Internet, navegación responsable

Fernando da Rosa
Rodolfo Pilas

5 de junio de 2010

Índice general

1. Internet **7**
- 1.1. Definición . . . 7
- 1.2. ¿Qué son los protocolos TCP/IP? . . . 7
- 1.3. La dirección IP . . . 8
  - 1.3.1. Direcciones IPv4 . . . 8
  - 1.3.2. Direcciones IPv6 . . . 8
- 1.4. ¿Qué es un DNS? . . . 9
- 1.5. La "magia"de la navegación web . . . 9
- 1.6. La "magia"del correo electrónico . . . 10

2. Internet y sus riesgos **15**
- 2.1. Riesgos con la información . . . 15
- 2.2. Riesgos de la comunicación interpersonal . . . 16
- 2.3. Riesgos en actividades económicas . . . 17
- 2.4. Riesgos de funcionamiento . . . 17
- 2.5. Riesgo de addicciones . . . 18
- 2.6. Riesgos por virtualización . . . 19

3. Redes sociales en Internet **21**
- 3.1. Facebook . . . 22
- 3.2. MySpace . . . 22
- 3.3. La privacidad en los servicios de redes sociales . . . 22
- 3.4. Elementos a tener en cuenta . . . 24
- 3.5. La creación de redes sociales en Internet especialmente para niños 24

4. Sexting **25**
- 4.1. Webcam y privacidad . . . 26

5. Cyberbullying o Ciberacoso **29**

6. Pornografía infantil **33**
- 6.1. Definición . . . 33
- 6.2. Formas de difusión . . . 33
- 6.3. Conclusiones de la investigación realizada para el IIN (Instituto Interamericano del Niño) año 2005 . . . 34
- 6.4. Recomendaciones de la investigación realizada para el IIN año 2005 34

7. Malware **37**
7.1. Adware . . . 37
7.2. Backdoor o Puerta Trasera . . . 37
7.3. Bomba fork . . . 38
7.4. Botnet . . . 38
7.5. Bug . . . 38
7.6. Cookies . . . 38
7.7. Crackers . . . 39
7.8. Cryptovirus, Ransomware o Secuestradores . . . 39
7.9. Dialers . . . 39
7.10. Exploit . . . 40
7.11. Falso antivirus . . . 40
7.12. Hijacker . . . 40
7.13. Hoaxes, Jokes o Bulos . . . 40
7.14. Keystroke o keyloggers . . . 41
7.15. Lamer . . . 41
7.16. Pharming . . . 41
7.17. Phishings . . . 42
7.18. Rabbit o conejos . . . 42
7.19. Riskware . . . 42
7.20. Rootkit . . . 42
7.21. Spam . . . 42
7.22. Spyware . . . 43
7.23. Troyano . . . 43
7.24. Virus informático . . . 43
7.25. Ventanas emergentes/POP-UPS . . . 43
7.26. Worms o gusanos . . . 44

8. Cómo protegerse **45**
8.1. Normas generales de seguridad en el uso del computador . . . 45
8.2. Evite los riesgos y piense . . . 45
8.3. Filtros de Contenido . . . 46
8.4. Control paterno . . . 46

9. Asegurar la Navegación **47**
9.1. Algunos consejos básicos . . . 47
9.2. Complementos que aumentan la seguridad de la navegación . . . 48
9.2.1. No Script . . . 48
9.2.2. Verify Redirect . . . 48
9.2.3. CS Lite . . . 48
9.2.4. Adblock Plus . . . 48
9.2.5. Domain Details . . . 48
9.2.6. Expand Short URL . . . 48

10. Asegurar el Correo Electrónico **49**
10.1. Normas básicas para mantener seguro su correo . . . 49
10.2. Complementos que aumentan la seguridad del correo . . . 50
10.2.1. Manejo y detección de SPAM (incluído) . . . 50
10.2.2. Privacidad Robusta (incluído) . . . 50
10.2.3. Protección contra Phishing (incluído) . . . 51

10.2.4. Display Mail User Agent 51
10.2.5. Enigmail 51

11.Básico de Criptografía por e-mail **53**
11.1. Asegurar Remitente 53
11.2. Asegurar destinatario 53
11.3. Integridad del mensaje 53
11.4. Algunas buenas prácticas 54

12.Netiquette **55**
12.1. Para estudiantes de educación primaria 55
12.2. Para estudiantes de centros de educación media 56
12.2.1. Sobre el envío de mensajes electrónicos 56

A. Redes Intra-aula **65**
A.1. La Propuesta 65
A.2. Implicancias desde el punto de vista pedagógico 66

B. Legislación **69**
B.1. Ley Nº 17.559 69
B.2. Ley Nº 17.815 69
B.3. Ley Nº 18.331 71

Capítulo 1

Internet

1.1. Definición

Internet ha sido definida como una "*red de redes*", básicamente es un gran conjunto de computadoras, de diversos tipos conectadas en redes que a su vez se conectan entre sí, compartiendo todas un protocolo de comunicación común, lo que posibilita que puedan funcionar en conjunto. Según el diccionario de la Real Academia Española, Internet es una "*Red informática mundial, descentralizada, formada por la conexión directa entre computadoras u ordenadores mediante un protocolo especial de comunicación.*"La definición de la Wikipedia es aún más precisa "*Internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.*"[33] La primera descripción registrada que se puede considerar origen de Internet, es una serie de notas escritas por JCR Licklider del MIT en agosto de 1962, hablando de su concepto de Galatic Network. Tuvo la visión de un mundo interconectado por un conjunto de ordenadores a través de los cuales uno podrían rápidamente tener acceso a datos y programas desde cualquier sitio. En espíritu, el concepto era muy parecido a la Internet de hoy. Luego Licklider fue uno de los líderes del proyecto que dió origen a Internet. El cual se remonta a las primeras conexiones entre computadoras utilizando un protocolo común a fines de la década de los 60, pero recién con el desarrollo de la World Wide Web por parte de Tim Berners Lee, a inicios de los años 90, es cuando se empieza a popularizar su uso. En ambos casos su desarrollo fue posible gracias al aporte de científicos, técnicos, programadores e instituciones que liberaron su trabajo de patentes y lo brindaron a la comunidad.[16][3]

1.2. ¿Qué son los protocolos TCP/IP?

Son parte de una familia más amplia de protocolos[1], todos los cuales sirven para facilitar la comunicación entre computadoras con distintos sistemas operativos. TCP significa "*Transmission Control Protocol*."IP "*Internet Protocol*". Muy básicamente podemos decir que el protocolo TCP sirve para fijar normas

[1]Conjunto de reglas normalizadas para la representación, señalización, autenticación y detección de errores necesario para enviar información a través de un canal de comunicación

de comunicación que garantizan la trasmisión correcta de los datos entre las computadoras. En el caso del protocolo IP el mismo sirve para organizar la información a ser enviada en paquetes, cada paquete incluye la dirección de la máquina de origen y destino, el famoso número IP, lo cual asegura la identificación de los paquetes, hoy en día estamos usando principalmente el protocolo IPv4 pero en vista de que debido a la cantidad de direcciones existentes el mismo se está agotando ya se está empezando a utilizar su sustituto futuro el IPv6, que entre otras cosas nos brinda un número mucho mayor de direcciones IP [12]. Ambos protocolos funcionando en conjunto aseguran la división de la información en paquetes y su llegada a destino. Pero TCP/IP son parte de una familia mucho más amplia de protocolos que permiten el funcionamiento de Internet, interactuando unos con otros, otros miembros de la familia son HTTP[2], SMTP[3], FTP[4], etc.

1.3. La dirección IP

Las computadoras se comunican entre sí a través de sus números IP o direcciones IP, podríamos decir que en un instante dado la dirección IP es el nombre propio de una computadora dentro de Internet. En algunos casos, las direcciones IP son públicas y fijas (por ejemplo para instalar un servidor), en otros casos son dinámicas, por eso decimos en un instante dado. Pero siempre es posible seguir la conexión hasta el número IP del cual surge y si se tiene acceso a los registros de los proveedores de Internet, saber que máquina estaba conectada a través de una determinada dirección IP en un momento dado.

1.3.1. Direcciones IPv4

Una dirección IP, en el caso del protocolo IPv4, podría ser la siguiente:

```
190.134.5.214
```

La cual corresponde a la dirección IP con la cual yo estoy conectado a Internet en el momento que escribo estas líneas. Analizando ese número puedo saber fácilmente que se trata de una computadora conectada desde Uruguay. Los números IP tienen una distribución geográfica. Una dirección IPv4 se puede representar con cuatro dígitos decimales que van del 0 al 255. El límite de 256 números viene dado porque cada número, representa un octeto binario y surge de las combinaciones posibles de 8 bits.

1.3.2. Direcciones IPv6

Las direcciones IPv4 permiten un total de 4.294.967.296 (2^{32}) direcciones de red diferentes, lo que es un problema en la Internet actual, ya que muchas máquinas requieren estar prendidas de continuo y necesitan direcciones permanentes y este número está resultando escaso. El nuevo protocolo de direcciones versión 6 permite (2^{128}) 340 sixtillones de direcciones diferentes. Esto realmente

[2]HyperText Transfer Protocol
[3]Simple Mail Transfer Protocol
[4]File Transfer Protocol

es un rango muy grande de direcciones. Si comparamos la cantidad de direcciones IPv6 posibles con la superficie de la Tierra, tendríamos unos 670 mil billones de direcciones por cada milímetro cuadrado de la Tierra. Una dirección IP, en el caso del protocolo IPv6, podría ser la siguiente:

```
2401:0db3:85a3:0000:1319:8a2e:0370:7343
```

Las direcciones IPv6 ya están disponibles para ser configuradas en la mayoría de los computadores y equipamiento de comunicaciones de Internet. Queda aún la migración de servicios (p.ejemplo, sitios web) que se configuren detrás de estas direcciones de la versión 6. De todas formas el proceso se realizará pronto.[14]

1.4. ¿Qué es un DNS?

El DNS (Domain Name System) o sistema de nombres de dominio, cumple principalmente con la función de asociar la dirección IP a algo más manejable por humanos, un nombre [1]. Como dato curioso prácticamente el único software utilizado en los servidores DNS es Bind[5], y es distribuido como Software Libre[6], lo que termina convirtiendo a cualquier usuario de Internet en un usuario de Software Libre. Gracias al DNS en lugar de tener que poner un número en mi navegador, es posible incluir un nombre el cual también tiene sus especificaciones de sintaxis.

1.5. La "magia"de la navegación web

Luego de que Usted hace click en un enlace o escribe una dirección web en la barra superior de su navegador y presiona ENTER se desatan una serie de procesos sucesivos que son los siguientes:

1. Supongamos que ha escrito `www.xo.org.uy` en su navegador, aquí comienza la etapa de resolución (averiguar la dirección IP)

2. Primeramente el navegador consultará el archivo hosts que se encuentra en todas las máquinas y donde generalmente están los números IP de las máquinas más próximas o más utilizadas.

3. Si no encuentra el IP en el archivo hosts, el navegador le consultará a los servidores DNS que tiene como pre-determinados cuál es la dirección IP correspondiente a ese dominio. Los servidores DNS predeterminados se configuran automáticamente en el momento que usted inicia su conexión con su proveedor de acceso.

4. En caso que los servidores pre-determinados no conozcan la dirección IP, informarán de esto a su navegador. Entonces existen unos servidores DNS que se llaman root-servers que conocen a todos los DNS de cada país. Y su navegador les preguntará a estos root-servers qué dirección IP es el DNS para el .uy, y éstos le responderán que es SECIU[7].

[5]Berkeley Internet Name Domain

[6]Software que respeta la libertad de los usuarios sobre su producto adquirido y, por tanto, una vez obtenido puede ser usado, copiado, estudiado, cambiado y redistribuido libremente

[7]Servicio Central de Informática de Universitaria

5. Entonces ahora su navegador le preguntará a los DNS de SECIU quién es el DNS para .org.uy y estos le volverán a responder nuevamente que es SECIU (p.ej. para .com.uy es Antel, pero no es el caso del ejemplo que seguimos). Entonces ahora su navegador volverá a preguntar quién es el DNS para `.xo.org.uy` y este le responderá la dirección IP del servidor DNS correspondiente.

6. Por último el navegador le pregunta al servidor "autoritativo" para el dominio `xo.org.uy` cuál es la dirección IP del servidor que `www.xo.org.uy`. Recién ahora se considera resuelto el nombre y se procede a la conexión web.

7. Su navegador pide la página web por defecto del sitio `www.xo.org.uy` utilizando la dirección IP y el servidor le enviará un archivo .html que el navegador interpretará.

8. El archivo .html tiene dentro indicaciones de otros "objetos" que terminan armando la página, e irá pidiendo al servidor cada uno de ellos, como ser:

   - Archivos de estilo .css
   - Archivos de código javascript .js
   - Imágenes .jpg
   - Animaciones flash .swf
   - etcétera.

9. Cuando todos estos archivos que conforman una página web son descargados en su computador, el navegador está en condiciones de mostrarle la página web. Cada dibujo de propaganda, cada imagen de una página requiere su conexión y transferencia. Como referencia, la página web de inicio de `www.xo.org.uy` tiene un total de 40 archivos diferentes y 800KB de información en total.

10. El navegador guardará esos archivos un "cache", la próxima vez que visite el sitio, los tomará de ese cache en su disco, en lugar de volver a descargarlos de Internet, logrando que su navegación sea más rápida. Cada cierto tiempo, el navegador caducará la información guardada en el caché para descargarla nuevamente y de esa forma mantener información actualizada.

11. La página Web que usted ve en su navegador es armada (diagramada) por su navegador y la forma en que la ve, puede variar de la forma que la ve otro navegante en otro computador, dependiendo de la configuración de su navegador (tamaños de letras) y de la pantalla del computador (resolución). También algunos navegadores, no precisamente muestran la página, pueden leerla mediante un software de interpretación de caracteres-a-voz.

1.6. La "magia"del correo electrónico

Usted ha terminado de redactar su correo, ha puesto sus adjuntos, ha escrito con negrita el texto a destacar y con letras rojas un par de frases especiales. Decidido presiona el botón enviar y se comienza el siguiente procedimiento:

1. Como ha realizado un texto "enriquecido", el mismo debe ser transformado a HTML, para que el destinatario vea sus textos en negrita y coloreados. Ese HTML no puede ser parte del correo (pues el correo electrónico no es HTML) entonces su texto viajará como un adjunto, mientras que su correo irá vacío. Los lectores modernos interpretan esto transparente para el lector, pero no todos los sistemas aseguran que funcione perfectamente (p.ej. si su interlocutor utiliza un lector de voz por problemas en la capacidad visual).

2. El adjunto tampoco puede viajar así como lo ha adjuntado. El correo solo puede transportar letras, así que su programa de correo debe realizar un proceso de conversión a letras. Esto hace que su adjunto tenga un tamaño mayor al que usted lo ve en su disco, generalmente un 10-20 % mayor (debe tener en cuenta esto si está enviando un adjunto del tamaño cerca de algún límite de aceptación).

3. Recién ahora su correo está pronto para ser enviado y el programa de correo contactará al servidor SMTP que tiene configurado para entrega.

4. Para contactar con el servidor SMTP tendrá que realizar un proceso de resolución del nombre a IP, semejante a cómo hace el navegador web para llegar a un sitio web.

5. Una vez contactado el servidor SMTP entrega (trasmite) el correo y a Ud. le informa que el correo ha sido enviado. No obstante esto es solamente la primera parte del proceso.

6. Ahora el correo en manos de su servidor de correo de envío, pasará opcionalmente por un antivirus que deberá recomponer (convertir de letras a formato binario) su adjunto y analizarlo y luego decidirá si el correo es para un usuario local (dentro de su mismo dominio) o para un usuario fuera de su dominio.

7. Si es para fuera de su dominio, deberá consultar al DNS para saber cuál es el computador en internet que recibe correo por el dominio que usted quiere llegar y esto le devolverá una IP de otro servidor SMTP.

8. Entonces su servidor contactará al servidor de destino y seguirá un protocolo de presentación, indicando quién es y los datos del correo que desea entregar. El servidor de destino realizará una serie de verificaciones tendientes a combatir el spam, antes de aceptar el correo:

   - Verificar si su servidor está debidamente identificado en el DNS
   - Confirmar que su servidor está autorizado a distribuir correo de su dominio
   - Revisar listas (clearing) de servidores denunciados como que alguna vez enviaron spam, para saber si su servidor esta allí.

9. Si la transferencia del correo no es autorizada (p.ej. porque usted escribió mal la dirección de correo del destinatario), su servidor recibirá un código de error y le enviará un mensaje de notificación.

10. Si el servidor de destino acepta la transferencia del correo, entonces se transfiere y ahora el correo está en manos del servidor de destino, que vuelve a tomar la decisión si es un correo para él, o debe encaminarlo a través de otro servidor.

11. Supongamos que es un correo para un usuario que tiene su cuenta en ese servidor entonces analizará el correo con un filtro anti-spam, verificando si su mensaje no tiene patrones de texto como un spam. También revisará el correo con un antivirus, volviendo a convertir el adjunto para analizarlo. Y al final dejará el correo en la casilla del destinatario.

12. Cuando el destinatario arranque su programa para leer correo, el mismo se conectará al servidor para bajar el correo nuevo y recién ahí quedará disponible para que lo lea.

