# Política de privacidad en la Internet: noción y tecnología

**Héctor Raúl González**
raulgonzalezval@gmail.com

**Neuquén, Argentina, agosto 2006**

**Resumen**

Este trabajo intenta encontrar sentido a la noción de intimidad analizando distintas definiciones; estudia algunas tecnologías que ponen en tensión esta noción. Desarrolla dos mecanismos que tienden a proteger la intimidad de las personas: la perspectiva de mayor legislación y la perspectiva enmarcada en el modelo que preconiza la autorregulación de las empresas utilizando la tecnología. Propone una guía que pueden asumir los padres y docentes para minimizar el riesgo de la intimidad de los niños; se aplica esta guía en el estudio de sitios Web en idioma español orientados a niños. Por último hay un breve estudio sobre los principios de privacidad en los sistemas e-learning y el estudio de los requerimientos de privacidad entre los componentes de un modelo estándar.

**Palabras claves**

Intimidad, política de privacidad, P3P, cookies, web bug, spam, ICRA, niños, tecnología, filtros, guía, software, sellos de autenticación, autorregulación, e-learning.

**Índice**

**AVN Online**

"We think it's critical to preserve the First Amendment right to free speech for the adult industry, and the best way to accomplish that is to regulate ourselves and maintain audience integrity, especially on the Internet. ICRA has provided an excellent vehicle and we encourage the entire adult industry to get with the program."

*Erik McFarland, publisher and managing editor, AVNonline.com*

## Introducción

Numerosos artículo, entre otros [Demner, 2001], [Turow, 2001], [FTC, 1998], ponen de manifiesto que los usuarios de Internet saben muy poco acerca de las consecuencias que tiene para su intimidad el vínculo –link- que aparece en letras pequeñas al final de las páginas principales de los sitios Web con el título "Política de privacidad". Presumo también que saben muy poco acerca del destino de los datos que entregan cotidianamente por alguna prestación ofrecidos en la Red. Este "saber poco" se hace más dramático y más urgente cuando vemos la apropiación que hacen nuestros niños de la Internet en la escuela, en el hogar y en los lugares públicos. Esta idea de que sabemos muy poco sobre lo que significan las políticas de privacidad y cómo se relacionan con las tecnologías que usamos para adentrarnos a Internet es la argumentación global que justifica este trabajo.

Partí de la nada cuando comencé a investigar sobre políticas de privacidad. Y esta ignorancia trajo aparejado la necesidad de contestarme qué significaba el concepto "política de privacidad" y de averiguar cómo se relacionaba con la tecnología que cotidianamente usamos en Internet. No tardé mucho en darme cuenta que la problemática que plantea las políticas de privacidad en las tecnologías de la información, en particular en la Internet, eran muy complejas y que debía acotar mis respuestas a unos pocos asuntos que tuvieran como consecuencia un trabajo de especialización con cierto grado de divulgación. De esta simplificación nació el título de este trabajo: "Política de privacidad en Internet: noción y tecnología". *Noción* es, según el Diccionario de la Real Academia, "Conocimiento o idea que se tiene de una cosa", entonces el primer objetivo es estudiar la noción de privacidad en la Internet. *Tecnología* es la disciplina que intenta explicar el variado mundo artificial[1]. En el mundo artificial nos encontramos con objetos tecnológicos que, en particular en la Internet, se utilizan para poner en tensión la noción de privacidad. Otro de los objetivos del trabajo, entonces, es hacer un recorrido de algunas de las tecnologías que se interrelacionan con la noción de privacidad. Algunas tecnologías[2] no las analizo porque

---

[1] Tomás BUCH*: Sistemas tecnológicos: contribución a una Teoría General de la Artificialidad*, Aique, Buenos Aires, 1999.

[2] Por ejemplo el *phishing* viola la privacidad de las personas, pero es conceptualmente distinto a las otras tecnologías que se tratan en este trabajo. El *phishing* es un engaño, como escribe [Rizzi, 2005], es una estafa, no es sistemática y está efectuado por sujetos y no corporaciones de alta concentración económica. Según [Wikipedia, 2006] es "un término utilizado en informática con el cual se denomina 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, mejor 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". Otro ejemplo es el *Spoofing*, "en términos de seguridad informática hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación". En: http://es.wikipedia.org/wiki/Spoofing. Último ejemplo es el *Sniffer*: "Según la definición de computing-dictionary.thefreedictionary.com, es "una herramienta de monitoreo de red que captura paquetes de datos y los decodifica usando conocimiento incorporado de los protocolos comunes. Pues es correcto, el

asumo la noción de privacidad en el contexto de los servicios más populares que ofrece la Internet: WWW, e-mail, chat, e-learning, etc.

El trabajo se distribuye a continuación en los siguientes apartados. Se analiza la noción de intimidad. Se estudian algunas tecnologías que ponen en tensión esta noción. Se dan a conocer algunas de las argumentaciones a favor y en contra de discutir los temas de intimidad en el contexto de la Internet y luego se analizan algunos mecanismos que tienden a protegerla intimidad de las personas. En el apartado "Los niños" se estudia una guía que tiene el propósito de orientar a padres y docentes acerca de lo que se debe espera que incluyan como contenido las declaraciones de política de privacidad que ofrecen los sitios Web -al final se agrega un apéndice B donde se aplica parte de esta guía, en el estudio de las políticas de privacidad en los sitios Web orientados a niños en idioma español-. En el apartado e-learning se trabajan tres cuestiones necesarias al momento de analizar el concepto de privacidad en sistemas e-learning: la conveniencia de colocar las declaraciones de privacidad en el sitio Web del curso; analizar la materialización de los *principios de privacidad* en un sistema e-leaning y los requerimientos de privacidad entre los componentes de un modelo e-learning. Como verá el lector al llegar al final del trabajo, he incluido un apéndice donde se hace una aproximación más acabada sobre la tecnología P3P. Se escribe este apéndice con dos objetivos: uno, de dar a conocer el esfuerzo, creo, más serio de diversas compañías, incluido el gobierno Norteamericano, de dar respuesta a la opción de que es posible la autorregulación utilizando la tecnología; dos, intentar explicar el modo de funcionamiento y las tecnologías involucrada en el proyecto P3P.

Por último, este texto está dirigido a mis compañeros de trabajo -la educación media- que cotidianamente interactúan con las nuevas tecnologías y a los padres que están interesados sobre las consecuencias que pueden esperar de la acción de sus hijos en la Internet.

## Algunas consideraciones sobre la noción de intimidad

Alan Westin, citado por [Ang, 2001], escribe "la privacidad es imposible definir porque el problema de la privacidad es una materia fundamentalmente de valores, intereses y poder". Si bien coincido con Westin intentaré desarrollar la noción de privacidad desde alguna perspectiva para acercarnos a su sentido.

La primera es usar el diccionario. La Real Academia dice que es la "Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia". El [Wordsmyth, 2006] dice entre otras definiciones: "the condition of not having one's personal life exposed to public knowledge". Estos significados nos dan una idea acerca de lo que estamos hablando. Ambos significado nos hablan de cierto estado de las personas que debe ser preservada de la exposición a otros. Es claro que las personas viven en interacción social y que debe haber alguna exposición para vivir en sociedad y establecer vínculos. Lo que no está claro cual es el umbral que no debe cruzarse para preservar la intimidad.

Desde el razonamiento legal algunos autores [Lessing, 1999], [Frauenholfer, 2004] [Castro, 2002], [Abad, 2001] mencionan el artículo publicado por el Harvard Law Review en 1890, escrito por Samuel Warren y Louis Brandeis, donde se reconoce

---

término *sniffer* proviene del inglés (*sniff* = olfatear, husmear). Es un *software* capaz de interceptar los paquetes o datagramas que pasan por un adaptador de red". En: http://www.microsoft.com/spanish/msdn/comunidad/mtj.net/voices/...

la privacidad como un derecho; definen el concepto de privacidad como "right to be let alone". La definición [Frauenholfer, 2004] esta impulsado por el reconocimiento de la facultad que posee la fotografía de capturar los rostros sin el consentimiento de una persona.

[Lessing, 1999], [Frauenholfer, 2004] destacan la participación de Brandeis en el caso Olmstead vs Estados Unidos, en el año 1928 en la Corte Suprema de ese país. El caso esta relacionado con las escuchas telefónicas usado por el gobierno federal para obtener pruebas. Los demandantes invocaron la Cuarta Enmienda de la Constitución de Estados Unidos. La Corte Suprema no estuvo de acuerdo. En opinión del juez que presidió la Corte, la Cuarta Enmienda sólo protegía contra la intromisión física y, puesto que las escuchas no suponían intromisión, la Cuarta Enmienda no protegía contra aquellas. Como consecuencia las pruebas obtenidas mediante escucha eran válidas para condenar a Olmstead. El juez Brandeis expreso un punto de vista diferente. Brandeis sostuvo que la Constitución tal como fue redactada, solo protegía contra la intromisión física. Pero cuando fue redactada, la intromisión física era la única forma posible de violar la privacidad de las personas. En 1928 parte de la vida de las persona transcurría por los cables telefónicos. En tales circunstancias, argumentó Brandeis, las protecciones de la Cuarta Enmienda debía ser interpretada para proteger la privacidad en las líneas telefónica tanto como en el interior del hogar. [Lessing, 1999] razona: "Brandeis intentó, en primer lugar, identificar los valores de la Cuarta Enmienda y, en segundo lugar, tradujo esos valores al contexto del ciberespacio".

[Desantes, 1991] y [Abad, 2001] coinciden en que la noción de intimidad es diferente a la noción de vida privada[3]. La primera está contenida en la segunda. La noción de intimidad siguiendo a [Desantes, 1991] tiene algunas características que le son propias: se refiere al mundo interior y a la parte más interna de la personalidad; lo propio de la intimidad es la reserva y no el secreto; la intimidad es algo comunicable y porque es comunicable se pude escrutar; va unida a la personalidad y es una construcción "propia" de la persona por lo tanto única; es la parte del espíritu del hombre donde es imposible la insinceridad. Para [Desantes, 1991] la intimidad es "aquella zona espiritual del hombre que considera inespecífica, distinta a cualquier otra, independientemente de que lo sea; y, por tanto, exclusivamente suya que tan sólo él puede libremente revelar".

Desde el punto de vista de los mecanismos del mercado según [Ang, 2001] la noción de intimidad o privacidad es un punto negociable, como un atributo, en vez de presentarse como un derecho humano inalienable. Se supone un consumidor dispuesto comerciar algunos aspectos de su intimidad como parte de la transacción de un servicio.

Las dos definiciones que siguen de política de privacidad asumen a los usuarios como consumidores; son descriptivas, narran aspectos relacionados a las formas y establece una única obligación para las empresas: que deben poner en un lugar del sitio Web las declaraciones de sus políticas de privacidad. De esta manera trasladan la responsabilidad a los consumidores, ellos son los que se deben informar acerca de los deberes y obligaciones que tienen las empresas en relación a la recogida y administración de los datos que solicitan.

---

[3] Desantes establece tres soluciones para definir la relación entre el derecho a la información y las esferas de la personalidad. Con respecto a la vida pública, "sin tomar ahora en consideración posibles elementos contingentes de excepción, puede y debe ser objeto de los mensajes informativos". Con relación a las cuestiones de la vida privada "no son, en general difundibles, excepto cuando estas cuestiones tiene repercusión en la vida pública o trasciende a ella". Con relación a la intimidad "La información nunca debe referirse a la intimidad personal".

La primera definición es la que cita [Correia, 2004]: “A privacy policy is defined as a comprehensive description of a Web site’s practices which is located in one place on the site and may be easily accessed [FTC98]. Every organization involved in electronic commerce transactions has a responsibility to adopt and implement a policy for protecting the privacy of individually identifiable information.”

La segunda es de la Federal Trade Commission [FTC, 1998] en un artículo dedicado a los consumidores, con un apartado dedicado a los niños: “a statement on a website describing what information about you is collected by the site, and how it is used. Ideally, the policy is posted prominently and offers you options about the use of your personal information. These options are called opt-in and opt-out. An opt-in choice means the website won't use your information unless you specifically say it's okay. An opt-out choice means the website can use the information unless you specifically direct it not to”.

Otra definición sobre política de privacidad más cerca del usuario y que pone al sujeto como corresponsal de un derecho ante el poder de las empresas es la que propone [Electronic, 2000], está sobreentendido como el derecho de un sujeto a controlar la acumulación, uso y divulgación de su información personal que es retenido por otro. Dos objetivos tiene el concepto de privacidad: transparencia y rectitud. Transparencia significa que cuando una organización reúne información sobre un sujeto, ellos deben hacer conocer qué información que es reunida y cómo será usada. Rectitud significa que la información sólo será usada con el propósito por el cual fue reunida; si una organización desea usar la información con un propósito adicional está obligada a obtener el permiso explicito del individuo involucrado.

**Amenaza a la intimidad: algunas tecnologías**

Cuando un usuario de Internet está en línea sus preocupaciones [Chung, 2002] deberían ser: a que se rastree su navegación secretamente en la Web; que la información personal y direcciones de e-mail sean capturado y usados para el comercio u otros propósitos sin su consentimiento; que la información recogida sea vendida a terceras partes sin consentimiento y, por último, robo de la identificación de las tarjetas de crédito.

El paradigma por donde se manifiesta la intromisión a la privacidad de los sujetos es redundar la tecnología, que en principio se usa para la interacción social o para obtener un servicio, para fisgonear a uno de los interlocutores. ¿Qué sucede con las nuevas tecnología de la información en este contexto? Según [Castro, 2002], las nuevas tecnologías de la información están caracterizadas por la eficacia en la recogida de datos –invisibilidad-, desventaja del usuario del poder que tiene en relación con el proveedor de servicios y escasa molestia al usuario en la recogida de datos. Como consecuencia las nuevas tecnologías han producido dos nuevas mercancías: los perfiles individuales y los colectivos de los usuarios. Según [Chung, 2002] la frecuencia, la facilidad y el relativo bajo costo de la recogida de información distingue el ambiente online de Internet de otros medios tradicionales de información y reunión de información. Algunas de las herramientas disponibles en la Web que pueden violentar la intimidad de los usuarios son fundamentalmente los cookies, los web bug y el spam.

En relación a los cookies, en principio decimos que el protocolo HTTP[4] usado por WWW se denomina protocolo sin estado [Cookies, 1999] [Electronic, 2000], esto significa que un servidor de HTTP carece de medios para relacionar información concerniente a una petición con otra petición anterior o posterior, es decir que jamás relaciona la solicitud a una página a un requerimiento subsiguiente. Los datos de la respuesta se basan exclusivamente en la información que el cliente envía en la petición. El protocolo HTTP no conoce a la persona a quien está enviando una página ni cuántas páginas le haya podido enviar, incluso aunque nos hayamos conectado hace escasamente algunos segundos, ya que cada petición de página se procesa independientemente. Para retener información que puede ser útil cuando el usuario retorna al sitio que visitó previamente nacieron las cookies en los laboratorios de Netscape. Los ingenieros de Netscape [Electronic, 2000] no tuvieron el propósito de invadir la intimidad. Pero desde 1996 fue usado para un único propósito: permitir al servidor Web recordar algunos datos concernientes al usuario, como sus preferencias para la visualización de las páginas de ese servidor, nombre y contraseña, productos que más le interesan, etc.

Una cookie [Cookies, 1999] no es más que un fichero de texto que algunos servidores piden a nuestro navegador que escriba en nuestro disco duro, con información acerca de lo que hemos estado haciendo por sus páginas. Entre las mayores ventajas de las cookies se cuenta el hecho de ser almacenadas en el disco duro del usuario, liberando así al servidor de una importante sobrecarga. Es el propio cliente –el browser[5]- el que almacena la información y quien se la devolverá posteriormente al

[4] HTTP: (Protocolo de Transporte de Hipertexto) Protocolo empleado para acceder a un documento de la World Wide Web. Un usuario podría encontrar el término HTTP en un Localizador Uniforme de Recursos (URL). Comer, D.E., 1998, "El libro de Internet", 2da. Edición, Prentice Hall, México, p. 298.

[5] Browser: (Navegador). Programa de computadora que permite a los usuarios visualizar documentos hipermedia en la World Wide Web. Algunos navegadores populares son los producidos por Microsoft –Internet Explorer-, Mozilla Foundation –Mozilla Firefox. Ibidem p. 292.

servidor cuando éste la solicite. Además, las cookies poseen una fecha de caducidad, que puede oscilar desde el tiempo que dure la sesión hasta una fecha futura especificada, a partir de la cual dejan de ser operativas.

Los cookies [Mayer, 2000] están basados en un proceso de dos fases. En la primera el cookies es almacenado en la computadora del usuario sin su consentimiento. Por ejemplo, supongamos un usuario del robot de búsqueda My Yahoo! que elige una categoría de interés a partir de la página Web. El servidor Web entonces crea un cookie específico, que es esencialmente una cadena de textos que contienen las preferencias del usuario, el servidor transmite este cookie a la computadora del usuario; el Web browser del usuario recibe el cookies y lo almacena en un archivo especial llamado lista de cookies. Esto sucede sin la notificación al usuario. Como resultado, la información personal –en este caso las preferencias de categoría del usuario- es formateado por el servidor Web, transmitido, y guardado en la compradora del usuario. Durante la segunda fase, el cookies es transmitido en forma clandestina y automáticamente desde la máquina del usuario al servidor Web.

Otro de los instrumentos para rastrear información de los usuarios son los web bag. Los web bug [Chung, 2002] son piezas invisibles de código que pueden ser usado para varios propósitos, por ejemplo, para rastrear en forma secreta la navegación de la gente o hurtar archivos de computadora. Una forma simple de un web bug es un pequeño gráfico que muta su forma de trabajo y se une con un cookie para enviar información a terceras partes sobre la navegación de un usuario en Internet; un web bug ejecutable puede instalar un archivo dentro del disco duro del usuario para reunir información cuando él esté navegando en Internet.

