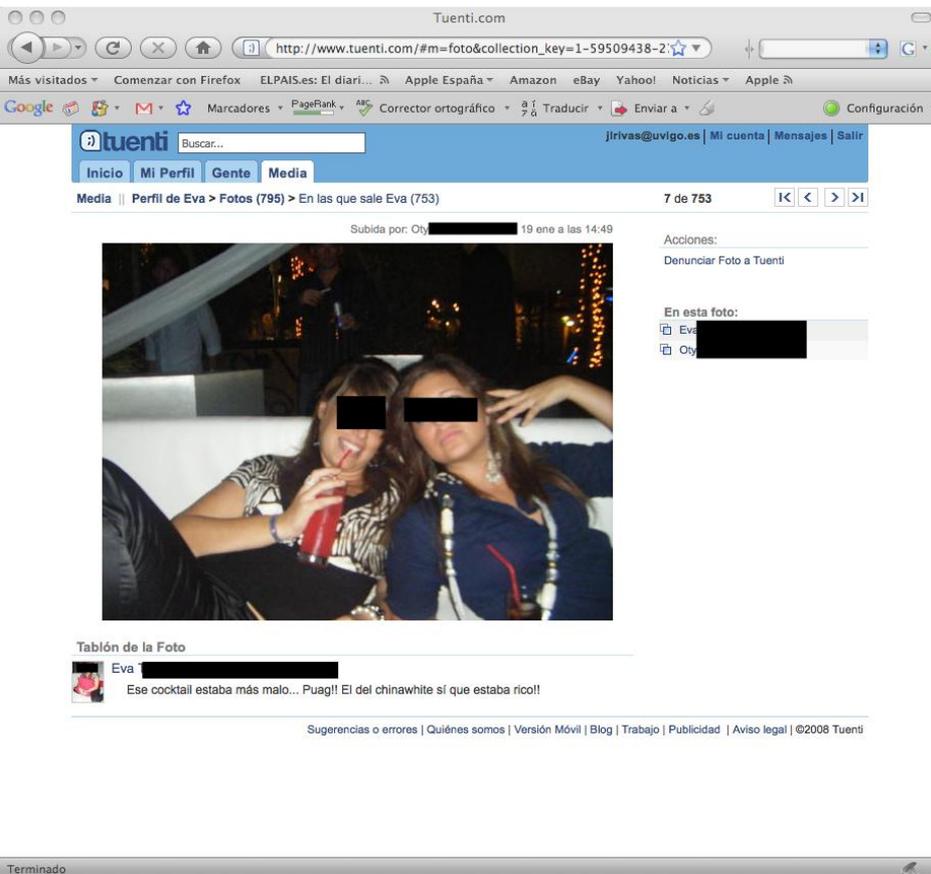
- **Asume la identidad de un niño**
- **Lenguaje acorde con la victima**
- **Solicita informaciones personales**
- **Desea encuentro por webcam o real**
- **Solicita fotos**