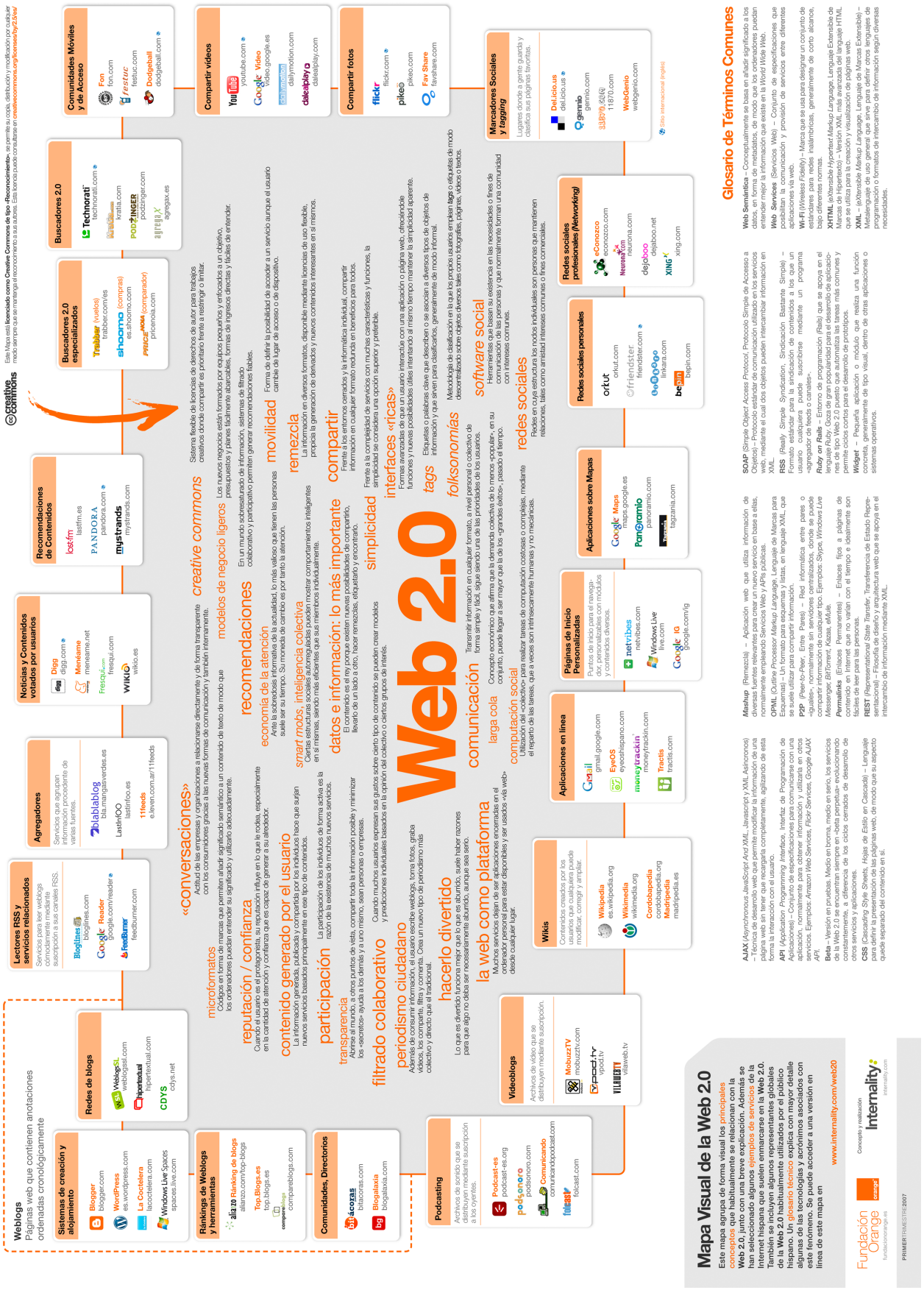


Figura 1.1: Fundación Orange: http://internality.com/web20/

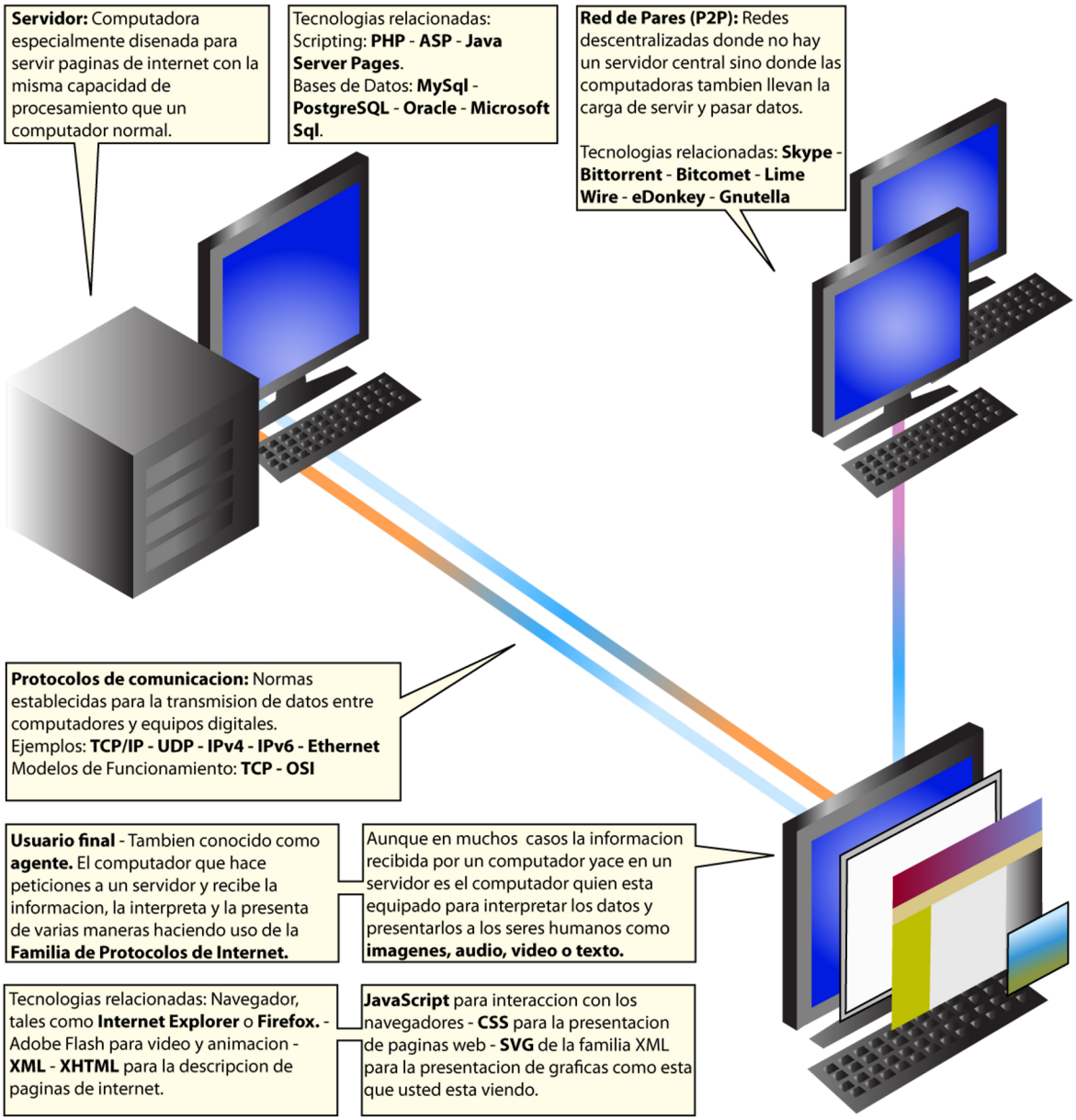


Figura 1.2: Autor: Camilo Sanchez

Capítulo 2

Internet y sus riesgos

Internet como herramienta, como tecnología, es independiente de riesgos o beneficios. El uso que luego se hace de esta herramienta o tecnología es la que le da el carácter beneficioso o riesgoso, dependiendo esto también de qué análisis se hace, quién realiza el análisis y en que escenario se realiza el análisis. De todas formas, concentrándonos exclusivamente en los riesgos, podemos definir varios tipos de problemas [17] en la actual Internet:

2.1. Riesgos con la información

Internet presenta abundancia de información, accesible fácil y rápidamente. Pero esta propia abundancia y comodidad de información presenta algunos problemas:

Fiabilidad o veracidad de la información. Cualquier persona publica contenidos en Internet y puede hablar de cualquier tema, desde la base del conocimiento cotidiano hasta el rigor científico. Pero también, cualquiera puede escribir información malintencionada o dañina. De todas formas los buscadores indexaran la información de igual manera y la dejarán al alcance de quién la acceda.
Acción: aprender a valorar y criticar la información

Abundancia de información. La dispersión de la información también es un riesgo, pues requiere que quién busca información dedique un tiempo importante a encontrar lo que necesita.
Acción: Aprender hábitos de trabajo en Internet

Acceso a información inapropiada o nociva. Existe información que puede resultar inapropiada o nociva para niños que no han tenido el correspondiente desarrollo cognitivo y afectivo. Muchos sitios web pueden tener imágenes de sexo, violencia, drogas, etc, que no son adecuadas, a pesar de que los temas estén tratados con adecuado rigor científico.
Acción: Atención de Padres y Educadores, software de protección

Acceso a información ilegal, inmoral o peligrosa. Información sobre sectas, creación de dispositivos explosivos, métodos de tortura, terrorismo,

pedofilia, consumo de drogas, ritos satánicos, y una larga lista de etcéteras está disponibles en Internet. Si bien su acceso no es simple, pues suelen estar perseguidos por la policía de delitos informáticos, la información de este tipo también es parte del ciberespacio.
Acción: Acción social, participación de todos los navegantes para denunciar estos sitios.

2.2. Riesgos de la comunicación interpersonal

Cuando las personas se comunican, establecen y mantienen relaciones y vínculos afectivos. Internet como viabilizador de las comunicaciones es el medio para que estas relaciones y vínculos se desarrollen. No obstante, esos vínculos pueden acarrear los siguientes riesgos:

Bloqueo de la cuenta de correo. Generalmente de produce por la ignorancia a las normas de "*netiquette*" (Ver Capítulo 12) y la denuncia de los perjudicados.
Acción: conocer las normas de netiquette.

Recibir spam. Muchas veces el spam es de contenido sexual, médico o de negocios. Otras veces contienen adjuntos que pueden ser un riesgo para el computador (virus, troyanos y otro malware (ver capítulo 7)).
Acción: cuidar la dirección de correo personal y disponer de filtros antispam y sistemas de detección de virus.

Recepción de mensajes ofensivos. Los foros o los mensajes escritos pueden ser un medio para recibir insultos u ofensas personales, a veces generan fuertes discusiones que incluyen amenazas. Inclusive los mensajes pueden llegar a niveles de violencia que atentan contra la intimidad del receptor.
Acciones: bloquear la recepción de este tipo de mensajes tan pronto empieza el problema, evitar entrar en discusión, mantener la "*netiquette*" (ver capítulo 12).

Perdida de la intimidad. Los datos que se proporcionan, tanto sean personales como familiares o de terceros, pueden ser accedidos por desconocidos y esto es, de por sí, un peligro. También se proporcionan datos en redes sociales, sitios web gratuitos, etc.
Acción: cuidar los datos personales, entender cuándo se dan datos de comunicación y cuándo datos personales.

Acciones ilegales. La facilidad de comunicación que ofrece Internet es, muchas veces, un estímulo para considerar que las leyes no deben ser observadas o pueden ser fácilmente quebradas. Ciertas conductas como el plagio de información, el insulto, la difamación o la amenaza son ilegales en Internet también. No observar los Derechos de Autor puede traer consecuencias legales.
Acción: educación y ejemplo por parte de padres y educadores

Contacto con personas inadecuadas. Algunos canales de chat, sitios que sugieren amistades o contactos, puede llevar a dar con personas que falsean su identidad y datos, con el riesgo de ser víctimas de abusos, violencia o

actos delictivos.
Acción: educar sobre los riesgos y mantener una observancia sobre los menores y el uso que hacen de Internet.

2.3. Riesgos en actividades económicas

Cuando en Internet se viabilizaron las transacciones comerciales, se produjo un gran auge y expansión de las actividades, sitios y oferta de mercaderías y servicios. Pero, las actividades económicas siempre están rodeadas de riesgos, en el ciberespacio los riesgos son:

Estafas. La virtualidad puede enmascarar engaños y estafas a compradores, principalmente cuando se trata de empresas u organizaciones de dudosa solvencia o reconocimiento.

Publicidad abusiva. Muchas veces para confirmar una compra, los sitios lo llevan por una intrincada suerte de "ofertas" complementarias donde a veces debe dar click en Aceptar y otras veces en Cancelar. O también pueden abrir otras ventanas donde le ofrecen otros productos distintos, siendo difícil separar el proceso de compra que uno está confirmando de la oferta, terminando todo en compras innecesarias.

Compras de menores sin autorización paterna. Son conocidas historias de niños o jóvenes que han realizado transacciones en Internet sin el correspondiente control familiar, utilizando incluso tarjetas de crédito habilitadas, que muchas veces quedan guardadas en en su perfil en los los sitios de compra.

Robos. Alguna información personal necesaria para las transacciones económicas puede ser robada para suplantar la personalidad de sus propietarios, por ej. información de la tarjeta de crédito.

Delitos vinculados a la Propiedad Intelectual. Obtener copias de obras (software, música, videos) sin los correspondientes derechos de autor, desactivar sistemas de protección y distribuir o difundir obras sin autorización constituyen delitos constituyen delitos que son penados por la Ley. Mucha gente comete estos delitos a veces sin conocer las sanciones o a veces sin saber que se está cometiendo el delito mediante su propia computadora.

Ante la gravedad de estos riesgos y la relativa novedad que supone Internet en nuestra sociedad para la mayor parte de los ciudadanos, deberían hacerse campañas informativas a nivel nacional a través de todos los medios de comunicación, con una especial énfasis en los centros docentes. Al mismo tiempo deben seguir desarrollándose la legislación que regule el uso de Internet y las medidas policiales dirigidas a la captura de los delincuentes del ciberespacio.

2.4. Riesgos de funcionamiento

Muchas veces la red no funciona en forma adecuada, los problemas pueden deberse a la presencia de malwares, a falta de control o por propia ignorancia de cómo funcionan las cosas por parte del usuario. Los problemas que aparecen son:

Lentitud en la navegación. Generalmente se debe al ancho de banda saturado (descargar varias cosas a la vez, abrir un programa P2P que comparte conexiones, etc) de las cuales el usuario es consciente; pero otras veces, el usuario convive con su ancho de banda degradado por la presencia de malware (spam, adware, etc.) que está haciendo uso de él, sin que el usuario tenga conocimiento.

Imposibilidad de conexión a una web o a un servicio. Generalmente se trata de un problema técnico que puede estar radicado en el servidor de destino o en cualquiera de los enlaces que llegan hasta él. Este problema puede generar un perjuicio importante.

Problemas de virus. Los virus pueden borrar o modificar información, bloquear el funcionamiento o el acceso a archivos. Algunos navegadores han sido tradicionalmente permeable a los virus, ejecutando código sin que el usuario tenga conocimiento, y provocando diferentes problemas.

Espionaje. Existen muchas formas de levantar información y patrones de comportamiento de los usuarios desde el computador y enviarla a centros de recopilación. Estos sistemas espías buscan detectar preferencias, generalmente para definir estrategias de marketing.

Publicidad, spam. Esto es algo que todos hemos recibido sin consentimiento y en forma diaria. Casi que basta tener una casilla de correo para comenzar a conocer este problema. El resultado es un riesgo en la pérdida de información, en el uso excesivo de los recursos (ancho de banda, espacio en disco, etc.), en la efectividad para encontrar la información necesaria, y otras consecuencias del estilo.

En siglos anteriores las vías de comunicación entre las ciudades resultaban también lentas e inseguras (mal firme, guerras, bandidos...). Seguro que dentro de unos pocos años todos estos problemas de Internet también se habrán solucionado. De momento hay que conocerlos y tenerlos en cuenta: no podemos confiar que todo Internet esté siempre operativo a nuestra disposición y debemos proteger nuestro ordenador con un sistema antivirus/espionaje adecuado.

2.5. Riesgo de addicciones

Las adicciones en internet son conocidas como IAD (Internet Addiction Disorder). En toda adicción siempre confluyen tres elementos: una persona, unas circunstancias personales determinadas y una sustancia o situación que produzca placer. Las horas de conexión a Internet no puede considerarse un indicador significativo de un caso IAD, ya que las horas de conexión se pueden deber a distintos factores, no todos vinculados a una adicción. Incluso las horas de ocio utilizadas o empleadas en Internet tampoco pueden ser un elemento determinante. De todas formas, se puede considerar una adicción cuando la persona no es capaz de controlar su tiempo de conexión, relegando obligaciones familiares, sociales, profesionales y/o académicas. Llegando incluso a dejar de lado necesidades físicas (sueño, alimentación, higiene) por mantenerse conectado. Algunos servicios o contenidos utilizados en demasía pueden ser considerados adicciones, como ser:

Adicción a la información. Consiste en buscar noticias, navegar por blogs, webs temáticas, webs de servicios. Generalmente se trata de la búsqueda de una temática en particular (violencia, pornografía, etc.) con el objetivo de encontrar sensaciones.

Addicción a los entornos sociales. El adicto busca gente nueva continuamente, tratando de encontrar el apoyo en los grupos de la red, llegando a crear y mantener (socialmente) varias personalidades virtuales. Cuando no hay adicción la comunicación suele ser más restrictiva, solamente con los amigos.

Juego compulsivo. Internet está lleno de juegos, algunos de tipo casino y de apuestas, otros competitivos y violentos, que pueden llegar a fomentar ludopatías.

Compras compulsivas. Utilizar el comercio electrónico y/o la participación en subastas para la compra compulsiva de objetos.

Para superar estas adicciones que distorsionan la vida normal de los individuos, muchas veces será necesaria la ayuda de las personas próximas y de médicos especialistas. En el caso de los menores, es importante que los padres estén atentos al uso que hacen sus hijos de Internet y detecten estos problemas lo antes posible. A partir de los datos que proporciona un estudio realizado en noviembre de 2002 por las organizaciones de protección de la infancia ACPI[1] y PROTEGELES[2] sobre "*Seguridad Infantil y Costumbres de los Menores en Internet*", se consideran las siguientes características que alertan sobre una posible adicción a Internet: necesidad de conectarse con frecuencia y a diario o casi a diario, navegar más de 10 horas semanales, buscar sensaciones y visitar tanto páginas de pornografía como de violencia, entrar en los chats creando personalidades distintas y con frecuencia del sexo opuesto.

2.6. Riesgos por virtualización

A pesar de que los riesgos a los que estamos expuestos en Internet son básicamente los mismos que encontramos en el "mundo físico" (no olvidemos que al acceder a Internet accedemos a un mundo paralelo o ciberespacio que en gran medida lo imita), la naturaleza "virtual" de Internet y su creciente ubicuidad en nuestra sociedad, la novedad que representan sus servicios y nuestra poca experiencia en su uso (aún estamos en fase de descubrir muchas de sus posibilidades), introducen nuevos factores que aumentan estos riesgos:

Fácil acceso a la información. En el mundo físico suele resultar difícil, y muchas veces costoso económicamente, encontrar muchas de las informaciones peligrosas que en Internet se encuentran con facilidad, gratis, y hasta a veces aparecen de manera ocasional: por ejemplo al teclear erróneamente una palabra en una búsqueda. Por contra, en el "mundo físico" las restricciones legales a la distribución de contenidos pornográficos y violentos suelen alejarlos de los entornos infantiles, y la necesidad de dinero

[1] http://www.asociacion-acpi.org
[2] http://www.protegeles.com

para adquirir determinados materiales y hasta la entidad física de los mismos (que hay que guardar en algún lugar) contribuye a facilitar un cierto control parental.

Fácil comunicación interpersonal. En el mundo físico los contactos personales nos aportan más datos sobre las personas con las que nos relacionamos que pueden alertarnos ante conductas extrañas de algunos individuos que se nos acerquen. Además, las personas y grupos se mueven en determinados espacios físicos, que muchas veces suponen un inconveniente para coincidir con ellos. En Internet no hay distancias, todo está a nuestro alcance, y la virtualidad permite moverse por el ciberespacio con personalidades ficticias.

Accesibilidad permanente. Internet, cada vez más, está siempre a nuestro alcance, de manera que facilita la inmediata realimentación de las adicciones: violencia, ludopatía...

Anonimato. En Internet pueden realizarse muchas acciones de manera anónima, con un escaso control social, lo que permite a algunas personas realizar actos en el "mundo virtual" que no se atreverían a hacer en el "mundo físico": comportamientos poco respetuosos en chats, visitar casinos, proveerse de pornografía...

Capítulo 3

Redes sociales en Internet

El inicio de las redes sociales en Internet o servicio de redes sociales, lo podemos apreciar desde la aparición de las denominadas BBS[1] o tablones de anuncios, en los años 80 y 90, en nuestro medio una muy conocida fue Compuservice. A mediados y fines de los 90 los servicios de redes sociales empiezan a usar la World Wide Web, logrando gran popularidad. El uso masivo de estas redes ha incidido y generado interrogantes sobre la protección de los datos personales y la protección de la propiedad intelectual. Si bien los usuarios suben información en forma totalmente voluntaria, en algunos casos no se les explica suficientemente el uso que se puede o se va a hacer de dicha información. Lo mismo ocurre con la propiedad intelectual de los materiales que se suben a dichas redes. La normativa sobre lo anterior ha ido evolucionando y seguramente lo hará aún más a futuro. Un ejemplo, en un principio algunas redes sociales no exigían una relación de confianza mutua para poner a los usuarios en contacto, en estos momentos es prácticamente una regla en todas las redes sociales. Al establecer un contacto ambos interesados deben estar de acuerdo. Eso no implica que no sigan existiendo coleccionistas de contactos, que suman integrantes a su red social con la única finalidad de aparecer con un gran número de "amigos". Algunas de las redes sociales más utilizadas son Facebook[2], Myspace[3] y Orkut[4]. Sobre las dos primeras nos vamos a extender en particular, en estos momentos son las de mayor difusión y compiten por el primer lugar, si bien la tendencia, parece ser, a un mayor crecimiento de Facebook. Según el Informe de abril de 2007, Teens, Social Networks & Safety de Pew Internet and American life Project32, el 93 % de los norteamericanos de entre 12 y 17 años utilizan Internet, de los cuales un 55 % utiliza las redes sociales. Por otro lado, es esencial destacar que el 77 % de los menores que utilizan redes sociales tienen visible su perfil público, de los cuales un 59 % afirma que sólo pueden ver su perfil sus amigos [15].