Un web bug [Smith, 1999], [Bugnosis, 2003] es un gráfico situado en una página Web o en un mensaje de e-mail para revisar o verificar quién es el que lee la página o el mensaje. Los web bug son frecuentemente invisibles porque son gráficos, medido en píxel, de 1 por 1. En muchos casos, los web bug son situados en las páginas Web por terceras partes interesados en reunir datos sobre los visitantes a determinadas páginas. Los web bug están representados por la etiqueta IMG del lenguaje de etiquetas HTML[6]. Por ejemplo, en la Web, la información que envía al servidor que está vinculada a la web bug es: la dirección IP[7] de la computadora que trajo al web bug; el URL[8] de la página donde está situado el gráfico que contiene el web bug; el URL del la imagen del web bug; el tiempo de visualización del web bug; el tipo de visualizador (browser) que trajo al web bug y el juego de valores almacenados previamente en un cookie.

En un mensaje de mail el web bug se usa para: descubrir si un mensaje de e-mail particular ha sido leído por alguna persona y cuando fue leído; provee la dirección IP de la máquina que recibe el mail y, dentro de una organización, puede dar una idea de la frecuencia que el mensaje es leído y reenviado. Por ejemplo se puede ver en detalle la

---

[6] HTML: (Lenguaje de Marcado de Hipertexto) Lenguaje de computadora que se usa para especificar el contenido y el formato de un documento de hipermedia en la World Wide Web (por ejemplo, una página hogar). Cuando los usuarios navegan, pocas veces ven el formato HTML de una página porque los navegadores interpretan el HTML y exhiben los resultados automáticamente. Ibidem p. 298.

[7] IP: (Internet Protocol, Protocolo Internet) Literalmente, es la especificación para el formato de los paquetes de información de computadora que se utiliza cuando éstos viajan a través de Internet. En la práctica, por lo regular se refiere al software IP que una computadora debe correr para comunicarse con Internet. Ibidem p. 300.

[8] URL: Abreviatura de *Localizador Uniforme de Recursos*. Ibidem p. 309.

utilización de "Gif de un píxel" por Yahoo! en su centro de privacidad http://privacy.yahoo.com/privacy/ar/pixels/details.html .

A través del correo electrónico se reciben periódicamente mensajes que no han sido solicitados. Entre los mensajes recibidos se encuentran correos comerciales con publicidad, cadenas solidarias y mensajes de otro tipo como el aviso de virus recientes, noticias ambientales, etc. A este tipo de correo se le denomina spam o junk mail. Con mayor precisión se dice que el primero, el envió de correos estrictamente comerciales no solicitados, se denomina spam; a los demás se denomina junke mail.

Según [Palazzi, 2004] "para ser considerado spam, el mensaje electrónico en principio debe cumplir con estos requisitos (i) no debe contener la identidad del receptor del mensaje; (ii) el mensaje debe haber sido enviado indistintamente a toda una gran clase de usuarios; (iii) el receptor no debe haber consentido previamente el mensaje y (iv) la transmisión y recepción del mensaje ofrece una ventaja desproporcionada al remitente, puesto que el proveedor de acceso a Internet o el usuario cargan con los costos económicos del mismo".

El problema de estos correos, según [Leon, 2001], se pueden analizar desde dos perspectiva. Uno: "al enviar estos mail incurren en costos que no son asumidos por quien envía el e-mail. Los asumen tanto el receptor como quien provee el acceso a Internet". Dos: "se está violando la privacidad de las personas al ingresar dentro del ámbito de su intimidad, a su casilla de correo y llenar este con mensajes de cualquier tipo".

Según [Lipskier, 2004] el spaming ocasiona los siguientes daños:

> "- El gasto de dinero en que incurre el usuario al tener que estar conectado para poder bajar, procesar y eliminar este correo.
> "- La pérdida de tiempo que tal proceder implica, lo que se podría configurar como *el hurto del tiempo*.
> "- La posibilidad de infectar la PC con algún virus, contaminando los archivos.
> "- Por la saturación que puede causar en una cuenta, imposibilitando la recepción de correo esperado y/o importante para el usuario."

**Las argumentaciones**

Existen los argumentos a favor y en contra de considerar los temas de intimidad. Según [Chung, 2002] los argumentos en contra dicen: si bien los cookies pueden usarse para identificar a los usuarios de un sitio Web, ellos no encuentran información personal a menos que el consumidor dé su información voluntariamente. Así, desde esta perspectiva, el uso de cookies no es un tema importante con respecto a los asuntos de intimidad. De hecho, algunas personas están dispuestas a dar a la distancia su información personal en respuesta a descuentos y otros beneficios particulares. El uso de cookies para compradores en línea no es diferente a los catálogos de compra por mail cuando la información personal es entregada voluntariamente.

Los argumentos a favor dicen que los consumidores están realmente interesados en salvaguardar su intimidad. Los temas de intimidad obstaculizan a muchos consumidores a comprar productos en la Web. Una investigación [Chung, 2002] de la

firma NFO Interactive, del año 1999, dice que tres de cuatro consumidores que usan Internet jamás hacen compras en línea. Estos consumidores dicen que pueden, probablemente, comprar en línea si los vendedores aseguran que su intimidad puede ser respetada. Un estudio del 2002 en el sector de viajes en Nueva Zelanda sugiere que la intimidad y la seguridad son los temas que paran las compras de boletos de viajes en línea. Las encuestas muestran que la gente está más tranquila si ven la declaración de intimidad, y están más seguros si la declaración de la intimidad fue aprobada por terceras partes, como por la empresa TRUSTe[9].

**Mecanismos que tienden a proteger la intimidad de las personas**

Algunos de los mecanismos para solucionar los asuntos de intimidad que desarrollaremos en este trabajo tienen que ver con la legislación y la autorregulación con solución tecnológica.

a) Los argumentos orientados a la legislación gubernamental [Ang, 2001] dicen que incrementa la confianza del consumidor, como consecuencia incrementa el comercio. La experiencia informa que algunas reglas hacen incrementar el comercio sin interferir con la labor que hace al libre mercado. La conclusión general, siguiendo a [Ang, 2001] , es que "definir y asignar derechos en forma clara, reglas eficientes para el mercado y contratos que se hagan cumplir por la ley, y buenas leyes para reducir la necesidad del consumidor de protegerse ellos mismos ayudaran al comercio…" Otros que proponen la legislación [Chung, 2002] sugieren que regular los asuntos de intimidad por leyes es bueno si la auto regulación falla al momento de orientar adecuadamente los asuntos de intimidad.

Desde la perspectiva legislativa [Ang, 2001] sostiene que la protección de los datos personales y a la privacidad en la Unión Europea está claramente establecido bajo una convención como un derecho humano fundamental. Y cita el artículo 8 de la Convención Europea sobre los Derechos Humanos del año 1963. Siguiendo a [Ang, 2001] el derecho a la privacidad de EEUU es interpretado por la Corte como implícita. No hay mención de la palabra "privacy" o de la frase "protection of privacy" en la Constitución de los EEUU. La Corte fundamenta el derecho a la privacidad, implícito en la Constitución, en las Enmiendas cuatro, nueve y diez.

El concepto de privacidad o intimidad según [Gregorio, 2003] ha tenido diferentes desarrollos dependiendo de la tradición que la contiene. "En la tradición anglosajona los derechos de privacidad abarcan un área más amplia: como el derecho de libertad; como una prevención y protección contra los totalitarismos y como el "derecho a ser dejado solo… En la tradición continental, principalmente España, Francia y América Latina, los derechos a la intimidad y a la propia imagen están estrechamente relacionados a la evolución de la defensa del honor."

En su trabajo [Castro, 2002] pone de manifiesto el Convenio 108 Europeo como norma base y modelo genérico, de contenido mínimos, para la legislación Española y Latinoamericana. "… en América Latina la adopción de medidas que protejan al ciudadano ante el auge de la tecnología ha sido más lenta que el resto del mundo, precisamente porque el desarrollo tecnológico ha llegado a estas naciones en forma tardía". La región, según esta autora, ha optado, generalmente por establecer legislaciones bajo la denominación de "Leyes sobre Habeas Data", recurriendo el

[9] Ver más abajo.

ciudadano a tal recurso como vía de defensa a la intimidad[10] ante la manipulación indiscriminada de sus datos[11]. Siguiendo a [Castro, 2002], "Precisamente, el *Habeas Data* es un recurso procesal para defender el derecho a la intimidad como un instrumento del individuo de control y disposición de sus datos personales. El *Habeas Data* cosiste en el instrumento de garantía que poseen los ciudadanos para el acceso a todos los bancos de datos que contengan información que afecte su vida privada siendo la finalidad de tal derecho, la protección contra cualquier ataque a la esfera de la intimidad. El *Habeas Data* ampara el derecho del ciudadano a exigir la exhibición o eliminación pública de sus datos, de conformidad con los ajustes normativos regionales, mediante un instrumento procesal que emula *Habeas Corpus* como defensa de un derecho fundamental (ya no la libertad o la vida sino a la intimidad personal)".

Argentina, según [Castro, 2002], [Valesani, 2003], fue pionero en establecer una legislación que protegiese la privacidad de los ciudadanos. En la Constitución Nacional [Constitución, 1994] existen los artículos que amparan la adopción de lo que es hoy en día su normativa en torno al *Habeas Data*, y se trata de los artículos 18 y 19:

> "Artículo 18. (…) El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación (…)"
>
> "Artículo 19**.** Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe".

La protección de los datos personales de los ciudadanos está en al artículo 43 de la Constitución reformada, párrafo tres:

> "Articulo 43. (…)Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística."

La Ley de Habeas Data de la Argentina fue aprobada por la cámara de Diputados [Castro, 2002] el 14 de setiembre de 2000. La Ley [Habeas, 2000] argentina recoge los principios generales de la Directiva 95/96 de la comunidad europea y se centra además en el derecho de los ciudadanos a recibir información. Esta Ley según [Valesani, 2003] "tiene como objetivo preservar la intimidad de las personas, garantizando la exactitud de los datos personales que cualquier registro público o privado pudiese tener con respecto a un ciudadano de Argentina vale decir que busca asegurar la autenticidad de los datos de las personas. Según surge de su articulado, esta

---

[10] "Es importante hacer notar que el Convenio 108 en su traducción oficial utiliza el término "vida privada" como anglicismo derivado de la obra de Warren y Brandeis, a partir del cual se empieza a hablar en doctrina de "privacy", e intenta establecer la protección genérica de lo que domina "vida privada" cuyo contenido es el derecho a la intimidad. No obstante, ante la doctrina imperante, la Directiva 95/96 de la Unión Europea retoma el término que mejor se ajusta a nuestra lengua: el de *intimidad*". [Castro, 2002], pag. 10

[11] El objeto del Convenio 108 del Consejo de Europa [Castro, 2002] en su artículo primero indica que es garantizar en el territorio de cada Estado Parte, el respeto a todas las personas de sus derechos y libertades fundamentales, concretamente del derecho a la vida privada con respecto al tratamiento automatizado de datos personales."

figura tiene como finalidades: acceder al registro de datos; actualizar aquellos datos que pudieran estar atrasados en ese registro; corregir la información inexacta que pudiera surgir del banco de datos; asegurar la confidencialidad de cierta información para que no trascienda a terceros y cancelar datos vinculados con la denominada información sensible[12]"

[Aguirre, 2006] dice que la "…protección de la intimidad en la Argentina está específicamente en el Código Civil en su artículo 1071 bis, agregado por la ley 21.173 en la siguiente forma: "El que arbitrariamente se entrometiere en la vida ajena publicando retratos, difundiendo correspondencia, mortificando a otro en sus costumbres o sentimientos, o perturbando de cualquier modo su intimidad, y el hecho no fuere un delito penal, será obligado a cesar en tales actividades, si antes no hubieren cesado, y a pagar una indemnización que fijará equitativamente el juez, de acuerdo con las circunstancias; además, podrá éste, a pedido del agraviado, ordenar la publicación de la sentencia en un diario o periódico del lugar, si esta medida fuese procedente para una adecuada reparación".

b) Aquellos que sostienen que debe haber menos regulación, arguyen que la regulación interfiere con la labor del mercado libre. En particular Estado Unidos [Castro, 2002] "considera que regular las autopistas de la información deviene en un menoscabo al desarrollo industrial y económico, lo que coincide con su legislación y política economicista".

Desde la perspectiva de la autorregulación -relacionado con la perspectiva de menos o nada de regulación legal- algunas compañías y organizaciones propusieron que la tecnología puede ser usada para solucionar los problemas de protección de la intimidad. Existen organizaciones y empresas que han producido tecnologías que: a) proponen que los sitios web expresen su prácticas de privacidad en un formato estandarizado que pueda ser recuperado e interpretado por un usuario agente[13]; b) certifican a través de un sello, puesto en el sitio Web de contenidos, el cumplimiento de la aplicación correcta de los términos de la política de privacidad; c) habilitan a los sitios de contenidos hacer su auto clasificación para que los padres puedan, a través de un software, elegir qué pueden ver sus hijos; d) ofrecen un software que permite filtrar contenidos corrosivo para los niños y e) luchar contra el spaming estableciendo, por un lado, normas y políticas entre las empresas y, por otra, soluciones tecnológicas.

El sistema que fue establecido bajo la noción de autorregulación [Garfinkel, 2000], es la Platform for Privacy Preferences o P3P. Entre los impulsores[14] de P3P esta la casa Blanca, las principales compañías de tecnologías como Microsoft y America

---

[12] Según [Castro, 2002] el Convenio 108 del Consejo de Europa dedica un capitulo a lo denomina principios, pero que en realidad se refiere a los deberes a los que se obligan las partes (Capítulo II). Dentro de los deberes incluye la prohibición de categorías particulares de datos, conocidos como sensibles, y que son aquellos relacionados a la raza, afinidad política, preferencia sexual, condiciones de salud, religión, condenas penales u opiniones particulares de los individuos en general.

[13] Un programa que actúa en nombre del usuario. El agente puede actuar con muchos propósitos, tal como filtrar contenidos, decidir sobre decisiones verdaderas o sobre la intimidad. De acuerdo a P3P un usuario agente actúa de acuerdo a las preferencias de privacidad del usuario. En: http://www.w3.org/TR/1998/NOTE-P3P10-principles-19980721 Un programa cuyo propósito es mediar la interacción con servicios en nombre de un usuario bajo las preferencias del usuario. Un usuario puede tener más de un agente usuario, el agente no necesita residir en la computadora del usuario, pero el agente debe ser controlado por el usuario y actuar a favor solo del usuario. En: http://www.w3.org/TR/P3P/.

[14] Según [Electronic, 2000] con fondos de muchas organizaciones del sector privado que se oponen a la legislación de la privacidad.

Online y organizaciones como Center for Democracy and Technology. P3P tiene su raíz en la Platform for Internet Content Selection (PICS) del World Wide Web Consortium (W3C). La PICS [Garfinkel, 2000] es un protocolo creado para hacer posible la censura. Fue concebido en el año 1999 durante el primer Congreso que intentó regular la pornografía en Internet, el PICS fue diseñado para hacer posible la prevención de los niños, por parte de los tutores, ante la vista de pornografía en Internet. La gran idea detrás de PICS fue que cada sitio Web en la Internet pueda tener una clasificación de la pornografía y que el visualizador –browser- de la Web pueda consultar esa clasificación antes de exhibir los contenidos de las páginas Web.

De acuerdo a W3C, P3P permite la creación de agentes usuarios –software- que son configurados para reflejar las preferencias de privacidad de los usuarios. Una vez configurado el agente puede comparar sus preferencias con las declaraciones de privacidad legibles por la máquina hecha para varios sitios Web. Si las políticas de privacidad de un sitio Web son igual a las preferencias de privacidad del usuario, el acceso al sitio Web está garantizado. Y si hay un conflicto, una ventana pop-up describe la discrepancia notificando al usuario, o informado que el acceso al sitio está bloqueado, para mayor información sobre P3P ver el apéndice A.

De acuerdo a [IRAM, 2006] se define certificación "… como "atestación por **tercera parte** relativa a productos, procesos, sistemas o personas", entendiéndose por atestación la actividad que se basa en la decisión tomada luego de la revisión y consiste en autorizar y emitir una **declaración** de que se ha demostrado que se cumplen los **requisitos especificados**. Esta **declaración** puede ser un certificado o una marca de conformidad. En todos los casos la declaración garantiza a los usuarios de la evaluación de la conformidad que se cumplen los requisitos especificados (futura ISO/IEC 17000).

"Para que la certificación se realice en forma imparcial debe ser realizada por una **tercera parte**, es decir un organismo independiente de los respectivos intereses del proveedor del objeto de la certificación (primera parte) y del usuario de la certificación (segunda parte)".

De acuerdo al modelo de certificación propuesto por [IRAM, 2006] existen empresas en la Web que realizan certificaciones. Es el caso de TRUSTe[15]. Muchas empresas, llevan el sello de certificación de TRUSTe. Siguiendo a [TRUSTe, 2006] "Los programas de TRUSTe están de acuerdo con muchas pautas gubernamentales e industriales relativas al uso de la información personal, incluyendo la Ley de Protección de la Confidencialidad en Línea del Estado de California [California Online Privacy Protection Act], la Ley Federal CAN-SPAM, los Reglamentos para el Uso Justo de la Información patrocinados por la Comisión Federal de Comercio y los Principios de Confidencialidad Safe Harbor del Departamento de Comercio de los Estados Unidos". El "sello de seguridad" TRUSTe se otorga sólo a los sitios que se adhieren a los estándares de privacidad establecidos sobre la divulgación, elección, acceso y seguridad. Los sitios Web que exhiben el sello de privacidad TRUSTe también acuerdan cumplir con la supervisión constante y a participar en la resolución de disputas. Al hacer clic sobre el icono de "sello de seguridad" los visitantes del sitio podrán revisar una declaración de la política de privacidad. Recientemente la empresa TRUSTe [MD, 2005], bajo el lema "WE DON'T SPAM", creó la certificación que

[15] Otras empresa que certifican sitios son BBBOnLine cuyo URL es http://www.bbbonline.org/ y IQNet cuyo URL es http://www.iqnet-certification.com/ .

asegura a los consumidores que los vendedores no les llenarán el buzón de correo electrónico de basura cuando les faciliten su dirección de e-mail.