AGENDA

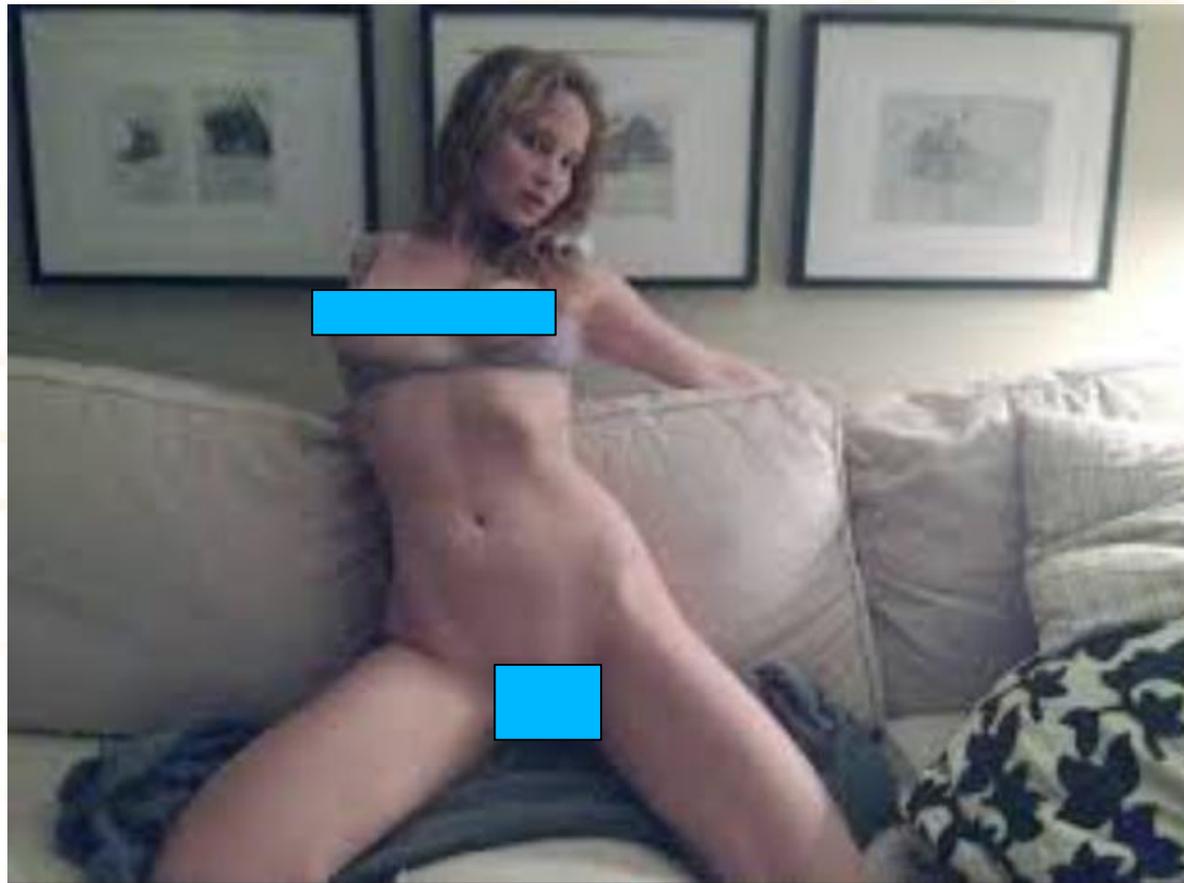
- **Introducción**
- **Datos interesantes**
- **Web 1.0 → Web 2.0**
- **Uso cotidiano del menor en las NNTT**
- **Perfil del acosador**
- **Peligros**
- **¿qué hacer para prevenir?**
- **Decálogo**



PELIGRO: PRIVACIDAD EN TUMENTI, FACEBOOK, ETC.



PELIGRO: PRIVACIDAD EN TUENTI, FACEBOOK, ETC.



PELIGRO: OBTENCIÓN DE DATOS PERSONALES I

Windows Internet Explorer

http://www.aldaniti.net/wingames/mercedes/index.php?

Archivo Edición Ver Favoritos Herramientas Ayuda

Llévate gratis tu modelo preferido de Mercedes - Benz

DATOS DEL FUTURO GANADOR

Estás dentro de plazo: 22 de Enero del 2009 a las 12:11 de la tarde

Para validar tu configuración simplemente debes rellenar los siguientes campos.

Tratamiento: Hombre Mujer

Nombre: Apellidos:

E-mail: Telf: C. postal:

¿Dónde enviamos los regalos?

Tipo de vía: Nombre de la vía: Número: Planta: Puerta:

Selección:

Población: País: España

EQUIPAMIENTO EXTRA - PERSONALIZA TU PREMIO

- Sí, necesito sillas para mis hijos
- Sí, necesito un "manos libres"

POLÍTICA LEGAL

- Declaro ser mayor de 18 años
- He leído y acepto las condiciones y la Política de protección de datos

REGALO valorado en 78€

7 NOCHES DE HOTEL GRATIS*
*CON CONSUMICIÓN MÍNIMA

HOTELBONO TE OFRECE ESTE REGALO

AGENDA

- **Introducción**
- **Datos interesantes**
- **Web 1.0 → Web 2.0**
- **Uso cotidiano del menor en las NNTT**
- **Perfil del acosador**
- **Peligros**
- **¿qué hacer para prevenir?**
- **Decálogo**