[1] Bulletin Board System
[2] http://www.facebook.com
[3] http://www.myspace.com
[4] http://www.orkut.com

3.1. Facebook

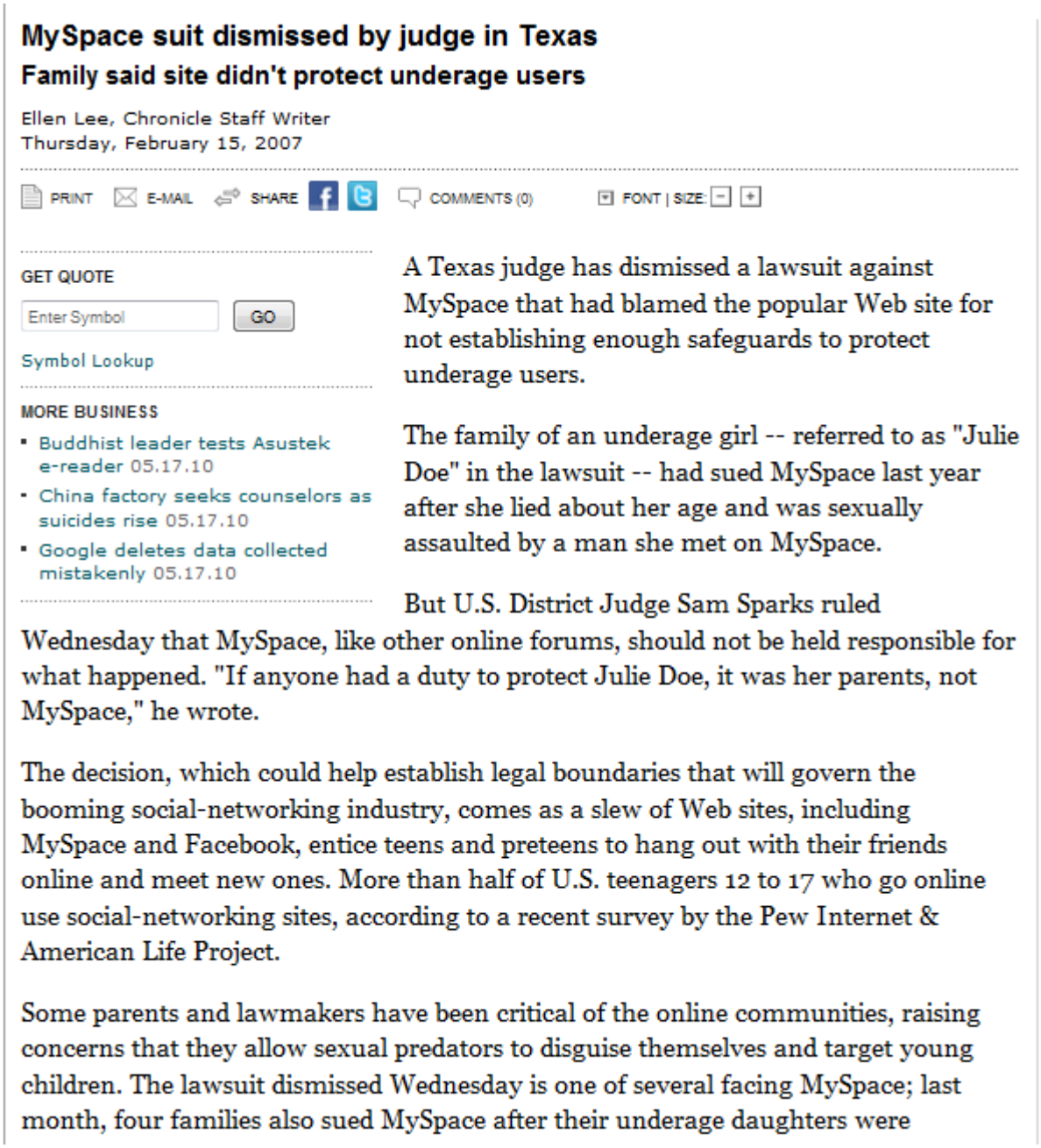
Facebook fue creada en 2004 por Mark Zuckerberg, como un sitio destinado a los estudiantes de la Universidad de Harvard. En enero de 2010, Facebook contaba con 380 millones de miembros, y traducciones a 70 idiomas, es el sitio más popular para subir fotografías con un promedio de más de 83 millones de fotos subidas a diario. Cuenta con más de 350 millones de usuarios a diciembre de 2009 [15].

3.2. MySpace

Surge en el 2003 y crece rápidamente, actualmente cuenta con más de 200 millones de usuarios. En el 2005 sufre serios problemas de seguridad siendo utilizada para difusión de virus y pishing. Lo cual la lleva a modificar sus políticas de seguridad. En julio de 2007, la compañía encontró y tuvo que eliminar las cuentas y perfiles de 29.000 delincuentes sexuales registrados en Estados Unidos. En febrero de 2007, un juez de EEUU desestimó una demanda contra MySpace iniciada por los padres de una niña de 13 años - a la que se refieren como Julie Doe en el juicio - que fue violada por un hombre que conoció a través de Myspace. El juez dictaminó que "*si alguien tenía el deber de proteger a la niña, eran sus padres, no Myspace*". Otro juez de Texas desestimó una demanda contra MySpace que había culpado al popular sitio Web por no establecer garantías suficientes para proteger a los usuarios menores de edad. Ver figura 3.1. "*Algunos padres de familia y legisladores han sido críticos de las comunidades en línea, aumentando su preocupación el que permitan a los depredadores sexuales disfrazarse y dirigirse a los niños pequeños. La demanda que se desestimó el miércoles es una de las varias que enfrenta MySpace; el mes pasado, cuatro familias también demandaron a MySpace después de que sus hijas, menores de edad, fueron asaltadas después de conocer hombres que habían encontrado primero en línea.*"

3.3. La privacidad en los servicios de redes sociales

Los ejemplos de los riesgos de subir información sensible a redes sociales son muchos y variados. Desde fotos que estimulan el ciberacoso hasta imágenes que hace daño a candidatos políticos. En nuestro medio hay claros ejemplos al respecto. El tema entonces es saber dosificar donde empieza lo privado y hasta donde confiamos en las redes sociales. Otro elemento importante a tener en cuenta es que una vez que un texto, imagen, video y/o audio circula por un cierto tiempo en una red social, luego es muy difícil que deje de circular por Internet, aún cuando demos de baja nuestra cuenta y los contenidos en cuestión. Es muy común hacer copias y divulgar en otros sitios los materiales que los usuarios de las redes sociales consideran interesantes. Algunos jóvenes al buscar trabajo vieron como sus posibilidades de conseguirlo se perdían, al saber que sus probables futuros empleadores los habían buscado en facebook y habían encontrado fotos comprometedoras de ellos. O simplemente mostrando una faceta poco profesional.



MySpace suit dismissed by judge in Texas

Family said site didn't protect underage users

Ellen Lee, Chronicle Staff Writer
Thursday, February 15, 2007

PRINT E-MAIL SHARE COMMENTS (0) FONT | SIZE:

GET QUOTE

Enter Symbol GO

Symbol Lookup

MORE BUSINESS

- Buddhist leader tests Asustek e-reader 05.17.10
- China factory seeks counselors as suicides rise 05.17.10
- Google deletes data collected mistakenly 05.17.10

A Texas judge has dismissed a lawsuit against MySpace that had blamed the popular Web site for not establishing enough safeguards to protect underage users.

The family of an underage girl -- referred to as "Julie Doe" in the lawsuit -- had sued MySpace last year after she lied about her age and was sexually assaulted by a man she met on MySpace.

But U.S. District Judge Sam Sparks ruled Wednesday that MySpace, like other online forums, should not be held responsible for what happened. "If anyone had a duty to protect Julie Doe, it was her parents, not MySpace," he wrote.

The decision, which could help establish legal boundaries that will govern the booming social-networking industry, comes as a slew of Web sites, including MySpace and Facebook, entice teens and preteens to hang out with their friends online and meet new ones. More than half of U.S. teenagers 12 to 17 who go online use social-networking sites, according to a recent survey by the Pew Internet & American Life Project.

Some parents and lawmakers have been critical of the online communities, raising concerns that they allow sexual predators to disguise themselves and target young children. The lawsuit dismissed Wednesday is one of several facing MySpace; last month, four families also sued MySpace after their underage daughters were

Figura 3.1: http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2007/02/15/BUGEKO4VU01.DTL&

3.4. Elementos a tener en cuenta

Las normas de seguridad para hacer un buen uso de las redes sociales son más o menos las mismas que hemos visto anteriormente. Pero en el caso de las redes sociales un elemento fundamental es cuidar la configuración de privacidad de la cuenta. En general es aconsejable configurar todos los items con el máximo nivel de seguridad, que los materiales que subimos solo puedan ser vistos solo por nuestro amigos. Y aún así tener cuidado con los materiales a subir. En el caso de los niños menores de 14 años, lo ideal es que no entren a Facebook u otras redes sociales usadas por adultos. Y tratar de que en todo caso utilicen redes creadas especialmente para niños. Por supuesto que el acompañamiento de la navegación por parte de los padres es fundamental.

3.5. La creación de redes sociales en Internet especialmente para niños

Existen redes especialmente creadas para niños, ejemplos:

- Recientemente, en 2009, surge Clan TV es una red social desarrollada con el apoyo de Radio Televisión Española y que apunta a ser controlada por los propios padres. La red no permite que los niños se registren solos, sino que deben ser registrados por sus padres, según dicha red "La comunidad infantil estará especialmente protegida. Por un lado nunca se presentarán datos de los niños; por otro todas las acciones estarán monitorizadas por los padres. De esta manera los niños pueden dar sus primeros pasitos en este nuevo entorno. Siempre con la garantía que tanto RTVE como sus padres están detrás de ellos apoyándolos."[24]
- Otro ejemplo es Kidswirl, la cual es muy parecida a Facebook en cuanto a interfase pero pensada para niños. Seguramente en breve aparezcan más redes sociales de este tipo, donde generalmente los padres son quienes hacen un seguimiento de sus hijos.

Capítulo 4

Sexting

Las primeras referencias al sexting datan de 2005 en la revista Sunday Telegraph. "*Mirar antes de saltar*" podría ser la frase para resumir como se debe manejar el tema de subir materiales a la web. El Sexting se relaciona con la costumbre, a través de los celulares u ordenadores, de enviar texto, fotos y/o videos propios, con la finalidad de excitar sexualmente al destinatario. Una encuesta realizada en EEUU en abril de 2009 por Cox Communications en asociación con el Centro Nacional para Menores Desaparecidos y Explotados y John Walsh, entre 655 adolescentes de entre 13 y 18 años, dió los siguientes resultados (Ver fuente): El 91 % de los adolescentes tienen una dirección de correo electrónico, el 72 % de los adolescentes tiene perfiles en redes sociales en línea, donde han publicado fotos de ellos y sus amigos junto con información personal. Más de 33 % de los adolescentes encuestados han sufrido ciberacoso o saben de casos, el 68 % piensan que es un problema grave. El 19 % ha participado en sexting, mediante envío o recepción de desnudos sugerentes. El 11 % reconocía que había enviado este tipo de material a gente que ni siquiera conocía. La difusión de este tipo de materiales se ha generado en buena medida por la facilidad que brindan hoy en día las TIC para difundir textos, fotos y/o videos. Desde el punto de vista legal se han generado grandes discusiones sobre si un adolescente que difunde fotos eróticas de otro adolescente debe o no ser acusado por difusión de pornografía infantil. Dado que el fenómeno es relativamente reciente aún no existe un marco legal claro al respecto. Lo fundamental para evitar los efectos negativos del sexting, que en muchos casos lleva al ciberacoso, es prevenir a los niños y niñas sobre las consecuencias negativas de difundir sus fotos en poses o actitudes inconvenientes, desnudos o semidesnudos, en redes sociales o a través de mensajes por celular (que luego pueden ir a parar a las redes sociales). "*La imagen era borrosa y la voz distorsionada, pero las palabras pronunciadas por una joven de Ohio eran inquietantes. Había enviado fotos de ella desnuda a su novio. Cuando se separaron, él las envió a otras chicas de su secundaria. Las chicas la estaban acosando, llamándola puta y diciendo que era una prostituta. Ella estaba triste y deprimida, con miedo incluso de ir a la escuela*"Y ahora Jesse Logan estaba en un canal de televisión de Cincinnati contando su historia. Su propósito era simple: "*Sólo quiero asegurarme de que nadie más tenga que pasar por esto otra vez*". Ver figura 4.1. La entrevista fue en mayo de 2008. Dos meses más tarde, Jessica Logan se ahorcó en su habitación. Tenía 18 años.[20]

4.1. Webcam y privacidad

Una escuela en EEUU, más precisamente Pennsylvania, instaló programas de monitoreo en la notebooks de los alumnos permitiendo vigilancia a través de la webcam inclusive en su domicilio. Ocurrió en el Lower Merion School District. Todo se descubrió cuando aplicaron una sanción a un estudiante por "conducta inadecuada en su casa". el subdirector del colegio utilizó una foto de la webcam del estudiante, tomada en su casa, como prueba. Luego los padres iniciaron una demanda.[18] Algunos proveedores de hardware ya están trabajando sobre el tema, una firma china GSOU está por sacar al mercado una webcam que se puede tapar, ya sea por software como presionando un botón en la misma.[25]

Her teen committed suicide over 'sexting'

Cynthia Logan's daughter was taunted about photo she sent to boyfriend

By Mike Celizic
TODAYshow.com contributor
updated 9:26 a.m. ET March 6, 2009

The image was blurred and the voice distorted, but the words spoken by a young Ohio woman are haunting. She had sent nude pictures of herself to a boyfriend. When they broke up, he sent them to other high school girls. The girls were harassing her, calling her a slut and a whore. She was miserable and depressed, afraid even to go to school.

And now Jesse Logan was going on a Cincinnati television station to tell her story. Her purpose was simple: "I just want to make sure no one else will have to go through this again."

The interview was in May 2008. Two months later, Jessica Logan hanged herself in her bedroom. She was 18.

Story continues below ↓

Video

Launch

'Sexting' leads teen to suicide
March 6: 18-year-old Jesse Logan took her own life after a nude picture of her was passed around by e-mail. TODAY's Matt Lauer talks to her mom, Cynthia Logan, and Internet safety expert Parry Aftab about the dangers of "sexting."
Today show

Figura 4.1: [20]


Zazzle Sites: Zazzle.es | Sell | Artsprojekt | LABz | International
¿Tienes una cuenta? Inscripción | Carrito | Mi Cuenta
zazzle .es
COMPRA
CREAR
VENTA
COMUNIDAD
Buscar 29.671.024.074 productos personalizables
Todos los Productos
Buscar
Portada > Humor, refranes > Gráficos extraños, fotos > Desconcierto
Vistas:
Modelo
Producto
Diseño
sexting
CONSEQUENCES
¡Personalízalo!
el sexting, consecuencias tshirt
Traducido por robots. Ver idioma original. (¿Que?)
Tamaño:
Elige un tamaño
Tabla de tallas
Cantidad:
1
camiseta. Sólo 7,46 € al por mayor
Agregar al carrito
11,65 €
por camiseta
Elige tu estilo y color
Ver todo...
Básica: Blanco
Camiseta básica
Camiseta básica
Camiseta Baby Doll para
Camisa EDUN LIVE Genesis
¡60 más!
Hombres
Mujeres
Joven
Bebé

Figura 4.2: [27]

Capítulo 5

Cyberbullying o Ciberacoso

Ciberacoso es el uso de las TIC (Tecnologías de la información y la comunicación) para acosar a un individuo o grupo. El término Cyberbullying fue usado por primera vez por el educador canadiense Bill Belsey. " *Ciberacoso implica el uso de tecnologías de información y comunicación para apoyar deliberada y repetida, y el comportamiento hostil por parte de un individuo o grupo, que se destina a dañar a otros.* Bill Belsey Una investigación de julio de 2008, realizada por Microsoft y presentada por Julie Inman Grant (Director del área de seguridad de Microsoft para el Asia y el Pacifico) detecto que un 25 % de los niños habían sufrido de Ciberacoso, un 31 % de los niños entre 14 y 17 años y un 21 % de niños entre 10 y 13 años. Uno de los elementos que estimula este tipo de conducta es la sensación de anonimato que brinda Internet. Por otra parte debemos entender que los jóvenes son la fuente más poderosa de influencia sobre otros jóvenes. En EEUU se dió un caso muy grave donde una joven se suicidó luego de ser acosada por la madre de una ex-amiga, el caso tuvo fuerte repercusión en la prensa: " *LOS ANGELES - Un jurado federal que aquí emitió lo que los expertos legales dijeron que fue el primer veredicto del país en un caso de cyberbullying, condena a una mujer de Missouri de tres cargos de delito menor por fraude informático por su participación en la creación de una cuenta falsa en MySpace para engañar a un adolescente, que luego se suicidó . El jurado no pudo con un cuarto cargo de conspiración contra la mujer, Lori Drew, de 49 años, el juez, George H. Wu de Tribunal Federal de Distrito, declaró nulo el juicio por ese delito. Aunque no está claro qué tan gravemente la Sra. Drew será castigada - el jurado redujo los cargos de delitos graves a delitos menores y no hay fijada fecha de sentencia - la condena fue muy significativa, según los expertos en fraude informático, porque es la primera vez que una ley federal para luchar contra los delitos informáticos se utiliza para procesar a alguien por abusar en el uso de una red social.*" Ver figura 5.1.[21]

1. Se debe establecer con el niño o niña un vinculo de confianza, de manera tal que los mismos puedan recurrir al docente o sus padres para contar un caso de acoso, ya sea de otros niños o adultos. No se debe hacer pensar a los niños que si son víctimas de un ataque a través de Internet se les va a impedir usar la computadora.

2. Lo primero, una vez sospechado un caso de ciberacoso es apoyar al niño, no magnificar ni minimizar el problema, conversar con él para ir recabando

Verdict in MySpace Suicide Case

Jonathan Alcorn for The New York Times

Lori Drew, center, of suburban St. Louis arriving Wednesday at the courthouse in Los Angeles with her daughter Sarah.

By JENNIFER STEINHAUER
Published: November 26, 2008

SIGN IN TO RECOMMEND
TWITTER
SIGN IN TO E-MAIL OR SAVE THIS
PRINT
REPRINTS
SHARE

LOS ANGELES — A federal jury here issued what legal experts said was the country's first cyberbullying verdict Wednesday, convicting a Missouri woman of three misdemeanor charges of computer fraud for her involvement in creating a phony account on MySpace to trick a teenager, who later committed suicide.

Related

Indictment (U.S. v. Drew) (findlaw.com)

Tina Meier, via Associated Press

Megan Meier, 13, who committed

The jury deadlocked on a fourth count of conspiracy against the woman, Lori Drew, 49, and the judge, George H. Wu of Federal District Court, declared a mistrial on that charge.

Although it was unclear how severely Ms. Drew would be punished — the jury reduced the charges to misdemeanors from felonies, and no sentencing date was set — the conviction was highly significant, computer fraud experts said, because it was the first time that a federal statute designed to combat computer crimes was used to prosecute what were essentially abuses of a user agreement on a social networking site.