Con relación a lo que define [IRAM, 2006] de la necesidad de imparcialidad no está muy claro con TRUSTE puesto que los miembros de la junta de directores[16] está formado por representantes de algunas de las principales corporaciones de los EEUU -Microsoft, Oracle Corporate Affaire, America Online, Inc., DoubleClick, Inc, Time Warner, Inc, etc.- "preocupados" por la seguridad de los niños en línea.

El ICRA –Internet Content Rating Association- según [ICRA, 2005] se define como una organización internacional sin fines de lucro de los líderes de Internet que trabajan para desarrollar una Internet segura. Tienen la esperanza que la autorregulación conduzca a un balance entre la circulación libre de los contenidos con la protección de los niños de material nocivo. ICRA desarrolló un sistema de etiquetado de contenido consultando a expertos internacionales en clasificación de contenido así como a líderes de la industria. El nuevo cuestionario de etiquetado permite a los proveedores de contenido etiquetar objetivamente el contenido de sus sitios.

Lo central de la organización está en su vocabulario descriptivo, denominado "el cuestionario de ICRA". La idea es que los proveedores de contenido chequeen qué contenido del cuestionario está presente o ausente en su sitio Web. Se genera un pequeño archivo que contiene la clasificación del sitio en cuestión. Los usuarios, particularmente los padres, usando un software con capacidad de filtrado, permiten o no el acceso al sitio Web basándose en la información declarada en el archivo de calificación.

ICRA, en su sitio Web, pone a disposición de los proveedores de contenidos un generador de clasificación -label generador- que consiste de cuatro pasos. El primer paso está relacionado a la elección de la clasificación de los contenidos para el sitio Web; el segundo paso a la elección de contenidos para parte del sitio Web que contiene alguna categoría diferente; en el tercer paso se genera el archivo con extensión .rdf con las calificaciones del sitio -el proveedor de contenidos debe poseer una dirección ftp, nombre de usuario y contraseña para que el servidor del ICRA baje el archivo al servidor del proveedor de contenidos; por último, en el cuarto paso, se coloca un "tag" especial que se incluye en la sección <head> dentro de cada página del sitio Web para vincular al archivo con las calificaciones de contenido.

Otra organización que ofrece la tecnología de filtrado es SafeSurf. Al igual que ICRA el creador de páginas Web es el que debe clasificar los contenidos. Si el creador de páginas Web quiere clasificar su propio sitio debe acceder al http://www.safesurf.com/classify/ donde deberá llenar un formulario en línea. Una vez llenado el formulario se crea un pequeño documento HTML con la clasificación del sitio. Un ejemplo sacado de [Safesurf, 2006]:

"<META http-equiv="PICS-Label" content='(PICS-1.1 "http://www.classify.org/safesurf/" l r (SS~~000 1))'>"

La computadora interpreta el código SS~~0001 como información general -los dos primeros ceros-, sin temas adultos -tercer cero- con grado benigno -el valor 1.

Esta clasificación puede aparecer antes o dentro de la sección <HEAD> de un documento HTML.

[16] Ver TRUSTe "Board of Directors" en el URL: http://www.truste.org/about/board_of_directors.php

"<HTML>
<HEAD>
<META http-equiv="PICS-Label" content='(PICS-1.1 "http://www.classify.org/safesurf/" l r
(SS~~000 1))'>
<TITLE> Your Document Title </TITLE>
</HEAD>"

La empresa Digimarc provee un sistema de filtrado de contenido para fotografías, imágenes, etc. -similar al propuesto por el ICRA- que consiste en incrustar en el archivo una "marca de agua" indeleble, que el usuario no percibe pero que resulta ostensible durante el proceso de datos.

Digimarc, a través de suscripción, entrega un único ID al proveedor de contenidos para integrar a sus archivos, al mismo tiempo posibilita a través de un software adecuado, agregar un atributo de "Contenido Adulto". El atributo "Contenido Adulto" marca a los archivos "con una bandera" para indicar que el contenido ha sido considerado inadecuado para niños, como las imágenes de violencia, desnudez, y el empleo de drogas prohibidas. La "marca de agua" integrada proporciona una identidad digital propia, completa y persistente que se quedará con los archivos cuando estas se distribuyen por el Web o por el correo electrónico.

El programa Adobe Photoshop [Photoshop, 2006] permite incrustar el ID de creador único entregado por Digimarc a las imágenes y sumar información como, por ejemplo, el año de copyright o un identificador de contenido de adulto[17].

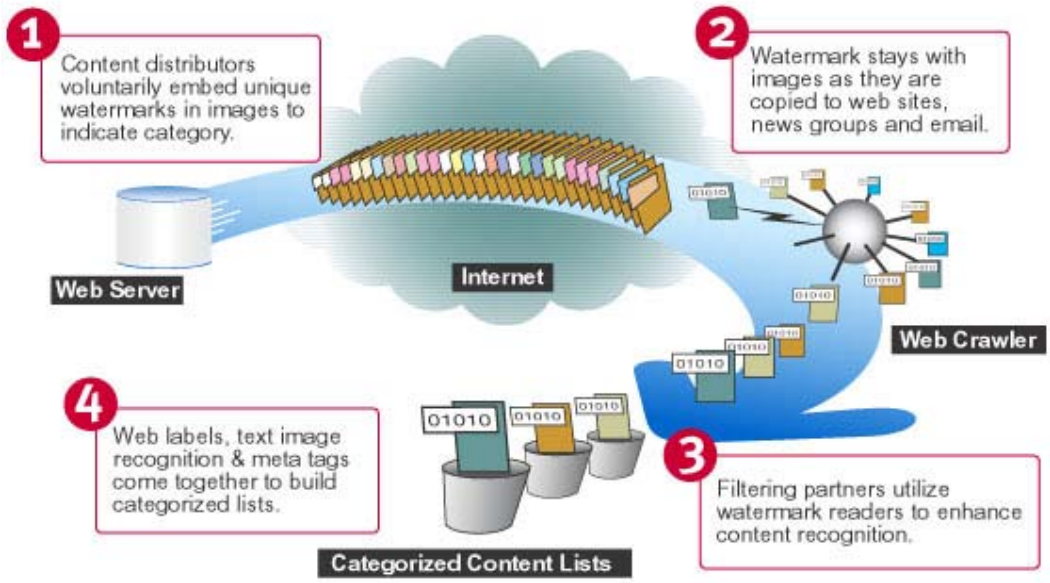



Figura Nº 1: Esquema extraído de http://www.icra.org/pkd/howitworks/

La empresa de software Net Nanny Software International Inc., ofrece las versiones Net Nanny 4 y Net Nanny 5 como herramienta útiles para filtrar los contenidos de la Internet.

Entre los servicios que ofrece Net Nanny se encuentran: controlar el acceso a sitios "inapropiados; prevenir el uso no autorizado de la PC; proteger la privacidad;

[17] El lector puede leer observaciones interesantes al sistema de filtrado en [Villate, 1998] y [Libertus, 1998].

monitorear las actividades de un individuo, un grupo o todos los usuario en el uso de Internet y manejo de amenaza por parte de virus y programas llamados “caballo de Troya”.

Nanny requiere que una persona de la familia se designe como el administrador del software. El administrador tiene todo el control y la responsabilidad del software Net Nanny y de establecer el conjunto de atributo a cada miembro de la familia.

El administrador accede al  Net Nanny Setting para:

-Agregar la cuenta de un nuevo usuario y definir su nivel de permisos;
-Seleccionar los atributos para Net Nanny ;
-Revisar las actividades diarias de los usuarios en la Internet;
-Activar o desactivar Net Nanny;
-Desinstalar el Net Nanny de la computadora.

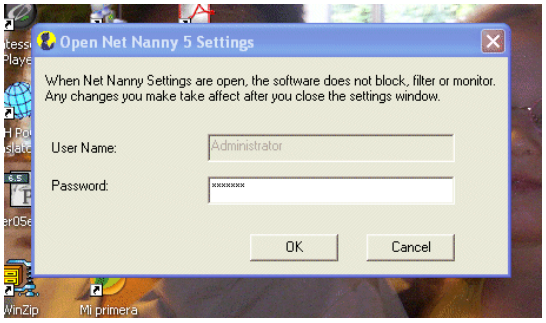



Figura Nº 2: Ingreso del administrador al Net Nanny Setting

En el Net Nanny Setting el administrador tiene 3 grupos de settings:

-El primer grupo consiste en aplicar permisos y restricciones en las cuentas de los usuarios individuales, previamente creados.
-El segundo grupo consiste en aplicar permisos y restricciones globales a todos los usuarios.
-El tercer grupo consiste en aplicar atributos relacionados al mantenimiento del sistema.

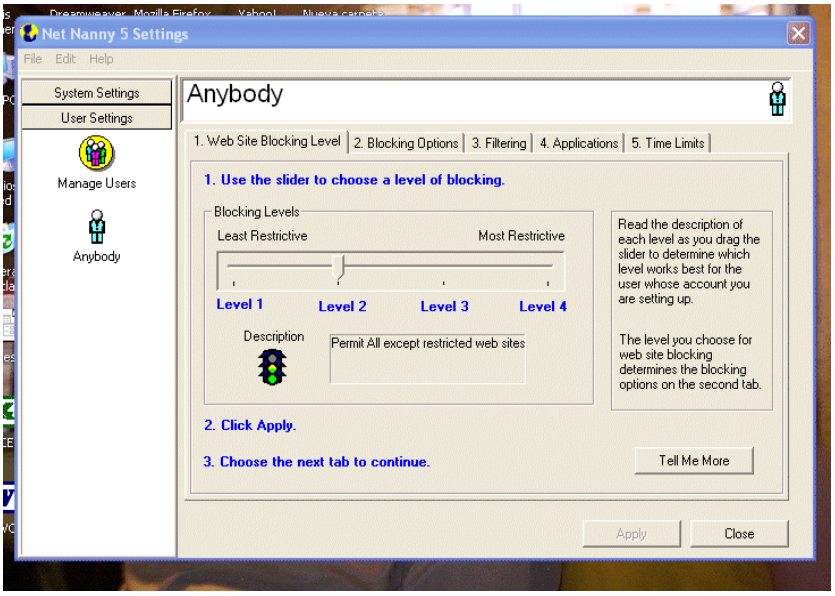



Figura Nº 3: Pantalla del Net Nanny Setting

Usando la opción "Manage Users" el administrador puede agregar usuario, remover usuario o editar usuarios.

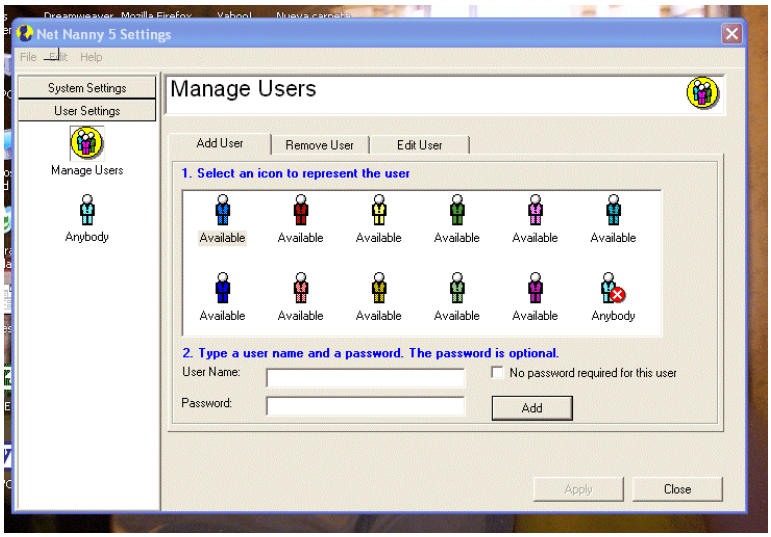



Figura Nº 4: Pantalla del Manage User

Luego de crear la cuenta de un usuario nuevo, se aplican los permisos y las restricciones.

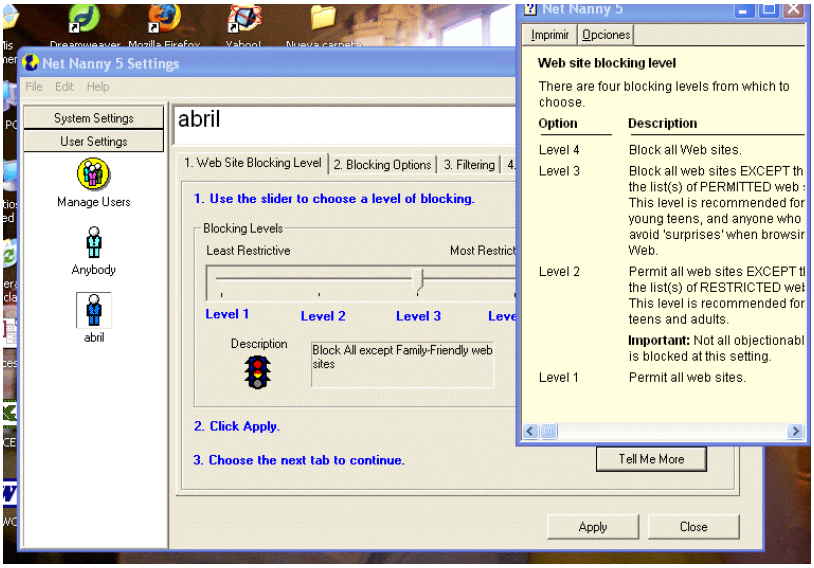



Figura Nº 5: Pantalla para administrar un usuario particular

Eligiendo la opción "System setting" se aplican los atributos relacionados al mantenimiento del sistema.

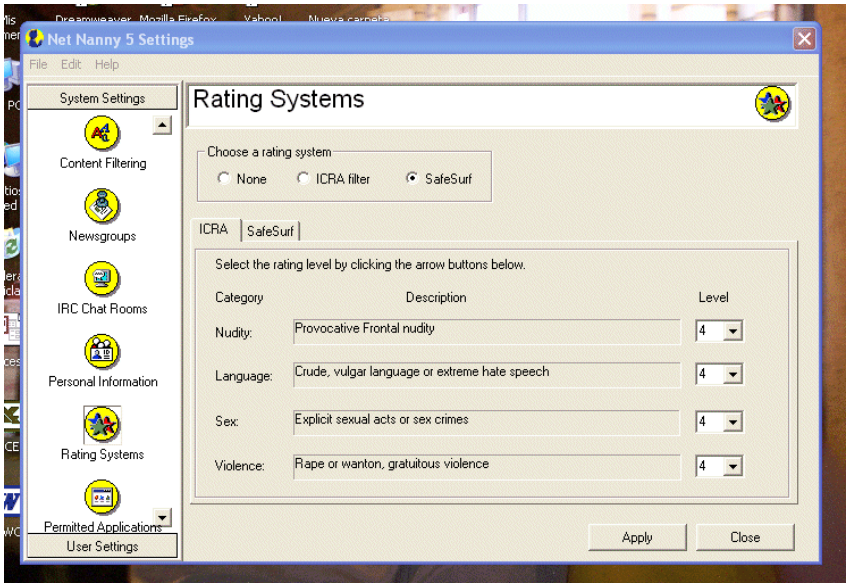



Figura Nº 6: Pantalla para administrar el sistema

Existen en el mercado otros programas que utilizan las técnicas de filtrado y de listas de sitios Web clasificados como autorizados o no autorizados[18]. Por ejemplo Cyber Patrol, Cyber Sitter y Surf Watch. Pueden bajarse versiones de prueba de Cyber Patrol en http://www.cyberpatrol.com, de Cyber Sitter en http://www.cybersitter.com y de Net Nanny en http://www.netnanny.com.

[18] En el sitio Web http://www.jornada.unam.mx/1997/11/18/virtualia.html el lector puede leer un resumen de cada programa.

Con relación al spaming las empresas han establecido algunos criterios de autorregulación proponiendo por un lado consenso para fijar listas y sistemas de tipo "Opt-in" y "Opt-out".

Según [Leon, 2001] "Mediante los sistemas "*Opt-in*" se establece que quien desee recibir algún tipo de mensaje comercial no solicitado se debe inscribir en una lista, listas que pueden tener carácter general o específico, para recibir determinados mensajes. El sistema "*Opt-out*", en cambio, busca que las personas que no desean recibir e-mails comerciales no solicitado deben inscribir sus nombres y direcciones electrónicas en estas listas".

La organización iCAUCE.Ar [iCAUCE.Ar, 2006] objeta el mecanismo Opt-out para frenar el spam porque dicen que:

> "a) Impracticabilidad e irrazonabilidad: Si cada Opt-out le toma sólo 5 segundos y recibe 100 mensajes basura por día -una cifra nada rara para direcciones estables de más de un par de años-, el tiempo total de respuesta diaria es de más de 10 minutos. En realidad, no pierde sólo 10 minutos. Usted interrumpe sus actividades -personales y/o profesionales- muchas veces, con una pérdida de productividad muy significativa.
>
> b) Ética: ¿Recuerda cuando hace varios años los Bancos le enviaban una tarjeta de crédito activada, y Usted debía devolverla si no quería usarla (y pagarla)?
>
> Lo mismo pasa con el opt-out. Si Usted no pidió que le envíen nada... ¿porqué tiene que incurrir en gastos para que dejen de enviarle publicidad, y encima a su costo?"