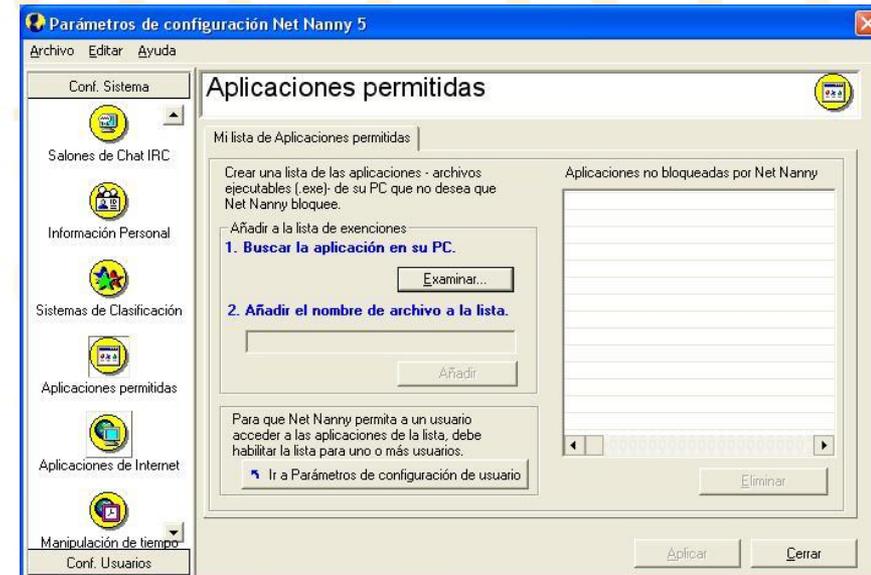
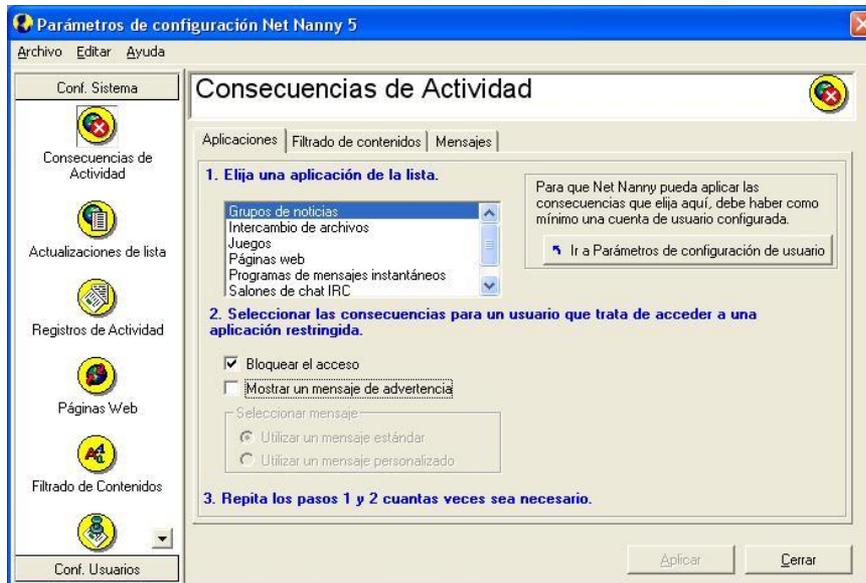
¿QUE HACER PARA PREVENIR? I

- **Educación**
- **Instalar el ordenador en zonas comunes**
- **Instalación de programas de control parental**
- **Limitar las horas de conexión**
- **Concienciar la importancia de no dar información personal**
- **Estar alerta ante comentarios que puedan hacer en casa**
- **No establecer citas reales sin consentimiento paterno**

¿QUÉ HACER PARA PREVENIR? II

- ¿Qué tenemos que buscar?
- **Bloquear paginas web inapropiadas o bloquear todas las páginas excepto las que autoricemos**
- **Impedir búsquedas por palabras inapropiadas**
- **Controlar el uso de internet durante horas determinadas**
- **Bloquear juegos no aptos**
- **Evitar mandar información privada (correo-e, cuenta bancaria, etc)**
- **Bloquear programas tipo P2P**
- **Controlar las paginas visitadas**