Figura 5.1: [21]

datos que permitan darle su real magnitud al caso.

3. Se debe evitar que el niño responda de la misma manera, reproduciendo la conducta del acosador. Eso solo sirve para agravar la situación y dar argumento al o los posibles acosadores. No responder, no seguir con la discusión desalienta al o los acosadores. En caso de verse obligado a responder, no se debe insultar al o los acosadores, se debe dar una respuesta firme y correcta desestimulante.

4. Al niño acosado se le debe dejar en claro que él no es culpable de lo que le ocurre, buscando reforzar su autoestima. Lo que generalmente busca el acosador es destruir la autoestima de la víctima.[4] [2] [31]

5. Algunas medidas a tomar luego de detectado un ciberacoso grave son:

   - Bloquear al agresor o ponerse en contacto con el administrador de la red para que él lo haga si es posible y según el ámbito.
   - Cambiar la dirección de correo electrónico.
   - Cambiar de usuario en una red social.
   - No borrar las pruebas.
   - Hacer la denuncia correspondiente.

6. Se debe explicar a los niños los daños que produce el ciberacoso y desestimular que se conviertan en testigos silenciosos del problema o cómplices de un acosador.

7. Para prevenir el acoso es conveniente tomar las siguientes medidas:

   - No difundir los datos personales en forma indiscriminada.
   - Buscarse a uno mismo en Internet cada cierto tiempo a fin de detectar publicaciones negativas.
   - No responder a las provocaciones, eso estimula aún más al acosador.
   - No enviar mensajes cuando uno está muy molesto por algo.
   - Estimular la empatía, explicar a los niños y niñas el daño que causa el acoso.
   - Explicar también las consecuencias negativas que puede tener para el o los acosadores.
   - Difundir el uso de la "*Netiquette*"

Capítulo 6

Pornografía infantil

6.1. Definición

El Grupo de Interpol Especializado en Crímenes contra los Niños utiliza la siguiente definición:

"La pornografía infantil se crea como consecuencia de la explotación o abuso de un niño. Puede definirse como toda forma de representación o promoción de la explotación sexual de los niños, incluidos los materiales escritos y de audio, que se concentren en la conducta sexual o los órganos genitales de los niños."

La definición de ECPAT refleja en gran medida la de Interpol:

"Pornografía visual: representación visual de un niño que lleva a cabo una actividad explícitamente sexual, real o simulada, o la exhibición obscena de genitales concebida parra la gratificación sexual del usuario; implica la producción, distribución y/o uso de dicho material. Pornografía de audio: El uso de cualquier dispositivo de audio que utilice la voz de un niño, real o simulada, destinada a conseguir la gratificación sexual del usuario; implica la producción, distribución y/o uso de dicho material."

El borrador de la Convención sobre el Delincuencia Informática del Consejo de Europa manifiesta que:

"*pornografía infantil*" incluirá material pornográfico que muestre visualmente a un menor entregado a una conducta sexualmente explícita; una persona con aspecto de menor entregada a una conducta sexualmente explícita; imágenes realistas que representen a un menor entregado a una conducta sexualmente explícita.

Recientemente se ha agregado, por parte de la Comisión de Derechos de la Mujer e Igualdad de Oportunidades del Parlamento Europeo, una solicitud de enmienda 18 a la definición de pornografía infantil, planteando que debe considerarse como pornografía infantil el material "*auditivo, visual o escrito que represente a niños con la intención de incitar deseos sexuales*".

6.2. Formas de difusión

1. Correo electrónico.

2. Canales de Chat.

3. Sitios Web

4. Comunidades virtuales

5. Programas P2P

6.3. Conclusiones de la investigación realizada para el IIN (Instituto Interamericano del Niño) año 2005

La difusión de pornografía infantil en la subregión es una realidad fácilmente palpable, todos los equipos de investigación fueron claros sobre la facilidad con que se puede acceder a materiales de pornografía infantil a través de Internet.

El material de pornografía infantil circula sin que sus distribuidores deban utilizar ningún sistema de camuflaje o encriptación del mismo, lo cual es índice claro del bajo control existente sobre esta forma de delito.

El nivel de permisividad para la difusión de la pornografía infantil, llega a extremos tales, que existen muchos sitios web, fuera de la subregión, que venden pornografía infantil mediante el uso de tarjetas de crédito.

Se ha detectado la utilización de palabras relacionadas con la pornografía infantil en metatags a fin de aumentar el número de visitas de algunos sitios web. Lo cual es una nueva manera de explotar el tema de la pornografía infantil.

El importante, rápido y sostenido crecimiento en el uso de Internet, en América Latina y el Caribe, ha sido funcional a la difusión de pornografía infantil. Y consideramos que ha sido uno de los motivos por los que, a diferencia de lo que sucede en los países desarrollados, los difusores de pornografía infantil no han necesitado utilizar recursos de encriptación de archivos.

Si bien en algunos países de la subregion no se ha detectado producción de pornografía infantil con destino a Internet, existen indicadores de que la misma podría existir aún en estos países donde no se ha detectado.

De acuerdo con el perfil de los niños, niñas y adolescentes utilizados por las redes de producción de pornografía infantil en la subregion, surge claramente que la situación de calle y la pobreza son elementos de riesgo fundamentales.

Tal cual surge del trabajo de investigación Análisis de las formas de difusión de la pornografía infantil a través de Internet "*Uno de los elementos que consideramos importante destacar es que las distintas formas de difusión de la pornografía infantil a través de Internet actúan en forma sinérgica, potenciándose unas a otras. Por otra parte la difusión de pornografía infantil a través de Internet es un proceso dinámico, los sitios más comprometidos cambian de nombre permanentemente así como las comunidades virtuales y las direcciones de correo de los usuarios. Lo que actúa como elemento de actualización en tiempo real de esta información son los canales de chat. Esto nos lleva a pensar que si bien habría que atacar el problema en todas sus formas, tal vez acentuar el trabajo en torno a los canales de chat dé buenos resultados.*"[6]

6.4. Recomendaciones de la investigación realizada para el IIN año 2005

Es fundamental evitar que se siga reproduciendo uno de los principales factores de abuso, que es la venta de pornografía infantil a través de Internet mediante el uso de tarjeta de crédito, la cual además de favorecer el consumo, financia el abuso de más niños, niñas y adolescentes. Para ello es importante involucrar a los emisores de tarjetas de crédito en la lucha contra la pornografía infantil y/o legislar al respecto.

Se debe estimular la creación de un marco legal global con relación a la difusión de pornografía infantil a través de Internet, ya que dadas las características propias de Internet – una red global – es imposible que medidas de legislación locales puedan solucionar el problema.

Es necesario sensibilizar a las empresas que brindan alojamiento a comunidades virtuales, sitios web y/o canales de Chat, y/o legislar, para que se hagan responsables de controlar los materiales alojados en sus servidores y/o financien grupos independientes encargados de realizar el control de los contenidos existentes.

Los proveedores de servicios de Internet, que permitan el acceso a canales de Chat, deberían también disponer de espacios de intercambio con moderador, dirigidos especialmente a niños y promocionar dichos espacios.

Toda computadora vendida en el mercado debería ir acompañada, de un documento escrito en un lenguaje accesible, que explique las normas básicas sobre la seguridad en línea de los niños. Esta medida también se podría extender a las facturas de las empresas que brinda conexión a Internet.

Se debería habilitar en la región un sitio web con la finalidad de recibir denuncias sobre pornografía infantil y unificar las denuncias realizadas.

Es necesario desarrollar software más eficiente para enfrentar el fenómeno de la pornografía infantil, tanto para detectar los sitios como para proteger a los niños mientras navegan por Internet.

Se debe sensibilizar a las empresas que manejan los buscadores de Internet y/o legislar, a fin de que borren el respaldo de los sitios de pornografía infantil y los eliminen a su vez de los índices de búsqueda.

Las empresas que brindan servicios de conexión a Internet, debería volcar parte de sus ganancias a la lucha contra la pornografía infantil y a la protección de los niños en situación de riesgo.

A nivel educativo se debe capacitar al personal docente en la detección y manejo de niños utilizados y/o expuestos a la pornografía infantil. Se debe brindar una educación sexual destinada a que niños, niñas y adolescentes no estén indefensos frente a lo que pueden encontrar en Internet. Se debe preparar los adolescentes, mediante el abordaje no solo de los aspectos de anatomía y fisiología de la sexualidad, sino tomando también en cuenta los aspectos culturales, estimulando el análisis crítico de los mensajes.

El fenómeno de la pornografía infantil debe ser atacado mediante la conformación de equipos multidisciplinarios que encaren el análisis del tema, formulando propuestas concretas, destinadas a atacar la difusión de la pornografía infantil desde todos los ángulos posibles. Se debe capacitar a los padres sobre los aspectos positivos y negativos de Internet.

Se debe disponer de recursos para la la identificación de las víctimas y su

atención.

Es necesario desarrollar campañas de sensibilización social con relación al tema e informar a la población respecto de esta problemática. En última instancia únicamente la prevención mediada por una asistencia a los niños, niñas y adolescentes en situación de riesgo, tanto de ser expuestos a la pornografía infantil como de convertirse en actores de la misma, servirá para modificar la situación en el futuro[9].

Capítulo 7

Malware

Malware (del inglés malicious software, también llamado badware, software malicioso o software malintencionado) es un software que tiene como objetivo infiltrarse en el sistema y/o dañar la computadora sin el conocimiento de su dueño, con finalidades muy diversas, ya que en esta categoría encontramos desde un troyano hasta un spyware [34]. Esta expresión es un término general muy utilizado por profesionales de la computación para definir una variedad de software o programas de códigos hostiles e intrusivos. Muchos usuarios de computadores no están aún familiarizados con este término y otros incluso nunca lo han utilizado. Sin embargo la expresión "virus informático" es más utilizada en el lenguaje cotidiano y a menudo en los medios de comunicación para describir todos los tipos de malware. Se debe considerar que el ataque a la vulnerabilidad por malware, puede ser a una aplicación, una computadora, un sistema operativo o una red. Es importante tener en cuenta que no todos los sistemas operativos tienen la misma vulnerabilidad con relación al malware, principalmente por temas de arquitectura y opción en cuanto a paradigmas de seguridad, algunos sistemas como GNU/Linux son menos vulnerables.

7.1. Adware

Un programa se considera un **adware** cuando automáticamente ejecuta, muestra o baja publicidad al computador. 'Ad' en la palabra 'adware' se refiere a 'advertisement' (anuncios) en inglés. Algunos programas de tipo *shareware* encuentran su financiamiento por el método de adware, ofreciendo quitar la propaganda cuando se registra el programa. Algunos pogramas adware también incluyen código para seguimiento del usuario, entrando en la categoría de *spyware*.

7.2. Backdoor o Puerta Trasera

Una puerta trasera o backdoor es un método para eludir los procedimientos normales de autenticación a la hora de conectarse a una computadora. Una vez que el sistema ha sido comprometido (p.ej. mediante un troyano) una puerta trasera puede ser instalada para permitir un acceso remoto más fácil en el futuro. Las puertas traseras también pueden ser instalados previamente al software

malicioso para permitir la entrada de los atacantes. Los crackers[1] suelen usar puertas traseras para asegurar el acceso remoto a una computadora, intentado permanecer ocultos ante una posible inspección. Para instalar puertas traseras los crackers pueden usar *troyanos*, *gusanos* u otros métodos.

7.3. Bomba fork

Con el nombre de **bomba fork** se conoce al programa (código ejecutable) que una vez ejecutado comienza a correr muchas copias de si mismo, de manera incontrolada y, cada una de las copias, hace exactamente lo mismo, es decir, correr más copias de si mismo. Generalmente se trata de códigos muy sencillos que logran este efecto valiéndose de algoritmos recursivos. Provocan el efecto de sobrecargar el sistema hasta que el mismo deja de ser utilizable.

7.4. Botnet

Botnet es la identificación de programas que actúan como robots informáticos, también conocidos como *bot*, que trabajan de forma autónoma y automática. La idea es controlar con ellos computadores en forma remota y con fines, generalmente, poco éticos. El uso más frecuente de los botnets es para el envío de spam, para la descargas de archivos en forma ilegal y para realizar ataques distribuidos de denegación de servicio (DDoS).

7.5. Bug

Es un defecto de software (*computer bug* en inglés), es el resultado de un fallo o deficiencia durante el proceso de creación de programas de computador (software). Dicho fallo puede presentarse en cualquiera de las etapas del ciclo de vida del software aunque los más evidentes se dan en la etapa de desarrollo y programación. No se trata de errores intencionales y se puede afirmar que todo el software va a fallar en algún momento, develando un bug.

7.6. Cookies

Una cookie es un fragmento de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página. Esta información puede ser luego recuperada por el servidor en posteriores visitas. Los usos más frecuentes de las cookies son:

- Llevar el control de usuarios: cuando un usuario introduce su nombre de usuario y contraseña, se almacena una cookie para que no tenga que estar introduciéndolas para cada página del servidor. Sin embargo una cookie no identifica a una persona, sino a una combinación de computador-navegador-usuario.

[1] Cracker se suele decir a la persona que accede al computador sin autorización con el objetivo de provocar daño.

- Conseguir información sobre los hábitos de navegación del usuario, e intentos de spyware, por parte de agencias de publicidad y otros. Esto puede causar problemas de privacidad y es una de las razones por la que las cookies tienen sus detractores.

Las cookies tienen implicaciones importantes en la privacidad y el anonimato de los usuarios de la web. Aunque las cookies sólo se envían al servidor que las definió o a otro en el mismo dominio, una página web puede contener imágenes y otros componentes almacenados en servidores de otros dominios. Las cookies que se crean durante las peticiones de estos componentes se llaman cookies de terceros.

7.7. Crackers

Se trata de una persona con altos conocimientos en informática y seguridad cuyo objetivo es algún beneficio personal o hacer daño. Se debe diferenciar el cracker del termino *hacker*: El hacker es aquél que accede a computadores, saltando las restricciones de seguridad impuestas, pero con objetivos éticos (verificar seguridad, lograr interoperabilidad, etc.) Tanto los crackers como los hackers utilizan los mismos procedimientos, por lo cual poseen conocimientos equivalentes; no obstante los crackers se identifican por sus objetivos no-éticos.

7.8. Cryptovirus, Ransomware o Secuestradores

Los ransomware, también llamados criptovirus o secuestradores, son programas que encriptan los archivos importantes para el usuario, haciéndolos inaccesibles, y piden que se pague un rescate"para poder recibir la contraseña que permite recuperar los archivos.

7.9. Dialers

Se trata de un programa que marca un número de teléfono de tarifa especial usando el módem. Los marcadores telefónicos son legítimos siempre y cuando no incurran en alguna de las siguientes actividades:

1. No se avisa de su instalación en la página que lo suministra.
2. Hace una reconexión a Internet sin previo aviso, o lo intenta.
3. Se instala silenciosamente en el ordenador utilizando vulnerabilidades del navegador, programa de correo electrónico (email), otros programas de acceso a Internet o el propio sistema operativo.
4. Puede dejar un acceso directo al escritorio sin conocimiento del usuario.
5. Puede instalarse unido a otros programas como barras de mejora para el navegador.
6. No informa de los costes de conexión.

Actualmente los modem por discado telefónico están dejando de ser un modo primordial de conexión, por lo que los dialers han perdido relevancia.

7.10. Exploit

Exploit (del inglés: explotar o aprovechar) es una programa, un fragmento de datos, o una secuencia de comandos con el fin de automatizar el aprovechamiento de un error, fallo o vulnerabilidad conocida. El objetivo es causar algún comportamiento no deseado o imprevisto en los programas informáticos, hardware, o componente electrónico (por lo general computarizado). Con frecuencia, esto incluye cosas tales la toma de control de un sistema o permitir la escalada de privilegios o un ataque de denegación de servicio. El fin del Exploit puede ser violar las medidas de seguridad para poder acceder al mismo de forma no autorizada y emplearlo en beneficio propio o como origen de otros ataques a terceros.

7.11. Falso antivirus

También se los conoce como **rogue software** hacen creer al usuario que la computadora está infectada por algún tipo de virus u otro tipo de software malicioso, esto induce al usuario a pagar por un software inútil o a instalar un software malicioso que supuestamente elimina las infecciones, pero el usuario no necesita ese software puesto que no está infectado.

7.12. Hijacker

Los hijackers son programas que realizan cambios en la configuración del navegador web, por ejemplo, cambiar la página de inicio del navegador por páginas web de publicidad o pornográficas, otros redireccionan los resultados de los buscadores hacia páginas con anuncios. También pueden llegar a técnicas más dañinas como interceptar el ingreso a bancos para redirigir el navegador a páginas de phishing.

7.13. Hoaxes, Jokes o Bulos

Un bulo (en inglés, hoax) o noticia falsa es un intento de hacer creer a un grupo de personas que algo falso es real. En el idioma español el término se popularizó principalmente al referirse a engaños masivos por medios electrónicos, especialmente Internet. A diferencia del fraude el cual tiene normalmente una o varias víctimas y es cometido con propósitos delictivos y de lucro ilícito, el bulo tiene como objetivo el ser divulgado de manera masiva haciendo uso de los medios de comunicación, siendo el más popular de ellos en la actualidad Internet, encontrando su máxima expresión en los foros y en las cadenas de mensajes de los correos electrónicos. No suelen tener fines lucrativos o no son su fin primario y sin embargo pueden llegar a resultar muy destructivos. Las personas que crean bulos tienen diversas motivaciones dentro de las que se encuentran el satisfacer su amor propio; el estar amargado con el trabajo en la empresa arremetiendo contra ella o sus trabajadores (hoy es muy fácil a través de internet); la intención de hacer una broma para avergonzar o señalar a alguien o la pretensión de provocar un cambio social haciendo que la gente se sienta prevenida frente a algo o alguien; querer mofarse y hacer evidente la credulidad de las personas y

de los medios de comunicación; también suele ser característico dentro de los autores de bulo el querer que los demás se adscriban a una determinada idea o pensamiento.

7.14. Keystroke o keyloggers

Es un tipo de software que se encarga de registrar las pulsaciones que se realizan en el teclado, para memorizarlas en un fichero y/o enviarlas a través de internet. Suele usarse como malware del tipo residente, permitiendo que otros usuarios tengan acceso a contraseñas importantes, como los números de una tarjeta de crédito, u otro tipo de información privada que se quiera obtener. El registro de lo que se teclea puede hacerse tanto con medios de hardware como de software. Los sistemas comerciales disponibles incluyen dispositivos que pueden conectarse al cable del teclado (lo que los hace inmediatamente disponibles pero visibles si un usuario revisa el teclado) y al teclado mismo (que no se ven pero que se necesita algún conocimiento de como soldarlos para instalarlos en el teclado). Escribir aplicaciones para realizar keylogging es trivial y, como cualquier programa computacional, puede ser distribuido a través de un troyano o como parte de un virus informático o gusano informático. Se dice que se puede utilizar un teclado virtual para evitar esto, ya que sólo requiere clics del ratón. Sin embargo, la aplicaciones más nuevas también registran screenshots (capturas de pantalla) al realizarse un click, que anulan la seguridad de esta medida. Cabe decir que esto podría ser falso ya que los eventos de mensajes del teclado deben ser enviados al programa externo para que se escriba el texto, por lo que cualquier keylogger podría registrar el texto escrito mediante un teclado virtual.