La misma Organización propone como solución a largo plazo, como mecanismo que colabore en la lucha contra el spam, el Opt-in verificado: "El opt-in verificado -a veces llamado doble o triple Opt In- es un mecanismo que permite en forma simple y confiable verificar el deseo de un usuario responsable de una dirección de e-mail de que esa dirección sea agregada a una lista de distribución de mensajes". Ver la propuesta en la dirección http://wiki.cauce.org.ar/cgi-bin/moin.cgi/OptInVerificado

Desde el lado tecnológico [Fernández, 2003] los sistemas de filtrado deben descubrir y bloquear el mayor numero de correos no deseados minimizando la cantidad de correos denominados *falsos positivos*: son mensajes lícitos pero que el sistema de filtrado los detecta como spam. Los programas de filtrado utilizan una combinación de técnicas para detectar los correos spam:

a) [Fernández, 2003] filtros inteligentes: los heurísticos y los adaptativos o bayesianos;

b) Enriqueciendo las listas negras, que son bases de datos de direcciones IP que por una causa o por otra son consideradas potenciales emisores de spam.

c) Enriqueciendo las listas blancas, que son fuentes confiables de direcciones IP.

Según [RedIris, 2003] la lucha contra el spam se puede dividir en dos grupos:

> "Reactivas: Es decir las que toman medidas ante la entrada del spam. Suelen ser las medidas tomadas por los usuarios que en forma de filtros borran los mensajes que tienen determinados contenidos u orígenes.
>
> Proactivas: Son las medidas que se toman para interceptar todo el tráfico SMTP proveniente de una dirección IP, es decir el tráfico bueno y el spam. El objetivo es fomentar entre los proveedores la erradicación de esta práctica y su canalización por técnicas menos agresivas (permission e-mail)."

Por último transcribo los doce consejos que cita [Abad, 2001] aportados por la Eletronic Frontier Foundation para mayor protección a la intimidad en línea: "a) No revelar información personal de forma inadvertida. b) Conectar el aviso de cookies en nuestro *web browser*. c) Realizar limpiezas de direcciones de correos. d) No revelar detalles personales a extraños o recién conocidos "amigos". e) Tener cuidado con los sitios que ofrecen algún tipo de recompensa o premio a cambio de nuestro contacto o otra información. f) No responder a los envíos de correos masivos –spammers- bajo ningún concepto. g) Ser consciente de la seguridad en la Web. h) Ser consciente de la seguridad de nuestra computadora. i) Examinar las políticas de privacidad y firmas. j) Recordar que tú decides qué información sobre ti mismo revelas, dónde, por qué y para qué. k) Usar la encriptación".

**Los niños**

A través de diversa fuentes de publicación, tanto en línea como impresa, se advierte el número creciente de sitios Web dedicados a los niños o sitios Web con un vínculo a una sección o área para niños. De acuerdo con reglamentaciones vigente en los EEUU [FTC, 1999], [FTC, 2000], se toman en consideración un listado de factores que dan cuenta del dominio de un sitio Web orientado a los niños: lenguaje utilizado, temática de interés, edad de los usuarios, contenidos visual o audio, diseño de la interfaz, propaganda dirigido a los chicos, si el sitio usa caracteres animados o otros rasgos orientados a niños, etc.

De acuerdo [Demner, 2001] las prestaciones de un sitio Web orientado a los niños se pueden describir con el término "edutainment" que coincide con la descripción del software que tiene el doble propósito de educar y entretener.

En una investigación de [FCR, 2003] y otro citado por [Demner, 2001] muestra que la tendencia de los niños en Internet es buscar ayuda para las tareas de estudio, bajar software gratuito, juegos y comunicación (chat, correo electrónico).

En el primer trabajo [FCR, 2003] encontramos que "El 41% de los niños europeos de 8 a 14 años se queja abiertamente de los contenidos nocivos no deseados en Internet, a los que llegan sin buscarlos debido a la dificultad para encontrar sus Web favoritas. Un 72% de ellos se muestra partidario de establecer restricciones de contenidos que favorezcan la seguridad en la red. Estos son algunos de los datos reflejados en un estudio sobre hábitos de uso infantil de Internet en 12 países europeos realizado recientemente por la *Fundació Catalana per a la Recerca* (FCR) y la *European Schoolnet* para la Comisión Europea". Paralelamente a los riesgos de contenido a lo que están expuestos los niños cuando usan la Internet [IS, 2005] debemos agregar la utilización de los datos solicitados por los sitios y que los niños entregan cuando están en línea [FTC, 1999], [FTC, 2000].

[Nouwt, 2002] de los trabajos publicados por Annenberg Public Policy Center concluye que el 75% de los padres norteamericanos están preocupados de que la información personal de sus hijos terminen en Internet; que el 74% de los padres norteamericanos están continuamente preocupados de que sus hijos entreguen información personal a la Internet; que un año después de haberse publicado Children's Online Privacy Protection Act –COPPA- los niños no observan los requerimientos legales; por último, los chicos entregan muy fácilmente sus datos personales por intercambio de algún un objeto "gratis"; de hecho dan sus datos personales incluyendo los datos de su vida familiar.

La Comisión Federal de Comercio -Federal Trade Comisión- de los EEUU estableció reglas que los operadores deben cumplir para hacer segura la Web y proteger la privacidad de los niños mientras están en línea. Estas reglas son parte de la Ley de Protección de Confidencialidad de Menores en Línea -Children's Online Privacy Protection Act, COPPA- vigente en EEUU. La COOPA es aplicable a los operadores comerciales de sitio Web y proveedores de servicios en línea para niños menores de 13 años; también es aplicable a los operadores de sitios Web de audiencia general, quienes intencionalmente, reúnen datos personales de los niños[19].

En este apartado proponemos una guía que pueda orientar a padres y docentes en la elección de sitios Web asumiendo los contenidos de las políticas de privacidad. A

[19] Ver [Nouwt, 2002] para leer en forma detallada un análisis de los alcance de la COOPA.

partir de las reglas propuestas por la FTC se construyó la guía que no es más que árbol de requerimiento de calidad [Olsina, 2000] especificando las características, subcaracterísticas y atributos que deben ser tomados en cuanta al momento de proponer un sitio Web orientado a los niños. En el apéndice B se presenta un estudio donde se aplica esta guía para: a) discutir algunos requerimientos de calidad de sitios Web orientados a niños, fundamentalmente, en la característica de *Seguridad y políticas de privacidad*, a ser considerados en proyectos Web operativos o en la fase de desarrollo, desde el punto de vista de una audiencia de niños menores de 13 años[20] y b) analizar qué atributos de seguridad se deben tener en cuenta, como padre y docente, al momento de decidir por sitios orientados a niños.

Daremos cuenta de algunas de las definiciones que detalla la COPPA para que se pueda entender con mayor profundidad la guía propuesta más abajo:

> *Niño*: se entiende por "niño" a un sujeto menor de 13 años.
>
> *Operador*: por el término "operador" se entiende a una persona que opera un sitio Web localizado en la Internet … que reúne o mantiene información personal de o sobre los usuarios o visitante del sitio Web… o cuyo interés por la información es reunirla o mantenerla, mientras el sitio Web opera con fines comerciales, ofrece productos o servicios para la venta …
>
> *Padre*: por padre se incluye al tutor legal.
>
> *Información personal*: significa la identificación individual de un sujeto que incluye: apellido y nombre, b) dirección física (calle, provincia, ciudad, etc.), c) correo electrónico, d) numero de teléfono, e) documento de identidad, f) otro tipo de información que permita el contacto físico o en línea del individuo (escuela, etc.), g) información concerniente a los padre.

La guía tiene cuatro apartados, el apartado uno significa que el operador debe poner un vinculo –link- para anunciar sus prácticas de información en la página principal -home page- y en cada área donde reúne información de los niños, el aviso debe tener los contenidos claro y no debe tener material confuso o no relacionado; el apartado dos refiere a que el aviso a los padres debe contener la misma información incluida en el aviso que aparece en el sitio Web; para los apartados tres y cuatro, tenemos que en el primer caso el operador tiene a su disposición distintas herramientas o métodos para lograr el consentimiento de los padres en función de la utilización que hace de los datos, por ejemplo es más crítico la divulgación a terceros que la utilización interna de los datos; en el segundo caso se utilizan las mismas herramientas o métodos para obtener en forma comprobable la autenticidad de los padres.

**Árbol de requerimiento de seguridad y política de privacidad para sitios Web orientados a niños.**

1. Notificación de privacidad (Privacy notice)

1.1. Colocación del vínculo del anuncio de privacidad (placement)
- *1.1.1. El anuncio de la política de privacidad está situado en la home page.*
- *1.1.2. Está situado en la página donde solicita información personal de los niños.*
- *1.1.3. El vínculo es claro y sobresaliente.*

[20] Esta caracterización de niño rige solo para EEUU. En la Argentina se considera niños a los sujetos menores de 15 años
[Mars, 2005].

1.2. Contenidos de las políticas de privacidad (content)

*1.2.1. El idioma es el mismo del sitio Web.*
*1.2.2. Las políticas de privacidad están resumidas (vista rápida).*
*1.2.3. Las políticas de privacidad están claramente escritas y son entendibles.*
*1.2.4. Está la información de los operadores (dirección, número de teléfono y correo electrónico).*
*1.2.5. Está anunciado qué información solicitan a los niños*
*1.2.6. Cómo la recepcionan la información de los niños.*
*1.2.6.1. Directamente de los niños.*
*1.2.6.2. Usa cookies.*
*1.2.6.3. Usa web bug.*
*1.2.7. Está anunciado cómo usa la información el operador.*
*1.2.7.1. Para enviar propaganda comercial a los niños.*
*1.2.7.2. Para invitar a participar a los niños en concursos.*
*1.2.7.3 Para invitar a que el niño participe en salas de chat.*
*1.2.7.4. Para publicar los datos de los niños en tablas de anuncio.*
*1.2.7.5 Para organizar los perfiles de los usuarios.*

*1.2.8. Está anunciado si el operador comparte la información con terceras partes.*
*1.2.9. Está anunciado si los padres pueden intervenir para negar el acceso de información por terceras partes.*
*1.2.10. Está anunciado si los padres pueden revisar la información entregado por los chicos.*
*1.2.11. Está anunciado si los padres pueden solicitar borrar la información entregado por los chicos.*
*1.2.12. El sitio informa si hace transacciones comerciales.*

2. Notificación orientado a los padres (direct notice to parent)

2.1. Contenidos (content)
*2.1.1. Los padres reciben las mismas notificaciones que están incluidas en el sitio Web.*
*2.1.2. Los padres están notificados que, cuando deseen, pueden revisar la información de sus niños.*
*2.1.3. Los padres están notificados de que el operador debe tener su consenso para usar y distribuir los datos previsto por los niños.*
*2.1.4. Las notificaciones a los padres están claramente escritas y son entendibles.*
*2.1.5. Los padres están informados de los métodos empleados por el operador para ser notificados*.

3. Medios que el operador puede usar para lograr el consentimiento de los padres en forma comprobable[21] (verifiable parental consent).

3.1. Para uso interno de los datos (internal use)
*3.1.1. Correo electrónico*
*3.1.2. Llamada por teléfono*
*3.1.2. Carta*

3.2. Para divulgación pública de los datos (public disclosures)
*3.2.1. Solicita la firma de los padres (vía correo postal o fax).*
*3.2.2. Aprobar y verificar el número de la tarjeta de crédito junto con la transacción.*
*3.2.3. Llamar a los padres por teléfono.*
*3.2.4. Correo electrónico con la firma digital.*

3.3. Para divulgación de los datos a terceras partes (disclosures to third parties)[22]
*3.3.1. Solicita el consentimiento de los padres antes de divulgarla a terceras partes.*

4. Acceso a los datos por parte de los padres (access)

[21] La FTC estableció una graduación de alerta para obtener el consentimiento de los padres de acuerdo a cómo el operador usa la información personal de los niños.
[22] Se entiende por el termino *tercera parte* según [FTC, 1999] a "alguna persona que no es el operador que reúne la información de los niños ni la persona que abastece el soporte para las operaciones internas del sitio Web o del servicio en línea".

4.1. Comprobación de la identidad de los padres (verification)[23]

*4.1.1. Obtener la firma de los padres (vía correo postal o fax).*

*4.1.2. Aceptar y verificar el número de la tarjeta de crédito.*

*4.1.3. Llamar a los padres por teléfono.*

*4.1.4. Correo electrónico con la firma digital[24].*

*4.1.5. Correo electrónico acompañado por un PIN o una contraseña (password) obtenida a través de uno de los métodos de comprobación mostrado más arriba.*

4.2. Cancelar y borrado de datos por parte de los padres (revoking & deleting)

*4.2.1. Pueden cancelar y borrar la información proporcionado por los niños al operador.*

[23] Métodos que puede usar el operador para la verificación comprobable de los padres.

[24] La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido. Esta función asocia un valor dentro de un conjunto finito (generalmente los números naturales) a su entrada. Cuando la entrada es un documento, el resultado de la función es un número que identifica casi unívocamente al texto. Si se adjunta este número al texto, el destinatario puede aplicar de nuevo la función y comprobar su resultado con el que ha recibido. No obstante esto presenta algunas dificultades. En: http://es.wikipedia.org/wiki/Firma_digital

## E-learning

Una de las claves de la sociedad de la información es el requerimiento del aprendizaje permanente. Los cambios ocupacionales, la competencia global y la explosión de las tecnologías de la información ponen de relieve la necesidad de la experiencia, del conocimiento y la instrucción. Compañías lideres, universidades nacionales e instituciones educativas privadas intentan dar respuesta a la solicitud del aprendizaje permanente de empleados, profesionales de la educación y de alumnos a través del dictado de cursos específicos y de grado. Uno de los mecanismos tecnológicos para hacer frente ha esta demanda es través del e-learning en línea, es decir a través del uso de la Internet.

Entiendo que el e-learning ocurre cuando la educación y la instrucción son entregadas y soportado por las redes de comunicación, en particular por la Internet y en particular con la utilización de la tecnología Web. Otra definición, un poco más general, dada por [Foix, 2002] dice que es: *"aquella actividad que utiliza de manera integrada y pertinente computadores y redes de comunicación, en la formación de un ambiente propicio para la construcción de la experiencia de aprendizaje"*.

En este apartado intento trabajar tres cuestiones necesarias al momento de analizar el concepto de privacidad en sistemas e-learning: a) analizaremos la conveniencia de divulgar las políticas de privacidad en los sistemas e-learning; b) reconoceremos algunos *principios de privacidad* para identificar algunos atributos de privacidad en la recolección de datos c) asumiremos un modelo estándar de e-learning para comentar brevemente algunos de sus componentes con la intención de poner de manifiesto el requerimiento de privacidad entre los mismos.

## Declaración de políticas de privacidad en los sistemas e-learning

En un ambiente e-learning frecuentemente ocurren dificultades en la comunicación en cuestiones muy importantes debido a la naturaleza misma del modelo de enseñanza/aprendizaje: la comunicación está basada en la tecnología y los alumnos por si mismo autorregulan su aprendizaje. Para que los instructores se anticipen a las necesidades de los estudiantes, eviten malos entendidos y eviten trabajos engorrosos, [Waterhouse, 2004] sugiere que los instructores y tutores coloquen en el sitio, en un lugar prominente, un documento que detalle claramente las políticas que rigen el curso. Propone nueve categorías de políticas del curso que el instructor puede considerar en explicitar:

- Políticas e-learning relacionadas con el programa de estudio.
- *Políticas de privacidad del estudiante*.
- Políticas de e-mail.
- Políticas de discusión.
- Políticas de normas de software
- Políticas de tareas.
- Políticas de ayuda técnica.
- Código del estudiante, políticas de conducta o proceder.
- Políticas del derecho a la propiedad intelectual.

Veremos qué implica *Políticas de privacidad del estudiante.* Esta categoría está relacionada a cumplir los derechos legales a la privacidad y confidencialidad de los datos de los estudiantes[25]. Las políticas de privacidad de la institución responsable del curso deben estar disponibles en línea, se debe colocar un vínculo –link- en el sitio del curso a un documento donde están explicitadas las declaraciones de privacidad. El instructor debe tener presente que la privacidad del estudiante se está violando cuando se requiere fotografías y otra información personal para ofrecerla en el sitio del curso; también se viola la privacidad cuando se hace referencia a características personales como raza, etnia, discapacidades, edad y sexo, podrán ser hecho público solo si el estudiante da el consentimiento formal. Hay estudiantes que no ponen objeciones que su información personal este disponible para otros estudiantes y visitantes del curso. Sin embargo los estudiantes apreciaran conocer que el acceso por otros a su información personal es permitido por ellos voluntariamente.

[Waterhouse, 2004] sugiere el siguiente modelo de autorización para obtener el consentimiento del alumno en la administración de su intimidad:

**Formulario de autorización**

Nombre del estudiante…….…… Curso…….

Nombre de los instructores……..

Doy al instructor nombrado arriba autorización para hacer público o referenciar aquellos ítems señalados en el listado de abajo. Esta autorización se aplica a los trabajos que he completado en el curso indicado.

_Mi comentarios en el chat.

_Mis comentarios en los forum electrónicos.

_Mis comentarios en el e-mail.

_Ejemplos de mis trabajos escritos.

_Mi nombre como parte del listado de estudiante de la clase.

_Mi fotografía.

_Mi biografía.

_Otros_____

Cuando mi trabajo sea usado, deseo que incluya una identificación de que el trabajo es mío.

Las políticas frecuentes para administrar la privacidad y la seguridad [El-Khatib, 2003] son expresadas generalmente en términos de autorización y de obligación imperativas sobre los individuos y sobre los objetos: las políticas de autorización definen las acciones autorizadas y no autorizadas de un individuo sobre los objetos; las políticas de obligación especifica las obligaciones negativas y positivas de un individuo en dirección a un objeto. Además así como en la educación tradicional cara a cara, la confianza es un tema importante en los sistemas e-learning. La confianza conforma un requerimiento fundamental entre el usuario y el proveedor del servicio. Por ejemplo un proveedor del servicio debe tener la seguridad de que el usuario que accede al servicio

[25] En la mayoría de las instituciones educacionales de los EEUU las política de privacidad están en consonancia con Family Educational Rights and Privacy Act –FERPA. En: http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

tiene verdaderamente su credencial y que no lo ha falsificado y que está autorizado a atender el curso. Del lado del estudiante debe también estar seguro de los servicios solicitado y que sus datos estarán resguardados bajo los principios de privacidad –ver en el próximo apartado. Los mecanismos comunes que aseguran la confianza están relacionados a la certificación digital. Normalmente un certificado consiste de una clave pública, que certifica la información y una firma digital que certifica la autoridad. La información que contiene el certificado es el nombre del usuario y otros datos pertinentes; la firma digital autentica al usuario como el dueño de la clave pública.