¿QUÉ HACER PARA PREVENIR? III



AGENDA

- **Introducción**
- **Datos interesantes**
- **Web 1.0 → Web 2.0**
- **Uso cotidiano del menor en las NNTT**
- **Perfil del acosador**
- **Peligros**
- **Ejemplo práctico**
- **¿qué hacer para prevenir?**
- **Decálogos**



DECALOGO GENERAL

- **Lo relevante debe ser siempre lo educativo y no lo tecnológico**
- **Los padres/profesores deben ser conscientes de que las TIC no tienen efectos sobre el aprendizaje ni genera automáticamente innovación**
- **Se debe de utilizar las TIC para que los menores aprendan haciendo cosas no para que no molesten durante un tiempo.**
- **Las TIC deben de usarse como herramientas de apoyo**
- **Se debe de estar con el menor cuando este navegando y explicarle los diferentes peligros existentes**

DECALOGO GENERAL II

- **Ante cualquier sospecha contactar con expertos**
- **Ante cualquier caso de intento de abuso, etc. denunciar ante la PJ.**

DECALOGO MOVILES I

- **Deben ser cuidadosos con las fotos y vídeos que comparten. Si no son apropiados pueden generar problemas de reputación y seguridad personal.**
- **No practiquen sexting (ni fotos, ni vídeos ni mensajes de sexo)**
- **No practiquen bulling (acoso ni intimidación)**
- **No se olviden de los buenos modales y principios éticos. Si no se saben comportar, tal vez es pronto para tener móvil**
- **Sentido común al acceder a redes sociales, o chats...el móvil está más desprotegido.**

DECALOGO MOVILES II

- Si el móvil tiene GPS o localizador. Que no difundan su situación . Sólo a la familia o amigos de confianza.
- Ignorar mensajes de desconocidos.
- Evitar dar el número de teléfono a cualquiera
- No flirtear con alguien desconocido, con número oculto
- Si se sienten amenazados o les llega algo raro, que tengan confianza en contarle...que confíen en su instinto.

DECALOGO REDES SOCIALES I

- Hay que configurar correctamente el perfil de privacidad en el momento de registrarse en una red social. Si el menor no está seguro, debe pedir ayuda a sus padres.
- Valorar siempre la información que quiere compartir.
- Cuando alguien quiera ser tu amigo, asegúrate de que realmente es alguien que conoces y quieres tener como amigo
- Prohibido poner en el perfil dónde vives, teléfono, en qué trabajan tus padre y madre, en qué colegio estudias (si no se lo dices a nadie por la calle aquí tampoco)
- No pongas fotos que te comprometan (los amigos/as de tus amigos/as podrían entrar en tu perfil)

DECALOGO REDES SOCIALES II

- **No flirtees en la red. Algunas personas crean perfiles falsos y ocultan su verdadera identidad para reírse o aprovecharse.**
- **Si un desconocido te pide o te habla de sexo, avisa inmediatamente a tu padres o madre. Puede ser un adulto. Hay que denunciar**
- **Ten cuidado con lo que escribes en las redes sociales (pertenece automáticamente a la empresa)**
- **Si un amigo/a que has conocido en Internet quiere quedar contigo: queda en lugar público, vete acompañado/a y dile a un adulto dónde vas**
- **Si te sientes amenazado, ten confianza en contarlo...confía en tu instinto.**



GOBIERNO
DE ESPAÑA

MINISTERIO
DE SANIDAD, SERVICIOS SOCIALES
E IGUALDAD



SECRETARÍA
DE ESTADO DE SERVICIOS SOCIALES
E IGUALDAD

INSTITUTO DE LA MUJER
Y PARA LA IGUALDAD DE OPORTUNIDADES



EXCMO. CONCELLO
DE
BAIÑA
(POVURCADA)



FIN



mentarios, cuestiones,
gerencias ,...

jlrvias@uvigo.es

jlrvias@laboratoriodeseguridadtelematica.com

<http://webs.uvigo.es/jlrvias>

MUCHAS GRACIAS POR SU ATENCIÓN