7.15. Lamer

Al igual que el *cracker*, el **lamer** se trata de una persona. Lamer es un anglicismo propio de la jerga de Internet que hace alusión a una persona falta de habilidades técnicas, sociabilidad o madurez considerada un incompetente en una materia, actividad específica o dentro de una comunidad, a pesar de llevar suficiente tiempo para aprender sobre la materia, actividad o adaptarse a la comunidad que le considera un lamer. Se trata de una persona que presume de tener unos conocimientos o habilidades que realmente no posee y que no tiene intención de aprender. Lo exactamente opuesto a un lamer es un *hacker*, que suele tener gran cantidad de conocimientos, no presume de ellos y los usa con fines éticos.

7.16. Pharming

El pharming es una técnica que suplanta al DNS, modificando el archivo hosts, para redirigir el dominio de una o varias páginas web a otra página web, muchas veces una web falsa que imita a la verdadera. Esta es una de las técnicas usadas por los hijackers en la modificación del sistema de navegación. El objetivo va desde mostrar propaganda (que alguien paga para que sea mostrada) hasta suplantar la página de acceso a un banco, para acciones de phishing.

7.17. Phishings

Phishing es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas

7.18. Rabbit o conejos

Se trata de un software que tiene un comportamiento semejante a los *virus* y a los *forks*, ya que cada vez que se copia a si mismo se pone a ejecutar, es decir crea instancias de si mismo corriendo simultáneamente. El objetivo es crear un efecto de denegación de servicios con programas válidos difícil de detectar.

7.19. Riskware

En sí, el **riskware** no es un programa considerado malware. Sino que se trata de un software, que por su función se considera un punto potencialmente crítico para acceder a crear daño dentro de la computadora. Generalmente se trata de software que puede detener la computadora o servicios que ella está prestando. Este software, que existe en todos los equipamientos informáticos, se utiliza con fines administrativos.

7.20. Rootkit

El rootkit, más que un software es una técnica de la cual se valen los programas maliciosos que son catalogados como rootkit para ocultarse al usuario (por ejemplo, evitando aparecer en la lista de procesos en ejecución o al explorador de archivos). Para esto los rootkit se valen de modificaciones al sistema operativo. Originalmente, un rootkit era un conjunto de herramientas instaladas por un atacante en un sistema Unix donde el atacante había obtenido acceso de administrador (acceso root). Actualmente, el término es usado mas generalmente para referirse a la ocultación de rutinas en un programa malicioso.

7.21. Spam

Correo no solicitado que se envía en forma masiva. El problema del spam es la recarga de los sistemas. Se trata de millones de correos que son enviados en forma masiva con distintos mensajes (algunos válidos y otros engañosos), que buscan ser filtrados en forma efectiva. Muchas veces el SPAM es utilizado para obtener direcciones de correo de contactos, validar direcciones de correo o permitir que el usuario instale malware en su computador.

7.22. Spyware

Los programas spyware son creados para recopilar información sobre las actividades realizadas por un usuario. El objetivo es distribuir esta información a agencias de publicidad u otras organizaciones interesadas. Los datos que recogen los spyware varían según las necesidades, desde información de las páginas web visitadas hasta direcciones de Email (para luego enviarles spam). La mayoría de los programas spyware son instalados como troyanos junto a software deseable bajado de Internet. Aunque algunos programas spyware recogen la información mediante cookies de terceros. También es muy utilizado el mecanismo de instalar barras de herramientas en los navegadores web. Algunos autores de spyware intentan actuar de manera legal y se presentan abiertamente como empresas de publicidad e incluyen unos términos de uso, en los que se explica de manera imprecisa el comportamiento del spyware, que los usuarios aceptan sin leer o sin entender [26].

7.23. Troyano

Los troyanos son programas maliciosos que están disfrazados como algo inocuo o atractivo, que invitan al usuario a instalarlo o ejecutarlo. Un ejemplo típico suelen ser los salva pantalla, pero puede estar oculto dentro de cualquier otro tipo de software de aspecto no-malicioso. Los troyanos suelen tener un efecto inmediato no deseado, desde borrar archivos, hasta descargar software adicional no-deseado o malicioso. Los troyanos conocidos como "droppers" son usados para empezar la propagación de un gusano inyectándolo dentro de una red local de un usuario.

7.24. Virus informático

El virus informático es un tipo de programa (software) que al ejecutarse logra copiarse a si mismo, generalmente incluyendo su código dentro de otro programa ejecutable de la misma computadora. También pueden tener funcionalidades adicionales que realicen otras acciones maliciosas, por ejemplo, borrar archivos o afectar los anti-virus para evitar ser detectados.[7]

7.25. Ventanas emergentes/POP-UPS

En las ventanas emergentes, aparte de ser una molestia para el usuario, pueden contener código malicioso que se ejecuta por el navegador en forma automática. También suelen ser utilizadas para mostrar elementos no deseados, vincular a sitios no aptos e incluso, contaminar la visual del navegante para que este se confunda al dar datos o navegar. Muchas veces las ventanas emergentes, mientras están abiertas, pueden rastrear la información que el usuario trasmite y/o recibe, convirtiéndose en *spyware*. Las ventanas emergentes no son un problemas en sitios conocidos y de confianza, donde generalmente prestan una utilidad para el usuario.

7.26. Worms o gusanos

Se trata de un programa que se transmite a sí mismo, explotando vulnerabilidades, en una red de computadoras para infectar otros equipos. El principal objetivo es infectar a la mayor cantidad de usuarios posible, también puede contener instrucciones dañinas al igual que los virus. La principal diferencia que tiene un gusano con un virus, es que el gusano contagia por sí solo, buscando acceder a otros computadores, mientras que el virus requiere de alguna intervención del usuario.

Capítulo 8

Cómo protegerse

8.1. Normas generales de seguridad en el uso del computador

Generalmente como usuario consideramos que el computador lo podemos usar, mientras que otros se encargarán de mantener la seguridad. Así día a día nos sentamos felices frente a nuestras pantallas para disfrutar de la experiencia y mantenemos una displicencia e inocencia frente a los problemas y riesgos de seguridad. Pero el primer nivel de seguridad debe estar en usted mismo. Comience a pensar y a incorporar la idea de que no está en un mundo seguro, que su computador vive en un medio peligroso cada vez que se conecta a Internet, cada vez que enchufa un pen-drive o que instala y abre un nuevo programa [22]. Igual que cuando subimos a nuestros vehículos para ir a trabajar, significa un riesgo. Cuando manejamos nuestro vehículo sabemos que debemos detenernos en las esquinas, mantener una velocidad segura, abrochar nuestro cinturón de seguridad, cuidarnos del auto que va al lado, atender si el de adelante frena y muchas cosas más, que no hacen a la propia tarea de conducir, sino que hacen a nuestra seguridad. En computación es igual, pero solemos ser muy despreocupados por los temas de seguridad. No debemos llegar a grados de paranoia inconducentes, pero debemos ser conscientes de los riesgos y nosotros mismos tomar la decisión de cuándo queremos enfrentar un riesgo, tal cual como cuando usamos el celular mientras manejamos.

8.2. Evite los riesgos y piense

Usted es el responsable directo por su seguridad, por la seguridad de sus datos y por que su computador siga funcionando. Si no conecta su computador a ninguna red y no conecta elementos externos a su computador eso ya lo mantiene seguro. Por supuesto, no se puede hacer eso, pues hoy día tenemos que estar conectados e intercambiar datos, es fundamental para que realizar nuestras actividades.

8.3. Filtros de Contenido

Un filtro de contenido (también conocido como censorware, control parental, filtro anti-pornografía) se refiere a un programa diseñado para controlar qué contenido se permite mostrar, especialmente para restringir el acceso a ciertos materiales de la Web [13]. El filtro de contenido determina qué contenido estará disponible en una máquina o red particular. Para esto se trabaja generalmente a dos niveles: Un nivel previo al acceso, cuando se pide acceso a una página web, el sistema posee listas de páginas prohibidas o listas de páginas autorizadas, dependiendo de lo cual, autoriza el acceso o lo deniega. Obviamente, por tratarse de listados los problemas con este sistema puede ser demasiado restrictivo y difícil de administrar. Un nivel posterior al acceso, donde el software lee previamente la página antes de mostrársela al usuario, decidiendo si el contenido es hábil para ser mostrado. Generalmente se utiliza un análisis de palabras reservadas, lo que puede generar algunos "falsos-positivos", por ejemplo al acceder al sitio http://www.diputados.gub.uy/, que contiene la palabra "puta" que podría estar prohibida También se utilizan análisis morfológicos de páginas, buscando patrones que suelen ser seguidos por páginas del tipo que se desea prohibir. Pero generalmente estos patrones suelen ser disimulados por muchos sitios cuando saben que con prohibidos. El motivo suele ser para prevenir a las personas ver contenido que el dueño de la computadora u otras autoridades consideran objetable. Los usos comunes de estos programas incluyen padres que desean limitar los sitios que sus hijos ven en sus computadoras domésticas, escuelas con el mismo objetivo, empleadores para restringir qué contenidos pueden ver los empleados en el trabajo.

8.4. Control paterno

El software de Control Paterno es una herramienta bastante útil para tener controlado los lugares a donde acceden los hijos. Es posible un control muy efectivo de los sitios que pueden ser visitados, también realizan un control sobre los textos que se intercambian por chat, las direcciones electrónicas a las que se puede escribir correo, llegando inclusive a controlar cuáles son las carpetas o los archivos que pueden ser accedidos. De todas formas, los software de control paterno siempre están "detrás del problemaçerrando la puerta a los sitios más obvios. Esta realidad, conocida por los productores de contenido, puede ser saltada con ciertas técnicas como ser:

- colocar el contenido detrás de un nombre inocente
- presentar el contenido dentro de un juego (p.ej en flash)
- presentar el contenido dentro de archivos multimedia (videos, sonidos, etc.)

Por lo que, suele ser una mejor opción el auto-control que el propio niño pueda hacer, basado en conversaciones sinceras y francas son sus padres, de forma que ellos entiendan la responsabilidad y las consecuencias de sus actos en Internet.

Capítulo 9

Asegurar la Navegación

Cuando hablamos de navegación segura nos queremos focalizar en aquellas precauciones o configuraciones que podemos tomar y configurar como navegantes, para evitar tener problemas o incidentes de seguridad [19].

9.1. Algunos consejos básicos

Utilice un navegador seguro, como Mozilla Firefox. Mozilla Firefox ha demostrado ser un navegador con altas consideraciones de seguridad, ampliación de funcionalidades mediante complementos y muchas otras prestaciones.[8]

Mantenga actualizado su antivirus. Busque y mantenga un antivirus actualizado en su sistema [11].

Active su cortafuegos (firewall) , evitará que en caso que algo ingrese a su computador pueda dejarlo desprotegido permitiendo conexiones no deseadas, desde Internet.

Bloquear ventanas emergentes , las ventanas emergentes pueden confundirlo con propaganda no deseada o pedidos de clave cuando no es necesario, tomando información de otros sitios y no del sitio principal en el cuál Ud. cree que se encuentra.

Verifique estar en el sitio que quiere ir , lea la URL que muestra arriba su navegador

Solo dé información (clave, nombre, etc.) si está en un sitio seguro. El candado, le confirma que Ud. se encuentra en el sitio que debe estar.

Utilice claves complejas para sus datos más importantes. Evite claves de palabras de diccionario. Puede utilizar un administrador de claves como KeePassX para guardar sus claves en forma segura.

9.2. Complementos que aumentan la seguridad de la navegación

9.2.1. No Script

Protección extra para su Firefox: NoScript sólo permite JavaScript, Java y otros plugins en los sitios web de confianza que Ud. elija (como la web de su banco). Este planteamiento preventivo basado en una lista blanca evita que se puedan explotar vulnerabilidades (conocidas o incluso desconocidas) sin pérdida de funcionalidad... Los expertos lo confirmarán: Firefox es realmente más seguro con NoScript

9.2.2. Verify Redirect

Este complemento lo ayuda a estar seguro que al sitio que va a visitar es exactamente el que espera llegar. Muchas veces se accede a una dirección genérica, pero luego es re-dirigido a una específica. También le ayuda con URL cortas. Siempre tendrá el poder de negar la que su navegador entre a sitios desconocidos.

9.2.3. CS Lite

Esta extensión le permitirá controlar las cookies. Se manejan desde la barra de estado o por el menú. Permite bloquear las cookies de un sitio en forma permanente o temporal. También baja listas de sitios que son considerados inseguros, para tener la el navegador asegurado ya antes de entrar.

9.2.4. Adblock Plus

Extensión para Firefox, se puede descargar desde la siguiente dirección: https://addons.mozilla.org/es-ES/firefox/addon/1865/ Permite controlar los banners, anuncios, etc.

9.2.5. Domain Details

Extensión para Firefox, permite desplegar información sobre el tipo de servidor, dirección IP, ubicación, y enlace a información de Whois Reports (nos permite saber quien a registrado el dominio y otros datos).

9.2.6. Expand Short URL

Complemento para Firefox el cuál, una vez instalado, permite hacer click derecho sobre un enlace y conocer la URL correcta que está detrás de la URL acortada. También es posible copiar la URL de destino para pegarla en una nueva solapa, antes de dar enter para navegar por ella.

Capítulo 10

Asegurar el Correo Electrónico

El correo electrónico es hoy día la herramienta más utilizada de Internet. Se puede decir que el correo electrónico se utiliza con más que el web, ya que todos los usuarios que acceden al web usan correo, pero también muchos que no usan web tienen cuenta de correo. Las bases del correo electrónico fueron formuladas en los inicios de la década del '70. Y luego de ello, fueron muy pocas las modificaciones que se le han introducido. En esa época el principal desafío que tenía que afrontar el correo electrónico era llegar a destino. Un correo electrónico tenía que pasar por diferentes computadores y a su vez por distintas conexiones (modem, micro-ondas, radio, cables, etc.). En aquella época, el correo electrónico podía no llegar a destino, entonces se establecieron todos los sistemas de verificación de entrega y notificación de problemas que usamos hoy día. Se definieron también los distintos protocolos de transferencia, registro y retención (guardar el correo hasta que pueda seguir su camino al destino). Desde sus inicios a la fecha, tal vez el mayor desafío que ha tenido que afrontar el correo electrónico ha sido el SPAM. Que ha generado diferentes políticas de seguridad, verificación y control que antes no se usaban, y que muchas de ellas son propuestas que están implementadas por algunos y no por otros. Desde el punto de vista de seguridad, se puede afirmar que el correo que utilizamos hoy en día maneja los principios que tenían sus precursores, o sea una baja seguridad. De esta forma, hacerse pasar por otra persona, leer el correo ajeno (en forma personal o automatizada), interrumpir el paso de un correo, modificar un correo ajeno y otros "ataques" a la seguridad, son muy fáciles de llevar adelante. La baja seguridad del correo electrónico no ha sido un obstáculo para que hoy sea el medio de comunicación preferido en Internet, como dijéramos al comenzar este capítulo.

10.1. Normas básicas para mantener seguro su correo

Nunca cambie su clave a partir de un correo electrónico que le da instrucciones al respecto. Si bien puede considerarse "normal" que su Banco

le pida confirmar sus datos, han sido tantos los robos de datos (phishing) utilizando esta metodología, que ninguna institución seria utilizará este camino para obtener o confirmar sus datos.

Nunca de click en los enlaces de correo electrónico. Muchos servicios utilizan esto para confirmar sus órdenes o instrucciones, en ese caso podría dar click, pero lo ideal es pintar y pegar en el navegador el enlace que le envían.

Configure su lector de correo para que no baje imágenes remotas , las imágenes remotas que descarga su navegador, pueden ser usadas para confirmar que su dirección de correo existe y es leída por una persona.

Evite entrar a sitios a partir de un correo electrónico. Muchos sitios le ofrecen información interesante por correo electrónico. Cuando Ud. entra está confirmando que su dirección de correo existe y es leída por una persona.

Evite publicar su dirección de correo en sitios web en forma exacta a como se usa. Muchos programas pueden rastrear en Internet la publicación de direcciones de correo y leer la que ha publicado. Si publica la dirección oscurecida (p.ej. joseARROBAceibalPUNTOeduPUNTOuy) o dentro de un gráfico, la mantendrá a salvo.

10.2. Complementos que aumentan la seguridad del correo

El programa lector de correo Mozilla-Thunderbird presenta unos sistemas de seguridad propios que lo hacen recomendable para leer correo con seguridad mejorada:

10.2.1. Manejo y detección de SPAM (incluído)

Thunderbird presenta un sistema de detección y manejo de SPAM que puede ser entrenado para detectar lo que cada persona considera como SPAM. Cada e-mail que se recibe pasa por una serie de filtros anti-SPAM, haciendo que el spam que se recibe no requiere ser leído. También si su proveedor de correo electrónico le informa del SPAM, Thunderbird es capaz de interpretar esta información y mejorar sus filtros de correo.

10.2.2. Privacidad Robusta (incluído)

Thunderbird automáticamente detecta y bloquea las imágenes contenidas en los correos que no están adjuntas al correo que ha recibido. Muchos spammers le envían mensajes con imágenes en lugares centralizados y de esa forma saben que se ha recibido y se ha leído el correo. De esta forma su privacidad queda asegurada pues no está descargando automáticamente ninguna imagen.

10.2.3. Protección contra Phishing (incluído)

Thunderbird lo protege de los intentos de engaño que buscan obtener sus datos personales o información confidencial, mediante maniobras de phishing, con mensajes de alerta. Como una segunda linea de defensa, Thunderbird lo alerta de enlaces dentro del correo electrónico que lo llevan a un sitio web diferente del que Usted esta leyendo en el texto del mensaje.

10.2.4. Display Mail User Agent

Esta extensión muestra el sistema de correo (programa) que ha usado quién ha redactado el correo que se recibe. Si Usted reconoce que el sistema de correo de quién envía no es el que suele utilizar, puede sospechar que alguien desea hacerse pasar por él. Es muy común que los intentos de Phishing haciéndose pasar por su Banco, vengan de un software que no es el que su Banco suele utilizar. Esta extensión no funciona automáticamente y requiere que el receptor identifique el correo sospechoso.

10.2.5. Enigmail

Enigmail es la extensión de Thunderbird que le permite el manejo de certificados digitales para que sus correos puedan ser, automáticamente firmados y/o cifrados digitalmente.

Capítulo 11

Básico de Criptografía por e-mail

11.1. Asegurar Remitente

Para el envío de correo electrónico, tomar la identidad ajena es muy simple. Si se están manejando datos relevantes (confirmación de compras, movimientos bancarios, reuniones, etc.) deberá utilizar algún otro método de validación (p.ej. llamada telefónica). El método 100 % seguro para confirmar la veracidad del remitente es que los correos vengan con firma digital. La firma digital es un archivo adjunto que se genera al enviar el correo y que tiene información que solo puede ser creada mediante el uso de una clave que solo el remitente conoce. Cuando el correo se recibe usted dispone de un software que utiliza un archivo que le envió el remitente (en una oportunidad previa) que verifica dicho adjunto de la firma.

11.2. Asegurar destinatario

Cuando envía un correo, el mismo puede ser leído por cualquiera; a veces con intencionalidad (espía) o sin intencionalidad (entrega equivocada). Si maneja información confidencial, es necesario que asegure que la información que trasmite sea leída en forma exclusiva por el destinatario y no por otra persona. El principal problema al espionaje de correo electrónico es que el mismo puede ser realizado en forma automatizada, con estadísticas de envío, patrones de comunicación, relevancia de datos y otros parámetros de análisis. En estos casos, es necesario cifrar el mensaje, para que solo el destinatario lo lea. Se utiliza para esto el mismo sistema de certificado digital que se utiliza para firmar el correo electrónico.

11.3. Integridad del mensaje

Tal vez, lo más improbable que suceda es que su correo sea modificado antes de que llegue a destino. Dependerá el tipo de datos que maneje y la relevancia que el mismo tenga para quién busca modificarlos. Si desea que su mensaje

llegue incambiado, utilice un sistema de firma y cifrado en forma conjunta. De esa forma no podrá ser cambiado y quién lo reciba podrá verificar el origen e integridad del mismo.