**Principios de privacidad**

En la actualidad diversas universidades ponen al servicios de sus alumnos cursos de actualización y perfeccionamiento utilizando la metodología e-leaning. Los software encargado de sostener esta metodología de enseñanza se los denomina sistemas de gestión de aprendizaje -*Learning Management Systems*- y, entre otras cosas, se encargan según [Foix, 2002] de: "a) gestionar los usuarios: inscripción, control de sus aprendizajes e historial, generación de informes, etc.; b) gestionar y lanzar los cursos, realizando un registro de la actividad del usuario: tanto los resultados de los tests y evaluaciones que realice, como de los tiempos y accesos al material formativo; c) gestionar los servicios de comunicación que son el apoyo al material online, foros de discusión, charlas, videoconferencia; programarlos y ofrecerlos conforme sean necesarios".

El crecimiento constante del uso de estas plataformas para ofrecer conocimientos en línea pone de manifiesto la necesidad, también creciente, de proteger la privacidad de los alumnos. La privacidad se describe según [El-Khatib, 2003] como la facultad del estudiante en conservar un "espacio personal", en cuyo interior él pude controlar las condiciones bajo el cual la información personal será compartida con otros. [Yang, 2002] define privacidad como el interés que poseen los estudiantes por mantener un "espacio personal" libre de la interferencia de otras gentes y otras organizaciones.

Los principios de privacidad fueron desarrollado para exponer las implicaciones de las leyes de privacidad [El-Khatib, 2003].y mostrar las "prácticas de la información" de las organizaciones encargada de reunir información [FTC, 1998]. A la luz de estos principios podemos valorar la aplicación de buenas prácticas de la información. Esos principios se pueden encontrar en:

a) [FTC, 1998] en el capítulo "III. Fair Information Practice Principles"- encontramos con los principios de notice/awareness –aviso/conocimiento-, choice/consent –elección/consentimiento-, access/participation –acceso/participación, integrity/security –integridad/seguridad y enforcement/redress –coacción/resarcir.

b) [FTC, 2000], principios que se encuentran en el "Children's Online Privacy Protection Act" -COPPA-, para verificar las prácticas de la información personal de menores de 13 años por parte de las organizaciones de los EEUU. Estos principios fueron trabajados en el apartado "Los niños".

c) [El-Khatib, 2003] describe diez principios de privacidad, incorporado en la *Ley de protección de información personal y documentos electrónicos* de Canadá. Estos principios nos hablan de: accountability; identifying purposes; consent; limiting collection; limiting use, disclosure, and retention; accuracy; safeguards; openness; individual access y challenging compliance.

A continuación en la tabla siguiente [El-Khatib, 2003] sugiere como cada principio puede ser implementado en un sistema e-learning:

| | |
|---|---|
| Accountability | El nombre y la información de contacto de la persona, quién es responsable, debe estar claramente divulgado en el sistema en línea de la organización. |
| Identifying purposes | Los propósitos deben estar claramente identificados por el sistema en línea de la organización y pueden ser recuperados a voluntad por el estudiante. |
| Consent | El consentimiento del estudiante es obtenido por el sistema en línea de la organización en la figura de una firma certificada que garantice la autenticación del alumno. |
| Limiting collection | El sistema de la organización conservara seguro los logs con sus datos acumulados y proveerá el acatamiento a los principios exigidos; por añadidura el sistema de la organización identificará cómo reunirá la información para mostrar que dicha acumulación fue hecha por medio honrados. |
| Limiting use, disclosure, and retention | El sistema de la organización conservara seguro los logs de sus usos, divulgación, o retención de los datos y que cumple con los principios demandados. |
| Accuracy | El sistema puede: a) solicitar que el estudiante verifique que los datos son precisos y completo al terminar su entrega, b) solicitar que el estudiante mantenga actualizado su información personal y c) identificar inconsistencia en los datos a través de verificaciones basados en reglas. |
| Safeguards | Implementar sistemas de autenticación y encriptación para garantizar la seguridad de los datos. |
| Openness | El sistema en línea de la organización debe advertir de sus políticas y prácticas relacionadas a la administración de la información personal del estudiante, tanto como proveer facilidad en el acceso a esta información. |
| Individual access | El sistema en línea de la organización debe proveer facilidad para que el estudiante ejecute todas las funciones necesarias para verificar que se cumplen los principios de privacidad. |
| Challenging compliance | El sistema en línea de la organización debe garantizar que el estudiante puede dirigirse al responsable para exigir que se cumpla con los principios de privacidad. |

**Un modelo de e-learning**

Según [Foix, 2002] al hablar sobre un estándar e-learning, "nos estamos refiriendo a un conjunto de reglas en común para las compañías dedicadas a la tecnología e-learning. Estas reglas especifican cómo los fabricantes pueden construir cursos en línea y las

plataformas sobre las cuales son impartidos estos cursos de tal manera de que puedan interactuar unas con otras".

A continuación daremos una noción de la norma Learning Technology Systems Architecture –LTSA- tomado de la IEEE P1484.1/D9, 2001-11-30 para analizar los requerimiento de privacidad en dicho modelo según [El-Khatib, 2003]. LTSA según [IEEE, 2001] es una norma que especifica una arquitectura de alto nivel para la educación, el aprendizaje y sistemas de instrucción apoyados en la tecnología de la información, describe el diseño de alto nivel y los componentes de este sistema. Esta norma cubre un amplio rango de sistemas, conocidos comúnmente como tecnología del aprendizaje, tecnología de la educación e instrucción, enseñanza basada en la computadora, instrucción asistida por computadoras, tutores inteligentes, metadatos, etc.

En general, el propósito de desarrollar arquitectura de sistemas es descubrir modelos de alto nivel para entender cierta clase de sistemas, sus subsistemas y su interacción con otros sistemas, es decir más de una arquitectura es posible.

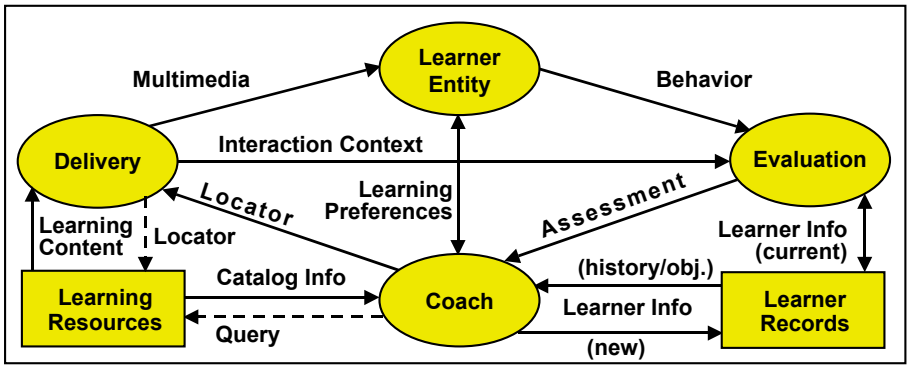
Una arquitectura es un modelo para diseñar un rango de sistemas que perduren en el tiempo, y para el análisis y comparación de estos sistemas, es decir, una arquitectura se usa para el análisis y comunicación.

Con la intensión descubrir los componentes compartido de sistemas diferentes a un nivel correcto de generalidad, una arquitectura promueve el diseño e implementación de componentes y subsistemas que son reusables, rentables y adaptables, es decir, la interoperabilidad de interfases y servicios están identificados.

La norma identificará los objetivos de actividades humanas y los procesos de computación y sus categorías invocadas de conducta, es decir que es posible identificar protocolos y métodos de cooperación y colaboración.

El LTSA identifica cuatro procesos: la entidad aprendiz - learner entity-, evaluación – evaluation-, entrenador – coach- y proceso de entrega - delivery process-; dos depósitos: archivo del estudiante y recursos del aprendizaje; y trece flujo de información entre estos componentes: las observaciones conductuales, la información de valoración, la información del aprendiz -tres veces-, pregunta –query-, información de catalogo, localizador –dos veces-, contenidos de aprendizaje, multimedio, el contexto de interacción, y preferencias de aprendizaje.

Un esquema de los componentes del sistema es el siguiente:




The LTSA system components

A continuación describiremos algunos componentes involucrados para luego mostrar en otro esquema los requerimientos de privacidad.

*Learner entity*: Un proceso conceptual que representa una abstracción de un aprendiz humano. La entidad del aprendiz puede representar un solo aprendiz, un grupo de aprendices que aprenden en forma individual, un grupo de aprendices que aprenden en forma colaborativa, un grupo de aprendices que aprenden en diferentes roles y así sucesivamente.

*Coach*: Un proceso conceptual que puede incorporar la información de varias fuentes, desde el aprendiz -preferencias del aprendizaje-, desde el proceso de la evaluación -valoración de la información-, desde la inscripción del aprendiz -la actuación, preferencia, y otra información del aprendiz-, y desde los recursos del aprendizaje -preguntas e información del catálogo-, y puede usar esta información para investigar y seleccionar contenidos para el aprendizaje -vía el proceso de entrega y multimedios- para la experiencia del aprendizaje.

*Evaluation*: un proceso conceptual que produce medidas de la entidad aprendiz - learner entity. Las entrada/salida de este proceso son:

-Entrada- Conducta observable de la entidad aprendiz - learner entity.

-Entrada- El contexto de interacción puede proporcionar el contexto para que la conducta del aprendiz -learner entity- establezca su evaluación apropiada.

-Salida- La información de valoración puede enviarse al proceso entrenador –coach.

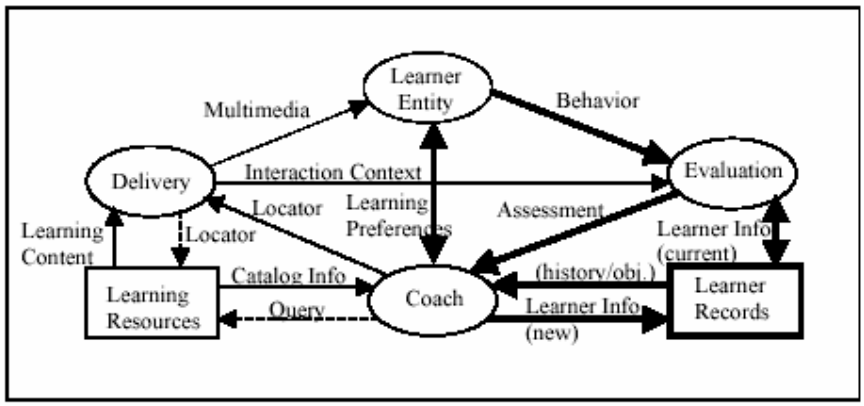
-Entrada/salida- La información del aprendiz puede ser recuperada y guardada durante el proceso de evaluación en los archivos del alumno.

Learner Records: un depósito de los datos, información del aprendiz tal como actuación, preferencia y otro tipo de información. El depósito de los datos puede guardar/recuperar información sobre el pasado –por ejemplo, archivos históricos de aprendiz-, puede también tener información sobre el presente –por ejemplo, valoración corriente para reasumir o suspender una sesión- y del futuro –por ejemplo, pedagogía, empleador objetivo, etc.

Learning Preferences: Un datos fluye en dos vías, mientras representa intercambio -por ejemplo, negociación- entre el proceso *learner entity* y el proceso *coach*. Además del aprendiz, el padre, maestro, mentor, patrón, y/o institución pueden participar en la negociación de las preferencias del aprendizaje.

En las preferencias del aprendizaje pueden incluir el tipo de información, como las preferencias de adaptación cultural, requisitos de la accesibilidad y preferencias para las personas con las limitaciones físicas -por ejemplo, ceguedad, sordera- y las limitaciones cognoscitivas.

Según [El-Khatib, 2003] en el esquema siguiente, tomando en consideración los componentes anteriores, podemos ver -líneas gruesas- el flujo de la información que requieren fundamentos de privacidad:




En detalle el flujo de la información que requiere fundamentos de privacidad se transmite desde:
-el canal de transmisión entre la learner entity y los módulos de evaluation y coach;
-el canal de transmisión entre el módulo evaluation y coach;
-el canal de transmisión entre el modulo evaluation y learner records;
-el canal de transmisión entre el coach y learner records y
-learner records con ellos.

## A modo de conclusión

Comencé este trabajo analizando algunas versiones sobre la noción de intimidad. La primera conclusión que podemos sacar sobre este apartado es que no hay una definición universal sobre lo que se entiende por privacidad o intimidad. Del esfuerzo de [Desantes, 1991] encontramos algunas notas distintivas de la noción de intimidad y que ayudan a entender que no es lo mismo recibir un correo electrónico que no se desea en nuestra casilla, que nuestras ideas, gustos, sentimientos y convicciones más personales, estén a disposición de empresas o gobiernos sin nuestro consentimiento. Por otro lado diferente son las versiones de intimidad si nacen de organizaciones comprometidas con los usuarios que navegan en Internet que de las empresas que sólo buscan que la tecnología les facilite el rédito comercial.

Del segundo apartado la conclusión que surge es que, aun conociendo en teoría algunas de las tecnologías que ponen en tensión la intimidad, la sensación que queda en los usuarios es que estamos indefensos ante la invisibilidad de la recogida de datos que pueden hacer las compañías comerciales o los gobiernos.

En el tercer apartado se hace una vista de las distintas tecnologías que intentan dar respuesta a los intentos de las compañías comerciales de autorregularse. Y la conclusión es que, asumo lo que escribe [Chung, 2002], que regular los asuntos de intimidad por leyes es bueno si la autorregulación falla al momento de orientar adecuadamente los asuntos de intimidad.

El último apartado está dedicado a los niños, la guía propuesta está en relación con el escepticismo ante la propuestas de que la propia tecnología da respuesta a los problemas de intimidad: la intimidad de los niños estará mejor protegida si los adultos participamos activamente en el análisis de las declaraciones de privacidad que proponen los sitios Web y actuamos en consecuencia.

En el apartado e-learning brevemente he mostrado a partir del trabajo de [El-Khatib, 2003] tres cuestiones importantes al momento de analizar una plataforma de e-learning. Se necesitan hacer conocer las políticas de privacidad de la institución encargada de impartir los cursos; se necesitas principios de privacidad para detectar las prácticas de información de una plataforma; por otro lado en un modelo de e-learning se puede visualizar las vías por donde es necesario requerimientos de privacidad.

Por último, como conclusión general, puedo escribir que la temática de la intimidad y su relación con las tecnologías de la información merecen aun mayor profundidad enfocando el análisis en: a) hacer estudios que involucren a los usuarios para detectar el grado de conocimiento que ellos tienen sobre los aspectos legales en el uso de la Internet, b) estudio de las distintas tecnologías del apartado tres con un grupo de usuarios para analizar las consecuencias del los mismos y si cumplen las expectativas que de ellos se esperan, c) estudiar algunas propuestas para que se incluya en la planificación escolar el tema de la intimidad en relación al uso de las nuevas tecnologías de la información, apuntado a evitar que los alumnos experimenten a contenidos que pongan en riesgo se estructura psíquica y d) para un trabajo futuro queda hace un estudio critico de las plataformas e-learning más populares para verificar los principios de privacidad y la relación estrecha con mecanismos de seguridad; por otro lado, analizar los distintos estándares propuesto de e-learning para verificar los fundamentos de privacidad.

**Apéndice A: P3P**

Según [P3PToolbox, 2005] las políticas de privacidad surgieron en la Web para mejorar el dialogo ente las compañías y los consumidores asumiendo el uso que hacen los primeros de la información de los segundos. Dichas políticas, sin embargo, siguiendo a [P3PToolbox, 2005] son engorrosos al momento que el consumidor quiere leerlas y entenderlas y, frecuentemente, es muy difícil rastrear las políticas de privacidad y la relación de varias entidades que reúnen información en sitio Web. El tiempo requerido para encontrar y leer las políticas de privacidad pueden ser excesivos y, además, puede no estar escrito para que sean fáciles de entender por los visitantes a la Web. Muchos usuarios, considerando aquellos que tiene preocupación por el destino de su información, simplemente ignoran las declaraciones de estas políticas de privacidad. Como consecuencia resulta necesario, escriben [P3PToolbox, 2005], modernizar la comunicación entre los usuarios y los sitios Web con el propósito de resguardar los datos personales de los primeros

Según [Cranor, 2002], que cuenta el desarrollo de P3P, los miembros de la Platform for Internet Content Selection –PICS- discutieron en el año 1995 la posibilidad de usar la PICS como herramienta para proteger la privacidad de los usuarios de Internet. La PICS, como dijimos más arriba, es un sistema de marcas de contenidos de la Web de acuerdo a un juego de criterios llamados sistema de clasificación -rating system-. A mediados de noviembre del año 1996 el Center for Democracy and Technology convoca al Internet Privacy Working Group para promover la exploración del desarrollo de una herramienta de privacidad con alguna características o forma de PICS. Resumiendo lo que cuenta [Cranor, 2002], P3P fue enfocado como un sistema de negociación para alcanzar un acuerdo sobre las prácticas de privacidad de los sitios Web y se sugería que P3P podía incluir mecanismos de transferencia de datos tomando en consideración dicho acuerdo. Posteriormente el grupo, aduciendo razones políticas y técnicas, rechaza los mecanismos de transferencia de datos. El término "negociación" fue evolucionando en todo el proyecto. Originalmente algunos de los participante tenían como visión un sistema que permitiría al sitio Web y un usuario agente hace un regateo sobre las prácticas de privacidad, obligándose ente ellos a una serie de ofertas y contra ofertas. Esta ronda de negociación fue reemplazada posteriormente por una única negociación en el cual el sitio tiene que brindar toda su oferta de una vez. Si hay más de una oferta el usuario agente puede elegir una. Finalmente la negociación fue rechazada por completo a fin de simplificar la implementación de P3P y que los sitios Web pudieran implementar P3P sin agregar un software especial a sus servidores.