11.4. Algunas buenas prácticas

1. El correo electrónico no es un mensajero.
2. Envíe adjuntos en formatos libres y estándares. Si no necesita que el documentos sea editado, utilice algún formato no editable (PDF)
3. Preste atención al tamaño de los adjuntos. Un adjunto debe ser convertido para ir en el correo electrónico y ocupará más espacio del original (aprox 30 % más). Si su correo es muy grande, demorará en llegar a destino o inclusive puede ser rechazado por tamaño.

Capítulo 12

Netiquette

La netiquette[1] es el conjunto de reglas que regulan el comportamiento de un usuario en una lista de correo, un foro de discusiones o al usar el correo electrónico. Por extensión, se utiliza también para referirse al conjunto de normas de comportamiento general en Internet [32]. La Netiqueta no es más que una adaptación de las reglas de etiqueta del mundo real a las tecnologías y el ambiente virtual. Aunque normalmente los lineamientos de etiqueta han evolucionado hasta llegar a formar incluso parte de las reglas de ciertos sistemas, es bastante común que las reglas de etiqueta se basen en un sistema de "honor"; es decir, que el infractor no recibe siquiera una reprimenda.

12.1. Para estudiantes de educación primaria

Esta lista es un conjunto de reglas y normas de conducta que deben seguir los usuarios de Internet. Éstas son las cosas que debes recordar cuando mandes un mensaje electrónico o cualquier tipo de mensaje en línea:

- Escribir todo en mayúsculas equivale a GRITAR. En lugar de mayúsculas usa los *asteriscos*.
- Escribe correctamente. Utiliza de forma correcta las mayúsculas cuando sea necesario, así como la puntuación y la ortografía.
- Identifica tu mensaje con un tema.
- No facilites la contraseña de tu ordenador ni de cualquier material secreto. Ni tan siquiera debes darla a tus mejores amigos.
- No digas a nadie cuál es tu nombre, la dirección ni el lugar donde vives, el número de teléfono ni tampoco expliques a qué escuela vas.
- No mandes fotografías tuyas (salvo que estés muy seguro de lo que haces) ni de cualquier otra persona que conozcas; tampoco envíes información personal.

[1] etiqueta en la red

- Pide permiso a tus padres u otras personas adultas, para bajar juegos, programas u otro material, antes de registrarte para participar en competiciones y antes de dar tu dirección de correo electrónico a nadie.
- Habla con tus padres, u otras personas adultas, si alguien te envía fotografías que te incomodan o si ves este tipo de fotografías en Internet.
- ¡Recuerda que nadie te puede obligar a hacer nada! Si alguien habla contigo en una sala de chat y te hace una pregunta que tú no quieres contestar, no tienes la obligación de hacerlo.
- Sé educado y respeta otras opiniones.
- Nunca respondas ningún mensaje electrónico desagradable, por ejemplo, mensajes de personas de las salas de chat. En lugar de contestar lo que deberías hacer es abandonar dicha sala.
- No participes en debates violentos, enviando mensajes groseros u ofensivos a otras personas.
- Recuerda que la gente que conoces a través de Internet no es necesariamente la gente que dice ser.
- Si optas por encontrarte con alguien que has conocido a través de Internet, nunca debes hacerlo solo/a con esta persona; es mejor que te acompañe un adulto en el primer encuentro. También es necesario que este encuentro se celebre en un lugar público y no en casa de nadie.
- No te dejes convencer para aceptar ofertas que parecen aparentemente buenas; normalmente implican algún tipo de trampa.
- Usa tu cabeza. Internet puede ser un lugar fantástico que te abre el mundo. ¡Sé inteligente y vivirás una excitante y memorable experiencia!

12.2. Para estudiantes de centros de educación media

En este punto se definen cuales son las pautas básicas para el envío de mensajes electrónicos, grupos de discusión y listas de distribución.

12.2.1. Sobre el envío de mensajes electrónicos

Recuerda las pautas siguientes en cuanto a comunicación en línea:

Contenido y estructura de tu mensaje

- Escribe mensajes breves y concisos y ponles un tema indicativo que refleje el contenido del mensaje.
- Usa correctamente la ortografía, la gramática y las mayúsculas;

- Usa cc (carbon copy) o bcc (blind carbon copy) en tus mensajes electrónicos si quieres guardar una copia. Te mostrará la fecha y la hora en que se han enviado los mensajes. Esto es especialmente útil para los informes de tareas en línea.
- Utiliza un buen programa de protección contra virus informáticos y analiza los archivos antes de abrirlos.
- No reenvíes un mensaje electrónico sin la autorización del remitente original; ni invadas la intimidad de otros.
- Ve con cuidado con la expresión de los estados de humor y el sarcasmo. Sin las ventajas del lenguaje corporal o la inflexión vocal, la palabra escrita se puede malinterpretar muy fácilmente.
- Intenta utilizar emoticones si estás seguro/a que el/la lector/a sabe que estás haciendo broma (pero siempre con moderación porque también se pueden molestar).
- Elimina el contenido de un mensaje en la respuesta y sólo incluye la parte que es pertinente para el/la receptor/a.
- Utiliza moderadamente los acrónimos, ya que no todos los lectores pueden conocer lo que significan. Por ejemplo: BTW = by the way
- No envíes nada que no querrías compartir en público.
- No se considera educado usa mayúsculas salvo que quieras enfatizar alguna cosa. Su uso equivale a GRITAR. Si quieres enfatizar algún punto, utiliza los *asteriscos* o subraya la palabra o frase que quieres resaltar.
- No envíes adjuntos archivos muy grandes sin el permiso del usuario. Algunas personas tienen una conexión a Internet muy lenta y el hecho de enviar un archivo de vídeo muy grande como una broma, por ejemplo, podría no ser tan divertido para ellos si esto hace que su ordenador se bloquee durante un largo rato.
- No mandes a todo el mundo aquellos mensajes de tipo humorístico y divertido. La gente está muy ocupada y es bueno asegurarse de que quieren recibir este tipo de mensajes. Ve con cuidado.
- Nunca facilites a nadie ni tu nombre de usuario ni tu contraseña.
- No facilites tu nombre, dirección, lugar donde vives, tu número de teléfono ni el nombre del centro donde estudias.
- No facilites los números de tu tarjeta de crédito ni cualquier tipo de información relacionada con tu banco, pasaporte u otros documentos importantes.
- No envíes fotografías tuyas (salvo que estés muy seguro de lo que haces) ni de nadie que conozcas ni tampoco ningún otro tipo de información personal.

- No expliques, ni siquiera a tus mejores amigos, la contraseña de acceso a tu ordenador ni tampoco a ningún otro material privado.
- Pide permiso a tus padres, o personas adultas para bajarte juegos, programas u otro material, antes de registrarte para participar en competiciones, y antes de enviar tu dirección de correo electrónico a alguien.
- Habla con tus padres, o personas adultas, si alguien te envía fotografías desagradables u ofensivas, o si encuentras este tipo de fotografías en Internet.
- ¡Recuerda que nadie puede obligarte a hacer nada! Si alguien habla contigo en una sala de chat y te hace una pregunta que no quieres responder, no tienes la obligación de hacerlo. No debes contestar ninguna pregunta, sobre todo si alguien te dice cosas que consideras desagradables y ofensivas. En lugar de esto, lo que deberías hacer es abandonar dicha sala.
- No contestes nunca ningún mensaje electrónico desagradable u ofensivo, por ejemplo, mensajes de gente de los grupos de discusión o listas de distribución. ¡Recuerda que la gente que conoces a través de Internet no es necesariamente quien dice ser en realidad!
- Si decides encontrarte con alguien que has conocido a través de Internet, NUNCA debes encontrarte con él/ella solo/a. Mejor que te acompañe una persona adulta en vuestro primer encuentro, el cual debería celebrarse en un sitio público y no en casa de nadie.
- No te dejes convencer para aceptar ofertas que parecen aparentemente buenas; normalmente implican algún tipo de trampa.
- Usa tu cabeza. Internet puede ser un sitio fantástico que te abre el mundo. ¡Sé inteligente y vivirás una excitante y memorable experiencia!

Sobre el uso de listas y foros

- Lee sin participar en los mensajes de los grupos de discusión en los cuales te hayas inscrito, ya que así podrás ver que tipo de mensajes se envían y se responden. Guarda mensajes relevantes del grupo.
- Cuando quieras enviar correo electrónico, en el campo “asunto” mira de poner algo que sea relevante, es decir, que refleje con exactitud el contenido de tu mensaje electrónico.
- Elimina toda aquella parte del mensaje original que sea innecesaria cuando respondas.
- Ve con cuidado con las expresiones de los estados de humor y sarcasmo. Sin las ventajas del lenguaje corporal o la inflexión vocal, la palabra escrita se puede malinterpretar muy fácilmente. Intenta utilizar emociones si estás seguro/a que el lector sabe que estás haciendo broma (pero siempre con moderación porque también se puede molestar).
- Utiliza moderadamente los acrónimos, ya que no todos los lectores pueden conocer lo que significan. Por ejemplo: BTW = by the way)

- Sé educado y respetuoso con la opinión de los demás.
- Comparte lo que tú sabes. ¡Esto es lo que hace interesante los grupos de discusión!
- Busca la página de ayuda o lee las FAQ (las preguntas más frecuentes) de un grupo si están disponibles.
- Incluye alguna nota en la línea de asunto (por ejemplo, [envío largo] si estás enviando alguna cosa que es particularmente larga.
- Recuerda que los recién llegados pueden cometer errores. Sé paciente.
- El uso de letras mayúsculas en línea equivale a GRITAR. Si quieres enfatizar algún punto, es mejor utilizar *asteriscos* o subrayar la palabra o la frase que quieres resaltar.
- Los mensajes incendiarios o insultantes son mensajes provocadores que se envían a una o diversas personas. Se considera de mala educación enviar este tipo de mensajes.
- No repitas lo que ya se ha dicho anteriormente.
- No mandes a nadie nada que no querrías que te volviesen a enviar más tarde a ti.
- No facilites tu nombre, dirección, lugar donde vives, tu número de teléfono, ni el nombre del centro donde estudias.
- No facilites los números de tu tarjeta de crédito, ni información relacionada con tu banco, pasaporte ni otros documentos importantes.
- No envíes fotografías tuyas (salvo que estés muy seguro de lo que haces) ni de cualquier otra persona que conozcas; tampoco mandes información personal.
- No expliques, ni siquiera a tus mejores amigos, la contraseña de acceso a tu ordenador ni a ningún otro material de tipo privado.
- Pide permiso a tus padres, o personas adultas, para bajar juegos, programas u otro material, antes de registrarte para participar en competiciones, y antes de enviar tu dirección de correo electrónico a alguien.
- Habla con tus padres, o personas adultas, si alguien te manda fotografías desagradables u ofensivas, o si encuentras este tipo de fotografías en Internet. Pide permiso a tus padres, u otras personas adultas, para bajar juegos, programas u otro material, antes de registrarte para participar en competiciones y antes de dar tu dirección de correo electrónico a nadie.
- No contestes nunca ningún mensaje electrónico desagradable u ofensivo, por ejemplo, mensajes de gente de los grupos de discusión o listas de distribución. Recuerda que la gente que conoces a través no dice necesariamente quien dice ser en realidad.

- Si decides encontrarte con alguien que has conocido a través de Internet, NUNCA debes hacerlo con él/ella a solas. Es mejor que te acompañe una persona adulta en vuestro primer encuentro, que se debería celebrar en un lugar público y no en casa de nadie.
- No te dejes convencer para aceptar ofertas que parecen aparentemente buenas; normalmente implican algún tipo de trampa.
- Usa tu cabeza. Internet puede ser un sitio fantástico que te abre el mundo. ¡Sé inteligente y vivirás una excitante y memorable experiencia! [5]

Bibliografía

[1] P. Albitz and C. Liu, *DNS and BIND, Fourth Ed.*, O'Reilly Media, EE.UU., 2001.

[2] B. Belsey, *Sitio sobre cyberbullying.* `http://www.cyberbullying.org/`, Junio, 3 2009.

[3] T. Berners-Lee, *Tejiendo la Red*, Siglo XXI, España, 2000.

[4] bullying.org, *Sitio sobre bullying.* `http://www.bullying.org/`, Junio, 3 2009.

[5] R. Conecta, *Uso de listas y foros.* `http://recursos.fundacionesplai.org/`, Mayo, 13 2010.

[6] F. da Rosa, *Análisis de las formas de difusión de la pornografía infantil a través de internet.* `http://www.fedaro.info/2004/04/02/anlisis-de-las-formas-de-difusin-de-la-pornografa-infantil-a-travs-de-internet/`, Abril, 2 2004.

[7] F. da Rosa, *Los virus y la política del avestruz.* `http://www.fedaro.info/2005/08/01/los-virus-y-la-poltica-del-avestruz/`, Agosto, 1 2005.

[8] F. da Rosa, *Navegación segura y responsable*, in En el camino del plan CEIBAL, G. Cyranek, ed., UNESCO, 2009, pp. 185–194.

[9] F. da Rosa and alt, *Investigación sobre pornografía infantil en internet, realizada para el iin.* `http://www.fedaro.info/2005/07/24/investigacion-sobre-pornografia-infantil-en-internet-realizada-para-el-iin/`, Mayo, 3 2010.

[10] F. da Rosa, M. Baez, and D. Roselli, *Redes intra-aula.* `http://www.fedaro.info/2009/06/29/redes-intra-aula/`, Junio, 29 2009.

[11] P. Galla, *PC Pest Control*, O'Reilly Media, EE.UU., 2005.

[12] C. García Rodicio, *Introducción al uso de internet.* `http://www.cesareox.com/docencia/simm/introduccion_a_internet.html`, Mayo, 19 2010.

[13] S. Garfinkel, G. Spafford, and A. Schwartz, *Practical UNIX and Internet Security, Third Ed.*, O'Reilly Media, EE.UU., 2003.

[14] IANA, *Number resources.* http://www.iana.org/numbers/, Junio, 3 2009.

[15] INTECO, *Redes Sociales, Menores de Edad y Privacidad en la Red*, Instituto Nacional de Tecnologías de la Comunicación, España, 2008.

[16] B. Leiner and alt., *A brief history of the internet.* http://www.isoc.org/internet/history/brief.shtml, Junio, 3 2009.

[17] P. D. Marques Graells, *Los riesgos de internet. consejos para su uso seguro. habilidades necesarias para el ciberespacio.* http://peremarques.pangea.org/habilweb.ht, Diciembre, 7 2009.

[18] C. McGinley, *Letter from dr. mcginley to parents/guardians regarding laptop security.* http://www.lmsd.org/sections/news/default.php?m=0&t=today&p=lmsd_anno&id=1138, Junio, 3 2009.

[19] Microsoft, *Correo electrónico sospechoso - protección frente a las estafas de suplantación de identidad (phishing).* http://www.microsoft.com/latam/protect/yourself/phishing/prevent.mspx, Mayo, 19 2010.

[20] NYTimes.com, *Parenting: Sexting leads teen to suicide.* http://today.msnbc.msn.com/id/29546030/#29546237, Mayo, 13 2010.

[21] ——, *Verdict in myspace suicide case - nytimes.com.* http://www.nytimes.com/2008/11/27/us/27myspace.html, Mayo, 12 2010.

[22] F. Picouto Ramos and alt, *Hacking y Seguridad en Internet*, Alfaomega+Ra-Ma, Mexico, 2008.

[23] C. R. and L. D., *Medios informáticos en educación a principios del siglo XXI*, Prometeo Libros, Buenos Aires, 2007.

[24] RTVE, *Clan portal para niños.* http://www.rtve.es/su/registro/pf_login_clan.jsp, Junio, 3 2009.

[25] G. Technology, *Anti-peep robot webcams.* http://gsou.en.ec21.com/Anti_peep_Robot_Webcams_New--4140614_4140615.html, Junio, 3 2009.

[26] E. Tittel, *Fighting spyware, viruses and malware*, PC Magazine, (Diciembre 2004).

[27] C. tshirt de Zazzle.es, *Parenting: Sexting leads teen to suicide.* http://www.zazzle.es/el_sexting_consecuencias_camiseta-235038178244714940, Mayo, 13 2010.

[28] P. Uruguay, *Ley 17559.* http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=17559&Anchor=, Junio, 3 2009.

[29] ——, *Ley 17815.* http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=17815&Anchor=, Junio, 3 2009.

[30] ——, *Ley 18331.* http://200.40.229.134/leyes/AccesoTextoLey.asp?Ley=18331&Anchor, Junio, 3 2009.

[31] P. Wallace, *La psicología de Internet*, Paidos, Barcelona, 2001.

[32] T. Weinberg, *The New Community Rules, Marketing on the Social Web*, O'Reilly Media, EE.UU., 2009.

[33] Wikipedia, *Internet*. `http://es.wikipedia.org/wiki/Internet`, Julio, 24 2005.

[34] ——, *Malware*. `http://es.wikipedia.org/wiki/Malware`, Junio, 2 2010.

Apéndice A

Redes Intra-aula

Una propuesta de apropiación tecnológica en el marco del Plan CEIBAL Presentado en el 4to Encuentro Internacional BTM 2009
Punta del Este, 26 y 27 de Junio Autores:
Prof. Fernando da Rosa,
Profa. Mónica Báez,
Ing. Diego Roselli

A.1. La Propuesta

En la propuesta de redes intra-aula por un lado se busca aportar una solución a problemas de infraestructura informática, pero lo más importante de la propuesta es la apuesta a la apropiación tecnológica por parte del docente, construyendo además un nuevo planteo de relacionamiento en el aula entre el docente, la tecnología y los estudiantes, aportando al desarrollo de nuevos usos con sentido de la misma. Si bien no existen estudios desde el punto de vista cuantitativo, hemos detectado en algunas escuelas problemas de saturación de la red interna lo cual impide aprovechar al máximo el potencial de uso de los equipos del Plan. Por otra parte en los lugares donde la red funciona adecuadamente también sucede que la dependencia de los servicios brindados desde Internet y la demanda de un hardware de mayores prestaciones que el disponible en las XO (los equipos distribuidos actualmente por el Plan CEIBAL), hace que su uso se vea limitado por la imposibilidad de reproducir adecuadamente algunos contenidos. Consideramos que se puede generar una nueva opción de intervención docente dentro del aula, basados en lo siguiente:

1. Recientemente dentro del Plan CEIBAL se ha abierto una instancia para que los docentes adquirieran notebooks de última generación con un procesador y memoria de almacenamiento muy superiores a las XO. Asimismo, aun persisten en muchos centros educativos equipos informáticos del Proyecto ITEEA[1], con lo cual el Plan CEIBAL, mediante "Redes intra-aula", será capaz de establecer un diálogo con al menos uno de los anteriores formatos ensayados por el Sistema educativo.

[1] 2003-2004, modalidad "Un PC en el aula"

2. Por su parte, los mencionados notebooks han sido adquiridos, en tan solo algunos meses, por aproximadamente once mil de los cuarenta mil docentes del Sistema y todo indica que abarcará a casi la totalidad de los docentes, dados los ventajosos planes de compra, subsidios y financiamiento de los equipos.

3. Los equipos antes mencionados tienen una capacidad de procesamiento de datos y memoria muy superior a los equipos distribuidos gratuitamente por el Plan entre los alumnos y docentes (las XO del Plan CEIBAL) y su incorporación al aula aumentaría las posibilidades de trabajo y habilitaría al desarrollo de nuevas estrategias didáctico-pedagógicas por parte de los docentes y nuevas modalidades de aprendizaje por parte de los estudiantes.