¿Qué es hoy P3P? De acuerdo a [W3C, 2005] P3P "facilita a los sitios Web expresar sus prácticas de privacidad en un formato normalizado que pude ser recuperado automáticamente e interpretado fácilmente por un agente usuario. Los agentes usuarios P3P permitirán a los usuarios estar informado de las prácticas del sitio –las prácticas de privacidad expresado en ambos formatos: legible por los humanos y por las máquinas- y tomar decisiones automáticas basadas en estas prácticas cuando son apropiadas. Así los usuarios no necesitan leer las políticas de cada sitio cuando son visitados… Aunque P3P provee un mecanismo técnico para asegurar al usuario estar informado sobre las políticas de privacidad antes que ellos liberen su información personal, no provee un mecanismo técnico para asegurar que los actos del sitio están acuerdo a las políticas que expresan… P3P no incluye mecanismos para transferir datos o para asegurar datos personales en el tránsito o el almacenaje".

Otra perspectiva para analizar P3P es siguiendo a [Williams, 1998]. Dice que la Internet se define por un juego de "protocolos" que definen el formato y la secuencia de comunicación sobre la red. Por ejemplo el Protocolo de Internet –IP- define las reglas básicas que debe seguir una computadora para comunicarse en Internet, especifica exactamente cómo se debe formar un paquete y cómo debe encaminar un ruteador cada paquete a su destino; pero este protocolo no resuelve todos los problemas que pueden ocurrir, entonces por capas adicionales de protocolo que se suman al IP se crean conductas más complejas. Por ejemplo el protocolo TCP le suma información adicional al IP para garantizar el manejo de los errores de comunicación, asegurando el envío de datos entre computadoras a través de la red. El HTTP le adiciona más capacidad al protocolo TCP, y así. P3P le adiciona capacidad al HTTP. En respuesta a un pedido habitual de información, un servidor habilitado con P3P responderá con una "propuesta" a quien solicita la información segura, señalando como las contestaciones estarán protegidas. El cliente usuario responderá aceptando o rechazando la "propuesta". El protocolo P3P define las reglas del juego de regateo entre un agente automatizado en un sitio Web y un visualizador de Web -Web browser-.

. En un nivel básico [P3PToolbox, 2005], P3P es un vocabulario y sintaxis legible por la máquina que expresan las prácticas de administración de los datos de los sitios Web. Las políticas P3P de lo sitios presentan una breve instantánea de cómo los sitios reúnen, tratan y usan la información personal de sus visitadores. Los visualizadores –browser- de la Web habilitados para P3P y otras aplicaciones P3P "leerán" y "entenderán" esta información instantánea en forma automática, comparara con el propio juego de preferencia de privacidad del usuario Web e informará al usuario cuando estas preferencias no son iguales a las prácticas del sitio que él o ella han visitado.

Según [W3C, 1998], P3P puede ser visto simplemente como un protocolo para intercambio de datos estructurados. Una extensión de mecanismo HTTP1.1 es usado transportar la información (ofertas y elementos de datos) entre un cliente y el servicio. En un nivel más detallado, P3P es una especificación de sintaxis y semántica para describir prácticas de la información y elementos de datos. La especificación usa XML[26] y RDF[27] para capturar la sintaxis, la estructura, y la semántica de la información.

El vocabulario de P3P, según [P3PToolbox, 2005], consiste en algunos de los siguientes interrogantes: quién es el que acopia los datos; qué datos acopia; para qué propósito se usarán los datos; hay alguna facultad para opt-in o opt-out del empleo de los datos; quien recibe los datos -alguien más allá del colector de datos-; qué es la política de retención de datos; qué información proporciona el colector de datos para el

[26] XML (eXtensible Markup Lenguaje) [W3C, 1997], describe una clase de objetos llamados documentos XML y describe parcialmente el comportamiento del programa de computadora que procesa el documento. XML es un perfil de un modo de uso o una forma restringida de SGML, el Standard Generalized Markup Lenguaje. Por su construcción, los documentos XML, se ajusta a los documentos SGML.

[27] [W3C, 1999] " …Los metadatos son "datos sobre los datos" (por ejemplo, un catálogo de biblioteca es [un registro] de metadatos, en el sentido de que describen publicaciones) o concretamente en el contexto de esta especificación "datos que describen recursos Web". La distinción entre "datos" y "metadatos" no es incuestionable; es una diferencia creada en primera instancia por una aplicación particular, y muchas veces el mismo recurso se interpretará de ambas formas [como dato y como metadato] simultáneamente…. Resource Description Framework (RDF) [Infraestructura para la Descripción de Recursos] es una base para procesar metadatos; proporciona interoperabilidad entre aplicaciones que intercambian información legible por máquina en la Web. RDF destaca por la facilidad para habilitar el procesamiento automatizado de los recursos Web".

acceso a los mismos ; dónde está la política de privacidad legible por los humanos; cómo serán resueltas las discusiones sobre la política de privacidad[28].

Cómo funciona P3P. Según [Garfinkel, 2002] las especificaciones de P3P incluyen: un vocabulario –vocabulary- normalizado para describir las prácticas de los datos del sitio Web; un juego de elementos de datos de apoyo –base data elements- que el sitio Web puede atribuir a sus políticas de privacidad P3P; un protocolo para solicitar y transmitir las políticas de privacidad del los sitios Web.

El protocolo P3P [Garfinkel, 2002] es una extensión del protocolo HTTP. De acuerdo a la figura Nº 1 el usuario agente P3P usa una solicitud HTTP para traer el *archivo de referencia de política* P3P desde una "localización conocida" en el sitio Web al cual el usuario está haciendo la solicitud. El archivo de de referencia de política indica la localización del *archivo de política*[29] P3P que aplicará a cada parte del sitio Web. Puede haber una política para el sitio entero o varias políticas que cubren diferentes partes del sitio. El usuario agente puede traer la política apropiada, analizar las partes, y tomar las acciones de acuerdo a sus preferencias.

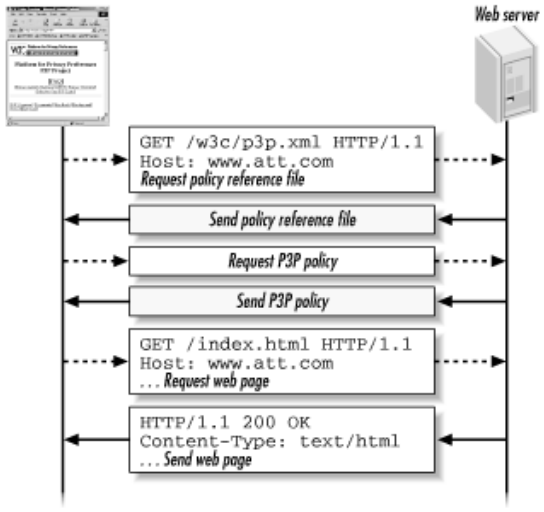



Figura Nº 7: el protocolo básico para traer una política P3P[30]

[28] El lector puede leer observaciones interesantes al sistema P3P en [Coyle, 1999].
[29] El *archivo de política P3P* es un documento que usa el código y sintaxis P3P, que entiende un usuario agente, en dicho documento se declaran las políticas de privacidad.
[30] Figura extraída del trabajo [Garfinkel, 2002].


Figura Nº 8: A la izquierda una declaración de privacidad en inglés, a la derecha en sintaxis P3P[31]

Para desarrollar declaraciones de políticas de privacidad para sitios Web que soportan el lenguaje P3P, IBM [IBM, 2000] creo una herramienta visual denominada P3P Policy Editor. Siguiendo a [IBM, 2000], una organización que publica sus políticas de privacidad de acuerdo a las especificaciones P3P debe colocar en su sitio Web las descripciones de las políticas en formato XML, que puede leer la máquina; incluyen en esta descripción el tipo de información que reúne, como es usada y quién tiene acceso a la información. Desarrollar las declaraciones P3P puede ser muy complicado y son susceptibles de error por parte de los administradores de la Web, por lo tanto la herramienta P3P Policy Editor permite automatizar el desarrollo de las políticas de privacidad, creando el formato XML y un documento en formato HTML que pude ser entendido por los usuarios.

[Garfinkel, 2002] escribe un esbozo de los pasos generales involucrados en el desarrollo de una política de privacidad bajo las especificaciones P3P. Suma, además, el esbozo de los puntos básicos que debe responder, como mínimo, una política de privacidad tomando en consideración los requerimiento del usuario.

Las consideraciones de [Garfinkel, 2002] son útiles para desarrollar las políticas de privacidad antes de implementarla en el P3P Policy Editor. El editor de IBM en su Help solicita que se planifique la política de privacidad tomando en cuenta, brevemente:

Organización: una política bajo P3P debe entregar el nombre legal del negocio u organización que hace las exigencias en la política de privacidad.

Garantía: esta información describe como las disputas y violaciones de las prácticas de privacidad de la propia organización pueden ser resueltas.

La reunión de los datos y usos: una política P3P debe contener un mínimo grupo de datos que declarar: el tipo de datos recogidos por el sitio Web, por qué se

[31] Ejemplo extraído de [Cranor, 1999].

recoge y quien recibe los datos. Cada tipo de dato reunido está representado en la política de privacidad como un elemento de dato (data element). Muchos elementos de datos ya son definidos por el P3P como esquema de datos (data schema). El esquema de los datos está compuesto de cuatro juego de datos: Dynamic data, User information, Third-party individual information y Business information.

Uso de categoría de datos: otra manera de describir los datos es usar categorías de datos. Un elemento de dato puede asignarse a una categoría de datos para dar a los usuarios y agente usuario indicios adicionales sobre el tipo de información que está reunido en el sitio de Web.

Planificar nuevos elementos de los datos: pueden crearse juegos de datos que representan tipos especializados de información que reúne un sitio de Web.

Grupo de datos: después de que se ha determinado los elementos de datos que se necesita en la política, se pude colocar los elementos de datos en uno o más grupos de datos. Cuando un elemento de dato o el juego de datos se pasan a un grupo de datos, se declaran como parte de la política y se conocen como un elemento de la política. Los grupos datos en una política son distinguidos por su propósito, para qué los datos son usados, y por el recipiente, quién usa los datos.

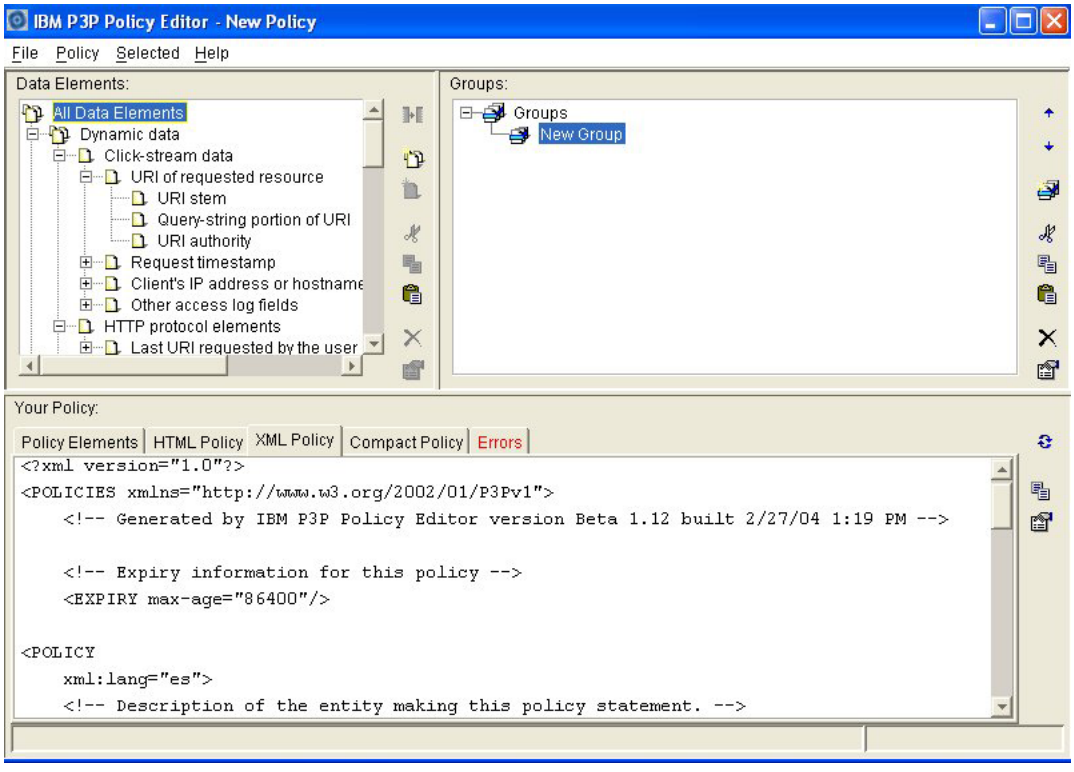



Figura Nº 9: Pantalla del IBM Policy Editor

Algunas organizaciones han publicado herramientas, agente usuarios, que soportan P3P y otros han anunciado planes para usarlo. Los tipos de agentes que pueden

aparecer incluyen visualizadores –browser- de Web y plug-ins para los browser que le entregan diferentes o adicionales características de privacidad P3P.

Según [Garfinkel, 2002] el primer agente usuario que aparece en la escena es el Internet Explorer 6.0 de Microsoft. Contiene un soporte restringido para P3P, limitado al llamado *políticas compacta* de P3P que describe cómo un sitio usa la información acumulada empleando cookies: establece si el usuario acepta o no acepta cookies de un sitio Web. Un usuario puede ver una advertencia cuando el browser encuentra un cookie que no tiene un acuerdo de política de P3P o que tiene una política P3P que no es igual al juego de preferencia de privacidad del usuario, establecido en IE bajo la solapa "Privacidad" en la opción "Opciones de Internet"[32].


Figura Nº 10

Haciendo clic en el icono advertencia el IE muestra el "Informe de privacidad" que está bajo la opción "Ver" del menú principal.

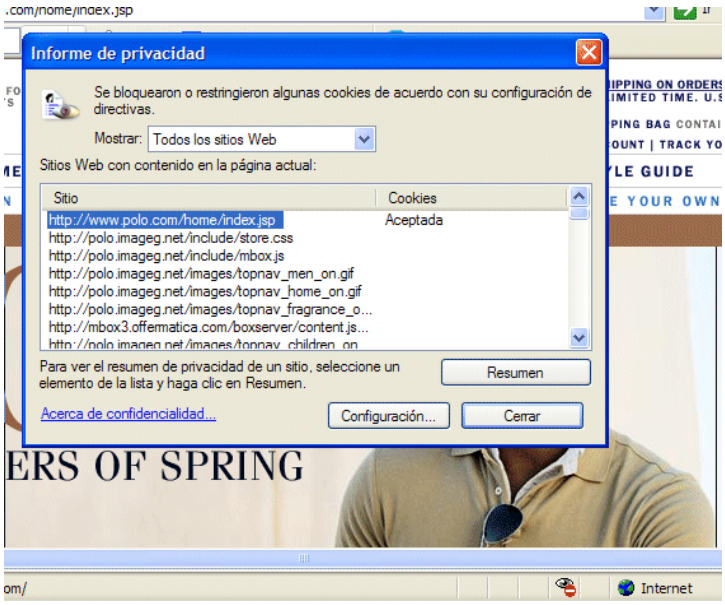



Figura Nº 11

Mientras visualiza la Web con el IE 6.0 el usuario haciendo clic en el botón "Resumen" verá la versión legible por los humanos de la política P3P. Y podrá ver algo como esto:

[32] Las pantallas usadas como ejemplo muestran las políticas P3P del sitio Ralph Lauren Polo.com cuyo URL es: http://www.polo.com/home/index.jsp

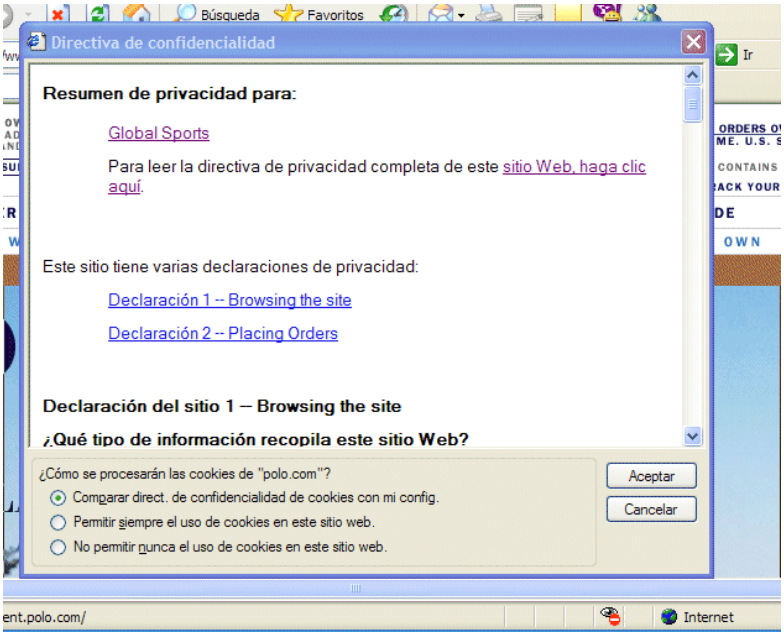



Figura Nº 12

Para modificar las preferencias de privacidad en IE 6.0, el usuario puede cambiar sus preferencias usando el botón que se desliza hacia arriba o hacia abajo:

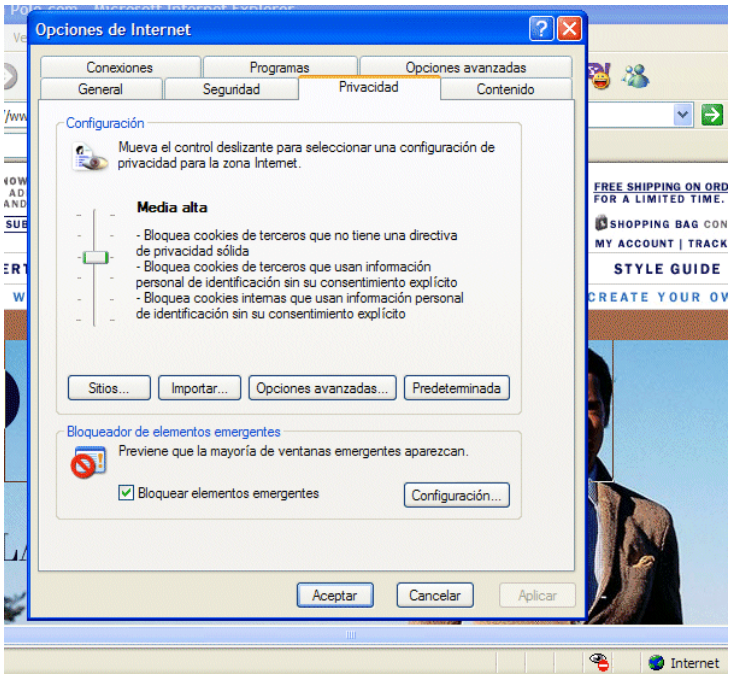



Figura Nº 13

En la dirección http://www.microsoft.com/latam/windowsxp/pro/usando/tutoriales/security/ie6.asp se informa cómo usar las características de seguridad y privacidad en Internet Explorer 6.

Otro usuario agente es el PrivacyFinder, [PrivacyFinder, 2006] software basado en el desarrollo original de AT&T Corp., operado en la actualidad por la CMU Usable Privacy and Security Laboratory (CUPS) de Carnegie Mellon University.

Es un artefacto de búsqueda que soporta P3P que el usuario puede incrementar de acuerdo a su preferencia. Una vez que el usuario declara sus preferencias (bajo, medio, alto, o personalizado), los resultados de la búsqueda son arreglados basado en cómo las políticas de privacidad leídas por la computadora cumple con las preferencias. Un pájaro rojo indica que el sitio tiene conflictos con las preferencias mientras un pájaro verde indica la complacencia. El pájaro amarillo indica que incapaz de sacar o leer una política de privacidad del sitio Web. El pájaro gris aparece cuando la política de privacidad ha sido inválida o no puede ser localizado.

Cómo trabaja PrivacyFinder. Siguiendo a [PrivacyFinder, 2006], después de escribir el término de búsqueda y seleccionar las preferencias de privacidad, PrivacyFinder usa el API[33] -mirar las opciones- del buscador de Yahoo! o de Google para recuperar una lista de resultados. Luego PrivacyFinder verificará cada uno de estos sitios Web haciendo el intento por localizar una política de P3P. Si una política válida se encuentra, la política se evalúa contra sus preferencias declaradas.


Figura Nº 14: Página principal de PrivacyFinder

[33] El servicio Google Web APIs es un programa beta que permite a desarrolladores encontrar y manipular fácilmente la información en la Web. En: http://www.google.com/apis/api_faq.html#gen1

## Apéndice B: Evaluación de declaración de políticas de privacidad en sitios Web orientados a niños


### Resumen

Este estudio es un intento de evaluar, por un lado, las declaraciones de políticas de privacidad de los sitios Web orientado a los niños, para ser considerado en la fase de operatividad y desarrollo y, por otro, orientar a docentes o padres en la elección de los mismos. Se toma como referencia una Guía de la Comisión Federal de Comercio de EEUU para construir un modelo de calidad representado por árbol de requerimiento de características y atributos. Se estudian 40 sitios Web, analizando 23 atributos de seguridad directamente mensurables. El trabajo nos da información útil para considerar las disponibilidades de atributos y características de seguridad, tomando en consideración al visitante de los sitios: niños menores de 13 años.



**Palabras claves:** métricas, política de privacidad, educación, niños


### Introducción

De acuerdo a un artículo de la [FTC, 1998] dirigido al Congreso norteamericano los niños representan un segmento en crecimiento como consumidores en línea y son el blanco de los sitios comerciales. Como consecuencia, hay un crecimiento constante, de sitios Web orientados a niños o sitios Web con áreas dedicados a niños.

Para caracterizar un sitio Web orientado a niños la FTC -Federal Trade Commission- considera varios factores: contenido del material, contenido visual o audio, propaganda dirigido a los niños, información en lo que respecta a la edad de la audiencia actual o a la que se tiene como propósito y si la interfase es de característica animada o tiene otros rasgos orientados a los niños. De acuerdo a [Demner, 2001] las prestaciones de un sitio Web orientado a los niños se pueden describir con el término "edutainment" que coincide con la descripción del software que tiene el doble propósito de educar y entretener.

En una investigación de [FCR, 2003], otro citado por [Demner, 2001] y en el capítulo "C.Children's Privacy Online" de la [FTC, 1998] muestra que la tendencia de los niños en Internet es buscar ayuda para las tareas de estudio, bajar software gratuito, juegos y comunicación con sus pares a través del chat, tablas de anuncio y correo electrónico.

Los sitios Web comerciales, de entretenimiento y con contenidos útiles para la escuela reúnen información personal a través de medios explícitos que incluyen: registrarse a los sitios, encuestas a los usuarios, respuestas en línea, llenado de formularios, etc. Además, los sitios reúnen información personal de los usuarios a través de medios no obvios como los usos de los cookies o los web bug [Chung, 2002].

Según [Castro, 2002], las nuevas tecnologías de la información están caracterizadas por la eficacia en la recogida de datos –invisibilidad-, desventaja del usuario del poder que tiene en relación con el proveedor de servicios y escasa molestia al usuario en la recogida de datos. Como consecuencia las nuevas tecnologías han producido dos nuevas mercancías: los perfiles individuales y los colectivos de los usuarios. Según [Chung, 2002] la frecuencia, la facilidad y el relativo bajo costo de la recogida de información distingue el ambiente online de Internet de otros medios tradicionales de información y reunión de información.

La Comisión Federal de Comercio de los EEUU estableció reglas que los operadores deben cumplir para hacer segura la Web y proteger la privacidad de los niños mientras están en línea. Estas reglas son parte de la Ley de Protección de Confidencialidad de Menores en Línea -Children's Online Privacy Protection Act, COPPA- vigente en EEUU. La COOPA es aplicable a los operadores comerciales de sitio Web y proveedores de servicios en línea para niños menores de 13 años; también es aplicable a los operadores de sitios Web de audiencia general, quienes intencionalmente, reúnen datos personales de los niños[34].

Este trabajo tiene dos propósitos: a) discutir algunos requerimientos de calidad de sitios Web orientados a niños, fundamentalmente, en la característica de *Seguridad y políticas de privacidad*, a ser considerados en proyectos Web operativos o en la fase de desarrollo, desde el punto de vista de una audiencia de niños menores de 13 años[35] y b) analizar qué atributos de seguridad se deben tener en cuenta, como padre y docente, al momento de decidir por sitios orientados a niños. Se parte de un modelo de calidad jerárquico representado por un árbol de características y atributo, conforme a una categorización específica para el dominio [Olsina 2000].

Para la construcción del árbol de características y atributos se tomo como referencia la Guía de la FTC denominada "How to Comply Whith The Children's Online Privacy Protection Rule" [FTC, 2000]. En particular para este estudio se asumió sólo el apartado referente a los contenidos denominados *Notificación de privacidad (Privacy Notice)*. Recordemos que esta Guía solo es aplicable en los EEUU, pero resulta de interés para este trabajo porque nos ayuda decidir qué atributos de seguridad son necesarios a tomar en cuanta al momento de construir un sitio para niños o al momento de decidir, por parte de los tutores, los sitios que los niños pueden frecuentar.

**Políticas de privacidad y otras definiciones**

Una política de privacidad o "una normativa de confidencialidad es una declaración que explica la manera en que un sitio Web usará los datos personales que sus visitantes proporcionan." [Yahoo, 2005].

La Federal Trade Commission [FTC, 1998] en un artículo dedicado a los consumidores, con un apartado dedicado a los niños dice que es: "a statement on a website describing what information about you is collected by the site, and how it is used. Ideally, the policy is posted prominently and offers you options about the use of your personal information. These options are called opt-in and opt-out. An opt-in choice means the website won't use your information unless you specifically say it's okay. An opt-out choice means the website can use the information unless you specifically direct it not to".

**Especificación de los requerimientos de seguridad**

El dominio de evaluación son los sitios Web orientados a niños; específicamente los productos a evaluar son aquellos sitios que cuyo contenidos están escritos en el idioma español y que solicitan datos a los niños. Para mostrar la característica de *Seguridad y política de privacidad* se tomaron en consideración 40 sitios Web y se analizaron 23 atributos directamente mensurables -bajo criterio binario.

---

[34] Ver [Nouwt, 2002] para leer en forma detallada un análisis de los alcance de la COOPA.

[35] Esta caracterización de niño rige solo para EEUU. En la Argentina se considera niños a los sujetos menores de 15 años
[Mars, 2005].

Para la búsqueda de URL's de sitios Web orientados a niños se utilizó los artefactos de búsquedas Google.com y Alltheweb.com con las expresiones de búsqueda para ambos artefactos "sitios web orientados a niños" y "niños".

El perfil de usuario es el visitante que manifiesta interés en usar el sitio para estudio o entretenimiento, y es un visitante que se define como niño [FTC, 1999], [FTC, 2000]. De la Guía tomamos en consideración la subcaracteristica *Notificación de privacidad (Privacy notice)*. Esta subcaracteristica dice que el operador debe poner un vínculo –link- para anunciar sus prácticas de información en la página principal -home page-; el aviso debe tener los contenidos legibles y no debe tener material confuso o no relacionado.

**Árbol de requerimiento de seguridad y política de privacidad para sitios Web orientados a niños.**

1. Notificación de privacidad (Privacy notice)

1.1. Colocación del vínculo del anuncio de privacidad (placement)
- *1.1.1. El anuncio de la política de privacidad está situado en la home page.*
- *1.1.2. Está situado en la página donde solicita información personal de los niños.*
- *1.1.3. El vínculo es claro y sobresaliente.*

1.2. Contenidos de las políticas de privacidad (content)
- *1.2.1. El idioma es el mismo del sitio Web.*
- *1.2.2. Las políticas de privacidad están resumidas (vista rápida).*
- *1.2.3. Las políticas de privacidad están claramente escritas y son entendibles.*
- *1.2.4. Está la información de los operadores (dirección, número de teléfono y correo electrónico).*
- *1.2.5. Está anunciado qué información solicitan a los niños*
- *1.2.6. Cómo la recepcionan la información de los niños.*
  - *1.2.6.1. Directamente de los niños.*
  - *1.2.6.2. Usa cookies.*
  - *1.2.6.3. Usa web bug.*
- *1.2.7. Está anunciado cómo usa la información el operador.*
  - *1.2.7.1. Para enviar propaganda comercial a los niños.*
  - *1.2.7.2. Para invitar a participar a los niños en concursos.*
  - *1.2.7.3 Para invitar a que el niño participe en salas de chat.*
  - *1.2.7.4. Para publicar los datos de los niños en tablas de anuncio.*
  - *1.2.7.5 Para organizar los perfiles de los usuarios.*

- *1.2.8. Está anunciado si el operador comparte la información con terceras partes.*
- *1.2.9. Está anunciado si los padres pueden intervenir para negar el acceso de información por terceras partes.*
- *1.2.10. Está anunciado si los padres pueden revisar la información entregado por los chicos.*
- *1.2.11. Está anunciado si los padres pueden solicitar borrar la información entregado por los chicos.*
- *1.2.12. El sitio informa si hace transacciones comerciales.*

**Evaluación de los sitios Web**

Consideramos que todos los atributos tiene el mismo nivel de relevancia; el criterio de evaluación que asumimos es el binario, esto es: disponible uno (1), no disponible cero

(0). Los valores considerados para los atributos se deben interpretar respectivamente como que satisface completamente el requerimiento de calidad (100%) o que no lo satisface en absoluto (0%).

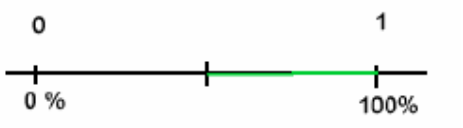



Figura Nº 1: Escala de preferencia

El registro de los atributos se hizo en forma manual. Se accedió a la *home page* de los sitios seleccionados, se verificó la existencia de declaración de privacidad; en los casos afirmativos se dio lectura exhaustiva para registrar la existencia o no de los atributos del árbol de requerimiento de calidad. Los valores de los atributos verificados se registraron en la tabla Nº 1.

**Análisis de los datos obtenidos**

De los sitios evaluados:

- ✓ 13 son argentinos -32%-; se constató que todos solicitan datos a los niños para participar en algún evento. Doce de estos sitios no poseen información acerca del modo que tratan y el destino de los datos obtenido de los niños.

- ✓ el 27.5% de lo sitios tienen políticas de privacidad. Todos tienen dominio en EEUU, menos del sitios S6, de origen argentino. Constatamos que:
  - A excepción del sitio S2, todos tienen el vínculo de política de privacidad en la Home page.
  - 5 sitios tienen el nombre del vínculo relacionado a la declaración de la política de privacidad, pero no son claro, ni sobresaliente.
  - Ningún sitio tienen las declaraciones de privacidad resumidas.
  - En general las declaraciones de políticas de privacidad no son fácilmente comprensibles, pero aceptamos que 4 sitios -10%- pasan el umbral aceptado.
  - El atributo 1.2.4 lo cumple el sitio S3. La apariencia es que diluye la responsabilidad por parte de las empresas porque los tutores deben tratar con operadores anónimos.
  - El atributo 1.2.5 relacionado a la información solicitada a los niños lo cumplen 5 sitios -12.5%.
  - En los atributos 1.2.6 relacionados a la forma que recepcionan la información de los niños encontramos: directamente a los niños 5 sitios -12.5%; a través de cookies, 5 sitios -12,5%; a través de web bug 2 sitios -5.0%.
  - En los atributos 1.2.7 relacionados a cómo usa la información el operador, encontramos que el mayor porcentaje lo llevan los atributos "1.2.7.1 Enviar propaganda comercial a los niños" y "1.2.7.5 Para organizar los perfiles de los usuarios" con el 12.5%; le sigue el atributo "1.2.7.2 Para invitar a participar a los niños en concursos", 10.0 %.
  - El atributo 1.2.8 relacionado a compartir la información con terceras partes lo cumplen 6 sitios -15.0%. Es un porcentaje alto, lo que está diciendo que hay una práctica entre sitios de un mismo conglomerado de empresas de compartir los datos solicitados a los niños –ver la tabla Nº 2 donde figuran los nombres de los sitios.

- El atributo 1.2.9 relacionado a la intervención de los padres en negar el acceso a los datos por terceras partes lo cumplen 6 sitios -15.0%.
- El atributo 1.2.10 relacionado a la intervención de los padres para revisar la información entregada por los chicos lo cumplen sólo 4 sitios -10.0%.
- 5 sitios cumplen los atributos 1.2.11 y 1.2.12 -12.5%- relacionado, el primero, con la posibilidad de los padres de solicitar borrar la información entregada por los chicos y, el segundo, si los sitios informan si hacen transacciones comerciales.

**Conclusión**

De los sitios argentinos evaluados, uno tiene declaración acerca de cómo administran los datos obtenidos a los niños. Como consecuencia se muestra por un lado, el desamparo de los niños que frecuentan los sitios argentinos y, por otro, la necesidad de orientar a los operadores de sitios Web para que informen qué herramientas usan para la recogida de datos, qué propósito tiene el almacenamiento de los datos y qué destino le dan a los mismos. Además los sitios deberían contener las tecnologías necesarias para asegurar que se cumplan los atributos 1.2.9, 12.10 y 1.2.11 relacionado a la interacción de los operadores con los tutores.

Por último, en la declaración debería figurar la adhesión a la Ley 25.326 "Protección de los datos personales" conocida como Habeas Data [Habeas, 2000] para que los padres pueden recurrir a dicha Ley para controlar los datos que sus niños entregan a los sitios Web puesto que, siguiendo a [Castro, 2002], "… el *Habeas Data* es un recurso procesal para defender el derecho a la intimidad como un instrumento del individuo de control y disposición de sus datos personales".