4. La idea es incorporar en el aula el poder de procesamiento y memoria de dichos equipos, cuando los docentes así lo deseen, creando una red interna intra-aula donde el equipo principal sea justamente el equipo del docente, con los contenidos que el docente desee ingresar a la red y/o aquellos que éste le permita a los estudiantes incorporar.

De acuerdo a las pruebas que ya hemos realizado, este sistema se puede estructurar de dos maneras:

1. Utilizando la red inalámbrica de la escuela, realizando una aplicación que facilite al docente indicar a sus estudiantes cómo conectarse a su máquina.

2. Utilizando, en aquellas escuelas donde la red se sature frecuentemente, un WAP[2] que se le debería brindar al propio docente de tal manera que su red intra-aula sea independiente de la red institucional.

En ambos casos la máquina del docente contará con un servidor Apache, en el cual se instalará software que pueda ser utilizado por los alumnos. Ya hemos realizado pruebas con una DokuWiki. El ancho de banda disponible en una red de estas características posibilita además compartir video sin problemas entre el equipo del docente y las XO de los alumnos. En el primer caso, si bien la red intra-aula utiliza la red inalámbrica del centro educativo, los estudiantes se conectan directamente al servidor del docente y acceden a los contenidos por él incluidos en su equipo.

A.2. Implicancias desde el punto de vista pedagógico

Partimos del supuesto de que los docentes realizarán un proceso de apropiación tecnológica, lo cual supone redefinir su rol y resignificar sus prácticas en función del cambio de modelo al que les invita esta experiencia enmarcada en el Plan CEIBAL. El adquirir la capacidad de construir su propia red intra-aula motivará a los docentes a incorporar a sus prácticas esta nueva tecnología, permitiéndoles particularmente potenciar aquellas tareas colaborativas y ampliar las posibilidades que ofrecen las modalidades de orientación y tutoría.

La idea busca hacer partícipes activos a los agentes involucrados en este proyecto, ya que no se trata solamente de fomentar el uso de esta tecnología,

[2] Wireless Access Point

sino de apropiarse de ella e integrarla al proyecto educativo, en el marco de una propuesta curricular concreta. Apropiarse desde el lugar que concibe que quedar excluido del acceso a las nuevas tecnologías también refiere al saber utilizarlas, a poder darle sentido a ese uso y colocarlas por tanto en la trama de significados que construyen día a día los docentes respecto a sus prácticas en las clases.

Por tanto, es condición sine qua non que exista una base consistente de reflexión acerca de esta nueva forma de "hacer Escuela" en el colectivo docente implicado en el proyecto. Esto se asegurará mediante la promoción de debates al respecto durante las instancias de capacitación, actualización y formación docente. Es de esperarse también que como consecuencia de la la participación en esta experiencia surjan prácticas tanto en los estudiantes como en el docente y una planificación del trabajo de este último diferentes a las habituales, ya que esta propuesta hace necesario modificar la estructura metodológica si se quieren capitalizar efectivamente las posibilidades que nos brinda esta tecnología.

Asimismo, deberán percibirse cambios en la evaluación y en el ejercicio de los roles tanto del docente como de los estudiantes. La mediación de esta nueva tecnología disponible y la adecuada intervención docente deberían operar como un efectivo apoyo a los canales existentes de comunicación intraáulicos, por lo cual luego de cierto tiempo deberíamos poder registrar formas innovadoras de comunicación estudiante-estudiante, estudiante-estudiantes, docente-estudiante, entre-estudiantes.

En síntesis la propuesta se enfoca en una modalidad de trabajo que facilite la apropiación de los recursos que provee el Plan Ceibal y que colabore a revertir la situación inicial de implementación donde al igual que en en otros países de la región "*. . . la relación entre los maestros y las tecnologías informáticas enfocada a través de la cuestión de las competencias tecnológicas está caracterizada por la distancia. Una de las formas en que se manifiesta esa distancia es la del temor a la tecnología; . . .*"[23] Es nuestro interés propender a que esa modalidad de relacionamiento del docente con la tecnología sea suplantada por otra donde las competencias tecnológicas se integren como parte de la identidad profesional docente.[10]

Apéndice B

Legislación

B.1. Ley Nº 17.559

Publicada D.O. 8 oct/002 - Nº 26109 [28]

Ley Nº 17.559 CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO PROTOCOLO FACULTATIVO RELATIVO A LA VENTA DE NIÑOS, LA PROSTITUCIÓN INFANTIL Y LA UTILIZACIÓN DE NIÑOS EN LA PORNOGRAFÍA El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General,

DECRETAN:

Artículo Único.- Apruébase el "Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía" aprobado el 25 de mayo de 2000, en la ciudad de Nueva York, en oportunidad de celebrarse el 54º período de sesiones de la Asamblea General de las Naciones Unidas.

Sala de Sesiones de la Cámara de Senadores, en Montevideo, a 17 de setiembre de 2002. LUIS HIERRO LÓPEZ, Presidente. Hugo Rodríguez Filippini, Secretario.

MINISTERIO DE RELACIONES EXTERIORES MINISTERIO DEL INTERIOR MINISTERIO DE EDUCACIÓN Y CULTURA

Montevideo, 27 de setiembre de 2002. Cúmplase, acúsese recibo, comuníquese, publíquese e insértese en el Registro Nacional de Leyes y Decretos. BATLLE. DIDIER OPERTTI. ANTONIO MERCADER

B.2. Ley Nº 17.815

Ley Nº 17.815 VIOLENCIA SEXUAL COMERCIAL O NO COMERCIAL COMETIDA CONTRA NIÑOS, ADOLESCENTES O INCAPACES[29] El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General, DECRETAN:

Artículo 1º. (Fabricación o producción de material pornográfico con utilización de personas menores de edad o incapaces).- El que de cualquier forma fabricare o produjere material pornográfico utilizando a personas menores de

edad o personas mayores de edad incapaces, o utilizare su imagen, será castigado con pena de veinticuatro meses de prisión a seis años de penitenciaría.

Artículo 2º. (Comercio y difusión de material pornográfico en que aparezca la imagen u otra forma de representación de personas menores de edad o personas incapaces).- El que comerciare, difundiere, exhibiere, almacenare con fines de distribución, importare, exportare, distribuyere u ofertare material pornográfico en el que aparezca la imagen o cualquier otra forma de representación de una persona menor de edad o persona incapaz, será castigado con pena de doce meses de prisión a cuatro años de penitenciaría.

Artículo 3º. (Facilitamiento de la comercialización y difusión de material pornográfico con la imagen u otra representación de una o más personas menores de edad o incapaces).- El que de cualquier modo facilitare, en beneficio propio o ajeno, la comercialización, difusión, exhibición, importación, exportación, distribución, oferta, almacenamiento o adquisición de material pornográfico que contenga la imagen o cualquier otra forma de representación de una o más personas menores de edad o incapaces será castigado con pena de seis meses de prisión a dos años de penitenciaría. A los efectos del presente artículo y de los anteriores, se entiende que es producto o material pornográfico todo aquel que por cualquier medio contenga la imagen u otra forma de representación de personas menores de edad o incapaces dedicadas a actividades sexuales explícitas, reales o simuladas, o la imagen o representación de sus partes genitales, con fines primordialmente sexuales. (Ley Nº 17.559, de 27 de setiembre de 2002, Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía).

Artículo 4º. (Retribución o promesa de retribución a personas menores de edad o incapaces para que ejecuten actos sexuales o eróticos de cualquier tipo).- El que pagare o prometiere pagar o dar a cambio una ventaja económica o de otra naturaleza a persona menor de edad o incapaz de cualquier sexo, para que ejecute actos sexuales o eróticos de cualquier tipo, será castigado con pena de dos a doce años de penitenciaría.

Artículo 5º. (Contribución a la explotación sexual de personas menores de edad o incapaces).- El que de cualquier modo contribuyere a la prostitución, explotación o servidumbre sexual de personas menores de edad o incapaces, será castigado con pena de dos a doce años de penitenciaría. La pena será elevada de un tercio a la mitad si se produjere con abuso de las relaciones domésticas o de la autoridad o jerarquía, pública o privada, o la condición de funcionario policial del agente.

Artículo 6º. (Tráfico de personas menores de edad o incapaces).- El que de cualquier modo favorezca o facilite la entrada o salida del país de personas menores de edad o incapaces, para ser prostituidas o explotadas sexualmente, será castigado con pena de dos a doce años de penitenciaría.

Sala de Sesiones de la Cámara de Senadores, en Montevideo, a 18 de agosto de 2004. ALEJANDRO ATCHUGARRY, Presidente. Mario Farachio, Secretario.

MINISTERIO DEL INTERIOR MINISTERIO DE RELACIONES EXTERIORES MINISTERIO DE ECONOMÍA Y FINANZAS MINISTERIO DE EDUCACIÓN Y CULTURA Montevideo, 6 de setiembre de 2004.

Cúmplase, acúsese recibo, comuníquese, publíquese e insértese en el Registro Nacional de Leyes y Decretos. BATLLE. DANIEL BORRELLI. DIDIER OPERT-

TI. ISAAC ALFIE. LEONARDO GUZMÁN.

B.3. Ley Nº 18.331

Ley Nº 18.331 PROTECCIÓN DE DATOS PERSONALES Y ACCIÓN DE "HABEAS DATA" [30]

NORMAS El Senado y la Cámara de Representantes de la República Oriental del Uruguay, reunidos en Asamblea General, DECRETAN:

CAPÍTULO I DISPOSICIONES GENERALES

Artículo 1º. Derecho humano.- El derecho a la protección de datos personales es inherente a la persona humana, por lo que está comprendido en el artículo 72 de la Constitución de la República.

Artículo 2º. Ámbito subjetivo.- El derecho a la protección de los datos personales se aplicará por extensión a las personas jurídicas, en cuanto corresponda.

Artículo 3º. Ámbito objetivo.- El régimen de la presente ley será de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado. No será de aplicación a las siguientes bases de datos: A) A las mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

B) Las que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito.

C) A las bases de datos creadas y reguladas por leyes especiales.

Artículo 4º. Definiciones.- A los efectos de la presente ley se entiende por: A) Base de datos: indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

B) Comunicación de datos: toda revelación de datos realizada a una persona distinta del titular de los datos.

C) Consentimiento del titular: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la cual el titular consienta el tratamiento de datos personales que le concierne.

D) Dato personal: información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables.

E) Dato sensible: datos personales que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual.

F) Destinatario: persona física o jurídica, pública o privada, que recibiere comunicación de datos, se trate o no de un tercero.

G) Disociación de datos: todo tratamiento de datos personales de manera que la información obtenida no pueda vincularse a persona determinada o determinable.

H) Encargado del tratamiento: persona física o jurídica, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable de la base de datos o del tratamiento.

I) Fuentes accesibles al público: aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin

más exigencia que, en su caso, el abono de una contraprestación.

J) Tercero: la persona física o jurídica, pública o privada, distinta del titular del dato, del responsable de la base de datos o tratamiento, del encargado y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable o del encargado del tratamiento.

K) Responsable de la base de datos o del tratamiento: persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento.

L) Titular de los datos: persona cuyos datos sean objeto de un tratamiento incluido dentro del ámbito de acción de la presente ley.

M) Tratamiento de datos: operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permitan el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

N) Usuario de datos: toda persona, pública o privada, que realice a su arbitrio el tratamiento de datos, ya sea en una base de datos propia o a través de conexión con los mismos.

CAPÍTULO II PRINCIPIOS GENERALES

Artículo 5º. Valor y fuerza.- La actuación de los responsables de las bases de datos, tanto públicos como privados, y, en general, de todos quienes actúen en relación a datos personales de terceros, deberá ajustarse a los siguientes principios generales: A) Legalidad.

B) Veracidad.

C) Finalidad.

D) Previo consentimiento informado.

E) Seguridad de los datos.

F) Reserva.

G) Responsabilidad.

Dichos principios generales servirán también de criterio interpretativo para resolver las cuestiones que puedan suscitarse en la aplicación de las disposiciones pertinentes.

Artículo 6º. Principio de legalidad.- La formación de bases de datos será lícita cuando se encuentren debidamente inscriptas, observando en su operación los principios que establecen la presente ley y las reglamentaciones que se dicten en consecuencia. Las bases de datos no pueden tener finalidades violatorias de derechos humanos o contrarias a las leyes o a la moral pública.

Artículo 7º. Principio de veracidad.- Los datos personales que se recogieren a los efectos de su tratamiento deberán ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad para la cual se hubieren obtenido. La recolección de datos no podrá hacerse por medios desleales, fraudulentos, abusivos, extorsivos o en forma contraria a las disposiciones a la presente ley. Los datos deberán ser exactos y actualizarse en el caso en que ello fuere necesario. Cuando se constate la inexactitud o falsedad de los datos, el responsable del tratamiento, en cuanto tenga conocimiento de dichas circunstancias, deberá suprimirlos, sustituirlos o completarlos por datos exactos, veraces y actualizados. Asimismo, deberán ser eliminados aquellos datos que hayan caducado de acuerdo a lo previsto en la presente ley.

Artículo 8º. Principio de finalidad.- Los datos objeto de tratamiento no podrán ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. Los datos deberán ser eliminados cuando hayan

dejado de ser necesarios o pertinentes a los fines para los cuales hubieren sido recolectados. La reglamentación determinará los casos y procedimientos en los que, por excepción, y atendidos los valores históricos, estadísticos o científicos, y de acuerdo con la legislación específica, se conserven datos personales aun cuando haya perimido tal necesidad o pertinencia. Tampoco podrán comunicarse datos entre bases de datos, sin que medie ley o previo consentimiento informado del titular.

Artículo 9º. Principio del previo consentimiento informado.- El tratamiento de datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso e informado, el que deberá documentarse. El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 12 de la presente ley. No será necesario el previo consentimiento cuando:

A) Los datos provengan de fuentes públicas de información, tales como registros o publicaciones en medios masivos de comunicación.

B) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

C) Se trate de listados cuyos datos se limiten en el caso de personas físicas a nombres y apellidos, documento de identidad, nacionalidad, domicilio y fecha de nacimiento. En el caso de personas jurídicas, razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma.

D) Deriven de una relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.

E) Se realice por personas físicas o jurídicas, privadas o públicas, para su uso exclusivo personal o doméstico.

Artículo 10. Principio de seguridad de los datos.- El responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. Los datos deberán ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular. Queda prohibido registrar datos personales en bases de datos que no reúnan condiciones técnicas de integridad y seguridad.

Artículo 11. Principio de reserva.- Aquellas personas físicas o jurídicas que obtuvieren legítimamente información proveniente de una base de datos que les brinde tratamiento, están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión de la misma a terceros. Las personas que, por su situación laboral u otra forma de relación con el responsable de una base de datos, tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales, están obligadas a guardar estricto secreto profesional sobre los mismos (artículo 302 del Código Penal), cuando hayan sido recogidos de fuentes no accesibles al público. Lo previsto no será de aplicación en los casos de orden de la Justicia competente, de acuerdo con las normas vigentes en esta materia o si mediare consentimiento del titular. Esta obligación subsistirá aun después de finalizada la relación con el responsable de la base de datos.

Artículo 12. Principio de responsabilidad.- El responsable de la base de datos

es responsable de la violación de las disposiciones de la presente ley.

CAPÍTULO III DERECHOS DE LOS TITULARES DE LOS DATOS

Artículo 13. Derecho de información frente a la recolección de datos.- Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa, precisa e inequívoca:

A) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios.

B) La existencia de la base de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable.

C) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles.

D) Las consecuencias de proporcionar los datos y de la negativa a hacerlo o su inexactitud.

E) La posibilidad del titular de ejercer los derechos de acceso, rectificación y supresión de los datos.

Artículo 14. Derecho de acceso.- Todo titular de datos personales que previamente acredite su identificación con el documento de identidad o poder respectivo, tendrá derecho a obtener toda la información que sobre sí mismo se halle en bases de datos públicas o privadas. Este derecho de acceso sólo podrá ser ejercido en forma gratuita a intervalos de seis meses, salvo que se hubiere suscitado nuevamente un interés legítimo de acuerdo con el ordenamiento jurídico. Cuando se trate de datos de personas fallecidas, el ejercicio del derecho al cual refiere este artículo, corresponderá a cualesquiera de sus sucesores universales, cuyo carácter se acreditará por la sentencia de declaratoria de herederos. La información debe ser proporcionada dentro de los cinco días hábiles de haber sido solicitada. Vencido el plazo sin que el pedido sea satisfecho o si fuera denegado por razones no justificadas de acuerdo con esta ley, quedará habilitada la acción de habeas data. La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen. La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado. La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin.

Artículo 15. Derecho de rectificación, actualización, inclusión o supresión.- Toda persona física o jurídica tendrá derecho a solicitar la rectificación, actualización, inclusión o supresión de los datos personales que le corresponda incluidos en una base de datos, al constatarse error o falsedad o exclusión en la información de la que es titular. El responsable de la base de datos o del tratamiento deberá proceder a realizar la rectificación, actualización, inclusión o supresión, mediante las operaciones necesarias a tal fin en un plazo máximo de cinco días hábiles de recibida la solicitud por el titular del dato o, en su caso, informar de las razones por las que estime no corresponde. El incumplimiento de esta obligación por parte del responsable de la base de datos o del tratamiento o el vencimiento del plazo, habilitará al titular del dato a promover la acción de habeas data prevista en esta ley. No procede la eliminación o supresión de datos personales salvo en aquellos casos de:

A) Perjuicios a los derechos e intereses legítimos de terceros.

B) Notorio error o falsedad.

C) Contravención a lo establecido por una obligación legal.

Durante el proceso de verificación, rectificación o inclusión de datos personales, el responsable de la base de datos o tratamiento, ante el requerimiento de terceros por acceder a informes sobre los mismos, deberá dejar constancia que dicha información se encuentra sometida a revisión. En el supuesto de comunicación o transferencia de datos, el responsable de la base de datos o del tratamiento debe notificar la rectificación, inclusión o supresión al destinatario dentro del quinto día hábil de efectuado el tratamiento del dato. La rectificación, actualización, inclusión, eliminación o supresión de datos personales cuando corresponda, se efectuará sin cargo alguno para el titular.

Artículo 16. Derecho a la impugnación de valoraciones personales.- Las personas tienen derecho a no verse sometidas a una decisión con efectos jurídicos que les afecte de manera significativa, que se base en un tratamiento automatizado o no de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, entre otros. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos personales que ofrezca una definición de sus características o personalidad. En este caso, el afectado tendrá derecho a obtener información del responsable de la base de datos tanto sobre los criterios de valoración como sobre el programa utilizado en el tratamiento que sirvió para adoptar la decisión manifestada en el acto. La valoración sobre el comportamiento de las personas, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Artículo 17. Derechos referentes a la comunicación de datos.- Los datos personales objeto de tratamiento sólo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo. El previo consentimiento para la comunicación es revocable. El previo consentimiento no será necesario cuando:

A) Así lo disponga una ley de interés general.

B) En los supuestos del artículo 9º de la presente ley.

C) Se trate de datos personales relativos a la salud y sea necesario por razones de salud e higiene públicas, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados.

D) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos no sean identificables. El destinatario quedará sujeto a las mismas obligaciones legales y reglamentarias del emisor y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate.