Tabla Nº 1: Registro de los valores de los atributos para la subcaracteristica de Notificación de privacidad (Privacy notice). Fecha de recolección 05/06/06

| | 1. Notificación de privacidad (Privacy notice) | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Códi. | 1.1.1 | 1.1.2 | 1.1.3 | 1.2.1 | 1.2.2 | 1.2.3 | 1.2.4 | 1.2.5 | 1.2.6 | | | 1.2.7 | | | | | 1.2.8 | 1.2.9 | 1.2.10 | 1.2.11 | 1.2.12 |
| | | | | | | | | | 1 | 2 | 3 | 1 | 2 | 3 | 4 | 5 | | | | | |
| S1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 |
| S2 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| S3 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| S4 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S5 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S6 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 |
| S7 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S8 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S9 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S10 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| S11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S13 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S14 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S15 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S16 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S17 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S18 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S19 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S20 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S21 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S22 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S23 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S24 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S25 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S26 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S27 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S28 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S29 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S30 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S31 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S32 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| S33 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S34 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S35 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S36 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S37 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S38 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S39 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| S40 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Total | 11 | 1 | 5 | 11 | 0 | 4 | 1 | 5 | 5 | 5 | 2 | 5 | 4 | 1 | 1 | 5 | 6 | 6 | 4 | 5 | 5 |
| % | 27.5 | 2.5 | 12.5 | 27.5 | 0 | 10.0 | 2.5 | 12.5 | 12.5 | 12.5 | 5.0 | 12.5 | 10.0 | 2.5 | 2.5 | 12.5 | 15.0 | 15.0 | 10.0 | 12.5 | 12.5 |

Tabla Nº 2: Sitios Web orientados a niños evaluados

| Códigos | Nombre | URL | Dominio |
|---|---|---|---|
| S1 | Barbie | http://es.barbie.com/ | EEUU |
| S2 | Disney | http://www.disneylatino.com/index-flash.html | EEUU |
| S3 | Space Place (NASA) | http://spaceplace.jpl.nasa.gov/sp/kids/ | EEUU |
| S4 | Chicomanía | http://www.chicomania.com/ | EEUU |
| S5 | miniSSan | http://www.minissan.com.mx/ | México |
| S6 | Micaela, una película mágica | http://www.micaela.terra.com.ar/ | Argentina |
| S7 | ABCchicos | http://abchicos.com.ar/abchicos/ | Argentina |
| S8 | El mundo de Manu | http://www.elmundodemanu.com.ar/ | Argentina |
| S9 | Chicos.net | http://chicos.net.ar/ | Argentina |
| S10 | Juguetes Imaginarium | http://www.imaginarium.es/vIE/index.asp | España |
| S11 | Juegos | http://www.pequenomundo.com.mx/juegos.htm | México |
| S12 | Historias, juegos | http://www.abctooncenter.com/spjourn.htm | EEUU |
| S13 | GlibalPCnet – Sitio | http://www.globalpc.net/entretenimiento/juegos/default.asp | |

| | | | |
|---|---|---|---|
| | infantil | | |
| S14 | Página de juegos de ingenio | http://www.geocities.com/Eureka/Promenade/5577/ | EEUU |
| S15 | Billiken on line | http://www.billiken.com.ar/ | Argentina |
| S16 | Sesamo | http://www.sesamo.com/mensajes/index.html | EEUU |
| S17 | Hola chicos | http://www.holachicos.com/globos.html | México |
| S18 | miniClub | http://www.miniclub.com/privacidad.asp | EEUU |
| S19 | Chiquititas | http://www.chiquititas.com.ar/ | Argentina |
| S20 | Chicos.net | http://chicos.net.ar/ | Argentina |
| S21 | México para niños | http://www.elbalero.gob.mx/index_esp.html | México |
| S22 | Andalucía para niños | http://www.terra.es/personal2/pfigares/ | España |
| S23 | Cuentos y poesía para niños | http://personal1.iddeo.es/bernal/marisa/ | España |
| S24 | Sección de Egipto para niños | http://www.egiptologia.com/ninyos/ | EEUU |
| S25 | Chile para niños | http://www.chileparaninos.cl/ | Chile |
| S26 | Mitología para niños | http://www.elhuevodechocolate.com/mitologia1.htm | EEUU |
| S27 | StoryPlace: La biblioteca digital de los niños | http://www.storyplace.org/sp/storyplace.asp | |
| S28 | Mundo latino | http://www.mundolatino.org/rinconcito/ | |
| S29 | Filosofía para niños | http://www.izar.net/fpn-argentina/ | |
| S30 | Derechos de los niños | http://www.margen.org/ninos/ | |
| S31 | Astronomía para niños | http://www.alucine.com/ninos.htm | EEUU |

| | | | |
|---|---|---|---|
| S32 | Yahoo en español para niños | http://espanol.paraninos.yahoo.com/ | EEUU |
| S33 | Museo de los niños Abasto | http://www.museoabasto.org.ar/home.php | Argentina |
| S34 | Revista baber.com Literatura infantil y juvenil | http://revistababar.com/web/index.php?option=com_frontpage&Itemid=1 | EEUU |
| S35 | Migacon.com.ar | http://www.migacon.com.ar/ | Argentina |
| S36 | Leemeuncuento | http://www.leemeuncuento.com.ar/index.html | Argentina |
| S37 | Edenorchicos | http://www.edenorchicos.com.ar/edenorchicosweb/paginas/juegos.html | Argentina |
| S38 | Portal del fútbol infantil | http://www.fulbi.com/ | EEUU |
| S39 | Republica de los niños | http://www.republica.laplata.gov.ar/espectaculos/inicio.htm | Argentina |
| S40 | Cuentos locos y graciosos del profesor Serapio | http://www.netic.com.ar/cuentinf/ | Argentina |

**Referencias:**


[Abad, 2001] Abad, L., 2001, "La lucha por la intimidad en Internet". En: http://www.ucm.es/info/cyberlaw/actual/9/leg04-09-01.htm

[Aguirre, 2006] Aguirre, G., 2006, "La Protección de la Privacidad en la República Argentina". En: http://www.dpi.bioetica.org/aguirre.htm

[Ang, 2001] Ang, P.H., "The rol of self-regulation of privacy and the Internet". En: http://www.jiad.org/vol1/no2/ang/ang.pdf

[Bugnosis, 2003] Bugnosis, 2003, "Web bug FAQ". En: http://www.bugnosis.org/faq.html

[Castro, 2002] Castro Bonilla, A., 2002, "La protección a la intimidad en el tratamiento de datos personales: en el caso de España y la nueva legislación latinoamericana". En: http://www.alfa-redi.com//apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/castro.pdf

[Chung, 2002] Chung W. y Paynter J., 2002, "Privacy Issues on the Internet". En: http://csdl2.computer.org/comp/proceedings/hicss/2002/1435/07/14350193b.pdf .

[Comer, 1998] Comer, D.E., 1998, "El libro de Internet", 2da. Edición, Prentice Hall, México.

[Constitución, 1994] Constitución Argentina, 1994, "Constitución de la Nación Argentina, 22 de agosto de 1994". En: http://www.pjn.gov.ar/cne/download/constitucion_nacional.pdf

[Cookies, 1999] "Qué son los cookies". En: http://www.iec.csic.es/criptonomicon/cookies/queson.html

[Correia, 2004] Correia, F, Silva, S., 2004, "P3P: Platform for Privacy Preferences Desenvolvida pelo Consórcio", Universidade do Minho. En: http://papadocs.dsi.uminho.pt:8080/retrieve/69/Apresentacao_P3P.pdf

[Coyle, 1999] Coyle, 1999, "P3P: Pretty poor privacy? A social analysis of the Platform for Privacy Preferences (P3P)". En: http://www.kcoyle.net/p3p.html

[Cranor, 1999] Cranor, 1999, "Agents of choice: tools that facilitate Notice and choice about web site data practices". En: http://lorrie.cranor.org/pubs/hk.pdf

[Cranor, 2002] Cranor L.F., 2002, "The role of privacy advocates and data protection authorities in the design and deployment of the platform for privacy preferences". En http://lorrie.cranor.org/pubs/p3p-cfp2002.html

[Demner, 2001] Demner, D., 2001, "Children on the Internet", En http://www.otal.umd.edu/UUPractice/children/ .

[Desantes, 1991] Desantes, J.M., 1991, "El derecho fundamental a la intimidad". En: http://www.cepchile.cl/dms/archivo_1212_1280/rev46_desantes.pdf

[El-Khatib, 2003] El-Khatib, K, Korba, L., Xu, Y., y Yee, G. 2003, "Privacy and Security in e-leraning". En: https://iit-iti.nrc-cnrc.gc.ca/iit-publications-iti/docs/NRC-45786.pdf

[Electronic, 2000] Electronic Privacy Information Center, 2000, "Pretty Poor Privacy: An assessment of P3P and Internet Privacy. En: http://www.epic.org/reports/prettypoorprivacy.html

[FCR, 2003] Fundació Catalana per a la Recerca European Schoolnet, 2003, "Los hábitos de los niñ@s en internet: estudio europeo". En: http://www.internetsegura.net/web2003ESP/default.asp

[Fernández, 2003] Fernández, G. J., 2003, "Métodos efectivos contra el correo basura". En: http://www.acens.com/descargas/metodos.pdf

[Foix, 2002] Foix, C, Zavando, S, 2002, "Estándares e-learning: Estado del Arte". En: http://empresas.sence.cl/documentos/elearning/INTEC%20-%20Estandares%20e-learning.pdf

[Frauenhofer, 2004] Frauenhofer, W.A., 2004, "Privacy and technology: definition and policy", Center for Education and Research in Information Assurance and Security, Pardue University. En: https://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2004-33.pdf

[FTC, 1998] Federal Trade Commission, 1998, "Privacy online: a report to congress". En: http://www.ftc.gov/reports/privacy3/priv-23a.pdf

[FTC, 1998] Federal Trade Commission, 1998, "Facts for Consumers". En: http://www.ftc.gov/bcp/conline/pubs/online/sitesee.htm#FILTER

[FTC, 1999] Federal Trade Commision, 1999; "Federal register: Part III: Children's Online Protection Rule; Final Rule". En: http://www.cdt.org/legislation/105th/privacy/64fr59888.pdf

[FTC, 2000] Federal Trade Commision, 2002; "How to Comply Whith the Children's Online Privacy Protection Rule". En: http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.pdf .

[Garfinkel, 2000] Garfinkel, S., 2000, "Can a labeling system protect your privacy? Salon.com Technology, En: http://archive.salon.com/tech/col/garf/2000/07/11/p3p/print.html

[Garfinkel, 2002] Garfinkel, S y Cranor L.F., 2002, "P3P: Privacy primer". En: http://www.oreillynet.com/lpt/a/1554

[Gregorio, 2003] Gregorio, C.G., Greco, S. y Balosian, J., "Impacto de la nuevas tecnologías de comunicación e información sobre los derechos de intimidad y privacidad". En: http://www.flacso.org.ec/docs/sfintgregorio.pdf

[Habeas, 2000] "Protección de los datos personales: Ley 25.326". En: http://www.anticorrupcion.jus.gov.ar/ley25326.pdf

[Hernando, 2005] Hernando, S, 2005, "Definición de phishing". En: http://www.sahw.com/wp/archivos/2005/04/26/definicion_de_phishing/

[IBM, 2000] IBM, 2000, "P3P Policy Editor". En: http://www.alphaworks.ibm.com/tech/p3peditor

[IEEE, 2001] IEEE LTSC LTSA, 2001, "Learning Technology Systems Architecture. En: http://ltsc.ieee.org/wg1/index.html

[iCAUCE.Ar, 2006] iCAUCE.Ar, 2006, "Derecho a la privacidad". En: http://www.cuace.org.ar

[ICRA, 2005] ICRA, 2005, "About ICRA". En: http://www.icra.org/

[IRAM, 2006] IRAM, 2006, "Qué es la certificación". En: http://www.iram.org.ar/

[IS, 2005] Internet Segura, 2005, "Posibles riesgos de Internet". En: http://www.internetsegura.net/web2003ESP/riscs.asp

[Leon, 2001] Leon Leon C., 2001**, "**Consideraciones legales relativas al envío de e-mails comerciales no solicitados". En: http://www.alfa-redi.org/rdi-articulo.shtml?x=730

[Lessing, 1999] Lessing, L., 1999, "La arquitectura de la privacidad". En: http://www.uned.es/ntedu/espanol/master/segundo/modulos/valores-y-etica/arquipri.htm

[Libertus, 1998] Libertus, 1998, "Will PICS torch free Speech on the Internet?" En: http://libertus.net/liberty/picscamla.html

[Lipskier, 2004] Lipskier, N.C., Olivera N.L. y Proto A.N., 2004, "Incidencia de los factores electrónicos en la contratación. El caso de las PYMES argentinas en el MERCOSUR", En: http://www.itba.edu.ar/capis/jis/jis-1-1/incidencia-de-los-factors-electr%F3nicos.pdf

[Mars, 2005] Mars.com, 2005. En : http://www.mars.com/privacy/np_spanish.html

[Mayer, 2000] Mayer-Schonberger, V., 2000, "The cookies concept", Cookiescentral.com. En: http://www.cookiecentral.com/c_concept.htm

[MD, 2005] MarketingDirecto.com, 2005, "TRUSTe inaugura el sello "We don't spam"". En: http://www.marketingdirecto.com/noticias/noticia.php?idnoticia=15920

[Nielsen, 2002] Nielsen, J., 2002, "Kids' Corner: Website Usability for Children". En: http://www.useit.com/alertbox/20020414.html

[Nouwt, 2002] Nouwt, S., 2002, "Kids' privacy on the Internet: collecting children's personal data on the Internet and the protection of privacy". En: http://arno.uvt.nl/show.cgi?fid=5344

[Olsina, 2000] Olsina, L., 2000, "Metodología cuantitativa para la evaluación y comparación de calidad de sitios Web". Tesis doctoral defendida en abril del 2000, Facultad de Ciencias Exactas, UNLP, La Plata. En: http://di002.edv.uniovi.es/~cueva/investigacion/tesis/WebsiteQEM.pdf

[Palazzi, 2004] Palazzi, A., 2004, "Aspectos legales del correo electrónico no solicitado". En: http://wiki.cauce.org.ar/spam-palazzi-icauce-argentina.pdf

[P3P, 1998] P3P 1988, "P3P Guiding Principles: W3C NOTE 21-July-1998". En: http://www.w3.org/TR/NOTE-P3P10-principles

[P3PToolbox, 2005] P3PToolbox, 2005, "The P3P Implementation Guide", Internet Education Foundation, En: http://p3ptoolbox.org/

[Photoshop, 2006] Photoshop, 2006, "Ayuda". En: http://www.mor.itesm.mx/~lssalced/Photo/Ayuda/help.html

[Portilla, 2005] Portilla Comezaña, O. y García Peñalvo, F.G., 2005, "Plataformas para educación basada en web: Herramientas, procesos de evaluación y seguridad. En: http://tejo.usal.es/inftec/2005/DPTOIA-IT-2005-001.pdf.

[PrivacyFinder, 2006] PrivacyFinder, 2006, "PrivacyFinder: FAQ". En: http://search.privacybird.com/

[RedIris, 2003] Rediris, 2003, "Plataforma Unificada AntiSpam de RedIRIS (PUAS)". En: http://www.rediris.es/

[Rizzi, 2005] Rizzi, A., 2005, "Los estafadores pescan en la Red", El País, en: http://www.elpais.es/articulo/reportajes/estafadores/pescan/Red/elpdomrpj/20050814elpdmgrep_1/Tes/

[Safesurf, 2006] Safesurf, 2006, "The SafeSurf Internet Rating Standard". En: http://www.safesurf.com/ssplan.htm

[Smith, 1999] Smith, R.M., 1999, "The Web Bug FAQ", Electronic Frontier Foundantion, En: http://www.eff.org/Privacy/Marketing/web_bug.html

[TRUSTe, 2006] TRUSTe, 2006, "Make Privacy Your Choice". En: http://www.truste.org/

[Turow, 2001] Turow, J., 2001, "Do They Play By the Rules?" En: http://www.annenbergpublicpolicycenter.org/04_info_society/family/2001_privacyreport.pdf

[Valesani, 2003] Valesani, M.E., Mariño, S.I. y La Red Martínez, D.L., "La Protección de los datos personales en los sistemas informáticos. La instrumentación en la Argentina". En: http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/hd_version3.PDF

[Villate, 1998] Villate, J., 1998, "La libertad de expresión en Internet: retos y amenazas". En: http://www.une.edu.ve/~iramirez/te1/censura_internet.html

[W3C, 1997] W3C, 1997, "Extensible Markup Languaje (XML). En: http://www.w3.org/TR/PR-xml-971208

[W3C, 1998] W3C, 1998, "The Platform for Privacy Preferences: P3P Note 06-November-1998", En: http://www.w3.org/TR/1998/NOTE-P3P-CACM-19981106/#intro

[W3C, 1999] W3C, 1999, "El W3C de la A a la Z". En: http://www.w3c.es/divulgacion/a-z/

[W3C, 1999] W3C, 1999, "Resource Description Framework (RDF). Especificación del Modelo y la Sintaxis. Recomendación del W3C 22 febrero 1999 (español). En: http://www.w3.org/TR/1999/REC-rdf-syntax-19990222

[W3C, 2005] W3C, 2005, "The Platform for Privacy Preferences 1.1 (P3P1.1) Specification. W3C Working Draft 1 July 2005", En: http://www.w3.org/TR/2005/WD-P3P11-20050701/

[Waterhouse, 2004] Waterhouse S., Rodney O.R., 2004, "The importance of policies in e-learning instruction". En: http://www.educause.edu/ir/library/pdf/eqm0433.pdf

[Wikipedia, 2006] Wikipedia, 2006, "Phishing". En:

http://es.wikipedia.org/wiki/Phishing#Anti-Phishing

[Williams, 1998] Williams, J.R., 1998, "Can a "Social" Protocol Help Protect Web Privacy?", Georgetown University Law Center, Information Privacy Seminar Professor Rotenberg. En: http://scholar.google.com/scholar?hl=en&lr=&q=cache:MSWIoXFkMNsJ:www.aspectsecurity.com/documents/p3p.pdf+link:SKZvbRqlbJsJ:scholar.google.com/

[Wordsmyth, 2006] Wordsmyth, 2006, "Wordsmyth: dictionary-Thesaurus". En: http://www.wordsmyth.net/

[Yahoo, 2005] Yahoo en español para niños, 2005. En: http://espanol.paraninos.yahoo.com/

.

.

[Yang, 2002] Yang, Ch, Lin, F.O. y Lin, H., 2002, "Policy-based privacy and security management for collaborative e-education system". En: http://iit-iti.nrc-cnrc.gc.ca/iit-publications-iti/docs/NRC-44906.pdf.

[Yee, 2003] Yee, G., Korba, L., 2003, "Feature interaction in policy-driven privacy management". En: http://iit-iti.nrc-cnrc.gc.ca/iit-publications-iti/docs/NRC-45785.pdf