CAPÍTULO IV DATOS ESPECIALMENTE PROTEGIDOS

Artículo 18. Datos sensibles.- Ninguna persona puede ser obligada a proporcionar datos sensibles. Éstos sólo podrán ser objeto de tratamiento con el consentimiento expreso y escrito del titular. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley, o cuando el organismo solicitante tenga mandato legal para hacerlo. También podrán ser tratados con finalidades estadísticas o científi-

cas cuando se disocien de sus titulares. Queda prohibida la formación de bases de datos que almacenen información que directa o indirectamente revele datos sensibles. Se exceptúan aquellos que posean los partidos políticos, sindicatos, iglesias, confesiones religiosas, asociaciones, fundaciones y otras entidades sin fines de lucro, cuya finalidad sea política, religiosa, filosófica, sindical, que hagan referencia al origen racial o étnico, a la salud y a la vida sexual, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio que la comunicación de dichos datos precisará siempre el previo consentimiento del titular del dato. Los datos personales relativos a la comisión de infracciones penales, civiles o administrativas sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas, sin perjuicio de las autorizaciones que la ley otorga u otorgare. Nada de lo establecido en esta ley impedirá a las autoridades públicas comunicar o hacer pública la identidad de las personas físicas o jurídicas que estén siendo investigadas por, o hayan cometido, infracciones a la normativa vigente, en los casos en que otras normas lo impongan o en los que lo consideren conveniente.

Artículo 19. Datos relativos a la salud.- Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional, la normativa específica y lo establecido en la presente ley.

Artículo 20. Datos relativos a las telecomunicaciones.- Los operadores que exploten redes públicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar, en el ejercicio de su actividad, la protección de los datos personales conforme a la presente ley. Asimismo, deberán adoptar las medidas técnicas y de gestiones adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios, con el fin de garantizar sus niveles de protección de los datos personales que sean exigidos por la normativa de desarrollo de esta ley en esta materia. En caso de que exista un riesgo particular de violación de la seguridad de la red pública de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y sobre las medidas a adoptar. La regulación contenida en esta ley se entiende sin perjuicio de lo previsto en la normativa específica sobre telecomunicaciones relacionadas con la seguridad pública y la defensa nacional.

Artículo 21. Datos relativos a bases de datos con fines de publicidad.- En la recopilación de domicilios, reparto de documentos, publicidad, venta u otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno. El titular podrá en cualquier momento solicitar el retiro o bloqueo de sus datos de los bancos de datos a los que se refiere el presente artículo.

Artículo 22. Datos relativos a la actividad comercial o crediticia.- Queda expresamente autorizado el tratamiento de datos personales destinados a brindar informes objetivos de carácter comercial, incluyendo aquellos relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial o credi-

ticia que permitan evaluar la concertación de negocios en general, la conducta comercial o la capacidad de pago del titular de los datos, en aquellos casos en que los mismos sean obtenidos de fuentes de acceso público o procedentes de informaciones facilitadas por el acreedor o en las circunstancias previstas en la presente ley. Para el caso de las personas jurídicas, además de las circunstancias previstas en la presente ley, se permite el tratamiento de toda información autorizada por la normativa vigente. Los datos personales relativos a obligaciones de carácter comercial de personas físicas sólo podrán estar registrados por un plazo de cinco años contados desde su incorporación. En caso que al vencimiento de dicho plazo la obligación permanezca incumplida, el acreedor podrá solicitar al responsable de la base de datos, por única vez, su nuevo registro por otros cinco años. Este nuevo registro deberá ser solicitado en el plazo de treinta días anteriores al vencimiento original. Las obligaciones canceladas o extinguidas por cualquier medio, permanecerán registradas, con expresa mención de este hecho, por un plazo máximo de cinco años, no renovable, a contar de la fecha de la cancelación o extinción. Los responsables de las bases de datos se limitarán a realizar el tratamiento objetivo de la información registrada tal cual ésta le fuera suministrada, debiendo abstenerse de efectuar valoraciones subjetivas sobre la misma. Cuando se haga efectiva la cancelación de cualquier obligación incumplida registrada en una base de datos, el acreedor deberá en un plazo máximo de cinco días hábiles de acontecido el hecho, comunicarlo al responsable de la base de datos o tratamiento correspondiente. Una vez recibida la comunicación por el responsable de la base de datos o tratamiento, éste dispondrá de un plazo máximo de tres días hábiles para proceder a la actualización del dato, asentando su nueva situación.

Artículo 23. Datos transferidos internacionalmente.- Se prohíbe la transferencia de datos personales de cualquier tipo con países u organismos internacionales que no proporcionen niveles de protección adecuados de acuerdo a los estándares del Derecho Internacional o Regional en la materia. La prohibición no regirá cuando se trate de:

1) Cooperación judicial internacional, de acuerdo al respectivo instrumento internacional, ya sea Tratado o Convención, atendidas las circunstancias del caso.

2) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado por razones de salud o higiene públicas.

3) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable.

4) Acuerdos en el marco de tratados internacionales en los cuales la República Oriental del Uruguay sea parte.

5) Cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico. También será posible realizar la transferencia internacional de datos en los siguientes supuestos:

A) Que el interesado haya dado su consentimiento inequívocamente a la transferencia prevista.

B) Que la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado.

C) Que la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero.

D) Que la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

E) Que la transferencia sea necesaria para la salvaguardia del interés vital del interesado.

F) Que la transferencia tenga lugar desde un registro que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para su consulta. Sin perjuicio de lo dispuesto en el primer inciso de este artículo, la Unidad Reguladora y de Control de Protección de Datos Personales podrá autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel adecuado de protección, cuando el responsable del tratamiento ofrezca garantías suficientes respecto a la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos. Dichas garantías podrán derivarse de cláusulas contractuales apropiadas.

CAPÍTULO V BASES DE DATOS DE TITULARIDAD PÚBLICA

Artículo 24. Creación, modificación o supresión.- La creación, modificación o supresión de bases de datos pertenecientes a organismos públicos deberán registrarse conforme lo previsto en el capítulo siguiente.

Artículo 25. Base de datos correspondientes a las Fuerzas Armadas, Organismos Policiales o de Inteligencia.- Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en las bases de datos de las fuerzas armadas, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichas bases de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales. El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, organismos policiales o inteligencia, sin previo consentimiento de los titulares, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Las bases de datos, en tales casos, deberán ser específicas y establecidas al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

Artículo 26. Excepciones a los derechos de acceso, rectificación y cancelación.- Los responsables de las bases de datos que contengan los datos a que se refieren los incisos segundo y tercero del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando. Los responsables de las bases de datos de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el inciso anterior cuando el mismo obstaculice las actuaciones administrativas tendientes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el titular del dato esté siendo objeto de actuaciones inspectivas.

El titular del dato al que se deniegue total o parcialmente el ejercicio de los derechos mencionados en los incisos anteriores podrá ponerlo en conocimiento del Órgano de Control, quien deberá asegurarse de la procedencia o improcedencia de la denegación.

Artículo 27. Excepciones al derecho a la información.- Lo dispuesto en la presente ley no será aplicable a la recolección de datos, cuando la información del titular afecte a la defensa nacional, a la seguridad pública o a la persecución de infracciones penales.

CAPÍTULO VI BASES DE DATOS DE TITULARIDAD PRIVADA

Artículo 28. Creación, modificación o supresión.- Las personas físicas o jurídicas privadas que creen, modifiquen o supriman bases de datos de carácter personal, que no sean para un uso exclusivamente individual o doméstico, deberán registrarse conforme lo previsto en el artículo siguiente.

Artículo 29. Inscripción registral.- Toda base de datos pública o privada debe inscribirse en el Registro que al efecto habilite el Órgano de Control, de acuerdo a los criterios reglamentarios que se establezcan. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que deberá contener la inscripción, entre los cuales figurarán necesariamente los siguientes:

A) Identificación de la base de datos y el responsable de la misma.

B) Naturaleza de los datos personales que contiene.

C) Procedimientos de obtención y tratamiento de los datos.

D) Medidas de seguridad y descripción técnica de la base de datos.

E) Protección de datos personales y ejercicio de derechos.

F) Destino de los datos y personas físicas o jurídicas a las que pueden ser transmitidos.

G) Tiempo de conservación de los datos.

H) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.

I) Cantidad de acreedores personas físicas que hayan cumplido los 5 años previstos en el artículo 22 de la presente ley.

J) Cantidad de cancelaciones por incumplimiento de la obligación de pago si correspondiera, de acuerdo a lo previsto en el artículo 22 de la presente ley.

Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro. El incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en la presente ley. Respecto a las bases de datos de carácter comercial ya inscriptos en el Órgano Regulador, se estará a lo previsto en la presente ley respecto del plazo de adecuación.

Artículo 30. Prestación de servicios informatizados de datos personales.- Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación. Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años.

CAPÍTULO VII ÓRGANO DE CONTROL

Artículo 31. Órgano de Control.- Créase como órgano desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Socie-

dad de la Información y del Conocimiento (AGESIC), dotado de la más amplia autonomía técnica, la Unidad Reguladora y de Control de Datos Personales. Estará dirigida por un Consejo integrado por tres miembros: el Director Ejecutivo de AGESIC y dos miembros designados por el Poder Ejecutivo entre personas que por sus antecedentes personales, profesionales y de conocimiento en la materia aseguren independencia de criterio, eficiencia, objetividad e imparcialidad en el desempeño de sus cargos. A excepción del Director Ejecutivo de la AGESIC, los miembros durarán cuatro años en sus cargos, pudiendo ser designados nuevamente. Sólo cesarán por la expiración de su mandato y designación de sus sucesores, o por su remoción dispuesta por el Poder Ejecutivo en los casos de ineptitud, omisión o delito, conforme a las garantías del debido proceso. Durante su mandato no recibirán órdenes ni instrucciones en el plano técnico.

Artículo 32. Consejo Consultivo.- El Consejo Ejecutivo de la Unidad Reguladora y de Control de Datos Personales funcionará asistido por un Consejo Consultivo, que estará integrado por cinco miembros: - Una persona con reconocida trayectoria en la promoción y defensa de los derechos humanos, designado por el Poder Legislativo, el que no podrá ser un Legislador en actividad.

- Un representante del Poder Judicial.
- Un representante del Ministerio Público.
- Un representante del área académica.
- Un representante del sector privado, que se elegirá en la forma establecida reglamentariamente. Sesionará presidido por el Presidente de la Unidad Reguladora y de Control de protección de Datos Personales. Sus integrantes durarán cuatro años en sus cargos y sesionarán a convocatoria del Presidente de la Unidad Reguladora y de Control de Datos Personales o de la mayoría de sus miembros.

Podrá ser consultado por el Consejo Ejecutivo sobre cualquier aspecto de su competencia y deberá ser consultado por éste cuando ejerza potestades de reglamentación.

Artículo 33. Recursos.- La Unidad Reguladora y de Control de Datos Personales formulará su propuesta de presupuesto de acuerdo a lo previsto en el artículo 214 de la Constitución de al República.

Artículo 34. Cometidos.- El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones:

A) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente ley y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza.

B) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley.

C) Realizar un censo de las bases de datos alcanzados por la ley y mantener el registro permanente de los mismos.

D) Controlar la observancia de las normas sobre integridad, veracidad y seguridad de datos por parte de los responsables de las bases de datos, pudiendo a tales efectos realizar las actuaciones de inspección pertinentes.

E) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados.

F) Emitir opinión toda vez que le sea requerida por las autoridades competentes, incluyendo solicitudes relacionadas con el dictado de sanciones administrativas que correspondan por la violación a las disposiciones de esta ley, de los reglamentos o de las resoluciones que regulan el tratamiento de datos personales comprendidos en ésta.

G) Asesorar en forma necesaria al Poder Ejecutivo en la consideración de los proyectos de ley que refieran total o parcialmente a protección de datos personales.

H) Informar a cualquier persona sobre la existencia de bases de datos personales, sus finalidades y la identidad de sus responsables, en forma gratuita.

Artículo 35. Potestades sancionatorias.- El órgano de control podrá aplicar las siguientes medidas sancionatorias a los responsables de las bases de datos o encargados del tratamiento de datos personales en caso que se violen las normas de la presente ley:

1) Apercibimiento.

2) Multa de hasta quinientas mil unidades indexadas.

3) Suspensión de la base de datos respectiva. A tal efecto se faculta a la AGESIC a promover ante los órganos jurisdiccionales competentes, la suspensión de las bases de datos, hasta por un lapso de seis días hábiles, respecto de los cuales se comprobare que infringieren o transgredieren la presente ley. Los hechos constitutivos de la infracción serán documentados de acuerdo a las formalidades legales y la suspensión deberá decretarse dentro de los tres días siguientes a aquel en que la hubiere solicitado la AGESIC, la cual quedará habilitada a disponer por sí la suspensión si el Juez no se pronunciare dentro de dicho término. En este último caso, si el Juez denegare posteriormente la suspensión, ésta deberá levantarse de inmediato por la AGESIC. Los recursos que se interpongan contra la resolución judicial que hiciere lugar a la suspensión, no tendrán efecto suspensivo. Para hacer cumplir dicha resolución, la AGESIC podrá requerir el auxilio de la fuerza pública. La competencia de los Tribunales actuantes se determinará por las normas de la Ley Orgánica de la Judicatura, Nº 15.750, de 24 de junio de 1985, sus modificativas y concordantes.

Artículo 36. Códigos de conducta.- Las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la presente ley. Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control, quien podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia.

CAPÍTULO VIII ACCIÓN DE PROTECCIÓN DE DATOS PERSONALES

Artículo 37. Habeas data.- Toda persona tendrá derecho a entablar una acción judicial efectiva para tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en bases de datos públicos o privados; y -en caso de error, falsedad, prohibición de tratamiento, discriminación o desactualización- a exigir su rectificación, inclusión, supresión o lo que entienda corresponder. Cuando se trate de datos personales cuyo registro esté amparado por una norma legal que consagre el secreto a su respecto, el Juez apreciará el levantamiento del mismo en atención a las circunstancias del caso.

Artículo 38. Procedencia y competencia.- El titular de datos personales

podrá entablar la acción de protección de datos personales o habeas data, contra todo responsable de una base de datos pública o privada, en los siguientes supuestos:

A) Cuando quiera conocer sus datos personales que se encuentran registrados en una base de datos o similar y dicha información le haya sido denegada, o no le hubiese sido proporcionada por el responsable de la base de datos, en las oportunidades y plazos previstos por la ley.

B) Cuando haya solicitado al responsable de la base de datos o tratamiento su rectificación, actualización, eliminación, inclusión o supresión y éste no hubiese procedido a ello o dado razones suficientes por las que no corresponde lo solicitado, en el plazo previsto al efecto en la ley. Serán competentes para conocer en las acciones de protección de datos personales o habeas data:

1) En la capital, los Juzgados Letrados de Primera Instancia en lo Contencioso Administrativo, cuando la acción se dirija contra una persona pública estatal, y los Juzgados Letrados de Primera Instancia en lo Civil en los restantes casos.

2) Los Juzgados Letrados de Primera Instancia del Interior a quienes se haya asignado competencia en dichas materias.

Artículo 39. Legitimación.- La acción de habeas data podrá ser ejercida por el propio afectado titular de los datos o sus representantes, ya sean tutores o curadores y, en caso de personas fallecidas, por sus sucesores universales, en línea directa o colateral hasta el segundo grado, por sí o por medio de apoderado. En el caso de personas jurídicas, la acción deberá ser interpuesta por sus representantes legales o los apoderados designados a tales efectos.

Artículo 40. Procedimiento.- Las acciones que se promuevan por violación a los derechos contemplados en la presente ley se regirán por las normas contenidas en los artículos que siguen al presente. Serán aplicables en lo pertinente los artículos 14 y 15 del Código General del Proceso.

Artículo 41. Trámite de primera instancia.- Salvo que la acción fuera manifiestamente improcedente, en cuyo caso el tribunal la rechazará sin sustanciarla y dispondrá el archivo de las actuaciones, se convocará a las partes a una audiencia pública dentro del plazo de tres días de la fecha de la presentación de la demanda. En dicha audiencia se oirán las explicaciones del demandado, se recibirán las pruebas y se producirán los alegatos. El tribunal, que podrá rechazar las pruebas manifiestamente impertinentes o innecesarias, presidirá la audiencia so pena de nulidad, e interrogará a los testigos y a las partes, sin perjuicio de que aquéllos sean, a su vez, repreguntados por los abogados. Gozará de los más amplios poderes de policía y de dirección de la audiencia. En cualquier momento podrá ordenar diligencias para mejor proveer. La sentencia se dictará en la audiencia o a más tardar, dentro de las veinticuatro horas de su celebración. Sólo en casos excepcionales podrá prorrogarse la audiencia por hasta tres días. Las notificaciones podrán realizarse por intermedio de la autoridad policial. A los efectos del cómputo de los plazos de cumplimiento de lo ordenado por la sentencia, se dejará constancia de la hora en que se efectuó la notificación.

Artículo 42. Medidas provisionales.- Si de la demanda o en cualquier otro momento del proceso resultare, a juicio del tribunal, la necesidad de su inmediata actuación, éste dispondrá, con carácter provisional, las medidas que correspondieren en amparo del derecho o libertad presuntamente violados.

Artículo 43. Contenido de la sentencia.- La sentencia que haga lugar al habeas data deberá contener:

A) La identificación concreta de la autoridad o el particular a quien se dirija y contra cuya acción, hecho u omisión se conceda el habeas data.

B) La determinación precisa de lo que deba o no deba hacerse y el plazo por el cual dicha resolución regirá, si es que corresponde fijarlo.

C) El plazo para el cumplimiento de lo dispuesto, que será fijado por el tribunal conforme las circunstancias de cada caso, y no será mayor de quince días corridos e ininterrumpidos, computados a partir de la notificación.

Artículo 44. Recurso de apelación y segunda instancia.- En el proceso de habeas data sólo serán apelables la sentencia definitiva y la que rechaza la acción por ser manifiestamente improcedente. El recurso de apelación deberá interponerse en escrito fundado, dentro del plazo perentorio de tres días. El tribunal elevará sin más trámite los autos al superior cuando hubiere desestimado la acción por improcedencia manifiesta, y lo sustanciará con un traslado a la contraparte, por tres días perentorios, cuando la sentencia apelada fuese la definitiva. El tribunal de alzada resolverá en acuerdo, dentro de los cuatro días siguientes a la recepción de los autos. La interposición del recurso no suspenderá las medidas de amparo decretadas, las cuales serán cumplidas inmediatamente después de notificada la sentencia, sin necesidad de tener que esperar el transcurso del plazo para su impugnación.

Artículo 45. Sumariedad. Otros aspectos.- En los procesos de habeas data no podrán deducirse cuestiones previas, reconvenciones ni incidentes. El tribunal, a petición de parte o de oficio, subsanará los vicios de procedimiento, asegurando, dentro de la naturaleza sumaria del proceso, la vigencia del principio de contradictorio. Cuando se planteare la inconstitucionalidad por vía de excepción o de oficio (artículos 509 numeral 2 y 510 numeral 2 del Código General del Proceso) se procederá a la suspensión del procedimiento sólo después que el Magistrado actuante haya dispuesto la adopción de las medidas provisorias referidas en la presente ley o, en su caso, dejando constancia circunstanciada de las razones de considerarlas innecesarias.

CAPÍTULO IX DISPOSICIONES TRANSITORIAS

Artículo 46. Adecuación de las bases de datos.- Las bases de datos deberán adecuarse a la presente ley dentro del plazo de un año de su entrada en vigor.

Artículo 47. Traslado del órgano de control referente a datos comerciales.- Se establece el plazo de ciento veinte días corridos para que el actual órgano de control en materia de protección de datos comerciales, a cargo del Ministerio de Economía y Finanzas, realice el traslado de la información y documentación a la AGESIC.

Artículo 48. Derogación.- Se deroga la Ley Nº 17.838, de 24 de setiembre de 2004.

Artículo 49. Reglamentación.- El Poder Ejecutivo deberá reglamentar la presente ley dentro de los ciento ochenta días de su promulgación. Sala de Sesiones de la Asamblea General, en Montevideo, a 6 de agosto de 2008.

RODOLFO NIN NOVOA, Presidente. Hugo Rodríguez Filippini, Secretario. Marti Dalgalarrondo Añón, Secretario.