

Aportes de ISOC Argentina para una mejor Internet

“Seguridad en Internet: un recorrido por los aspectos claves”



ISOC.Ar
Capitulo
Argentina

Oradores:

Dr. Pedro Less Andrade - Dra. Mónica Abalo Laforgia - Dr. Ariel Manoff

International Internet Technologies
NH City Hotel
Buenos Aires - 18 y 19 de Abril de 2007



SEGURIDAD EN INTERNET

“Un recorrido por los aspectos clave”



ISOC.Ar
Capítulo
Argentina

AGENDA

- ➔ *Aspectos de la Seguridad en Internet*
- ➔ *La Protección de Datos y de la Propiedad Intelectual en la Sociedad de la Información*
- ➔ *Conclusiones y Propuestas de ISOC.Ar*
- ➔ *Preguntas*



SEGURIDAD EN INTERNET

“Un recorrido por los aspectos clave”

AGENDA



Aspectos de la Seguridad en Internet

- ✓ *Qué es la Seguridad*
- ✓ *Definición e identificación de Vulnerabilidades y Amenazas*
- ✓ *Concepto y Características del Delito Informático*
- ✓ *Clases y Evolución*
- ✓ *El Proyecto de Ley. Criterios de regulación*

QUÉ ES LA SEGURIDAD



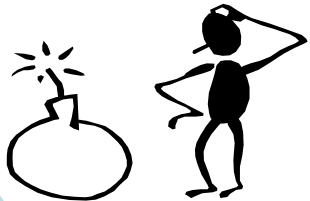
Preocupa a individuos y organizaciones

Concepto relativo

Clases



SEGURIDAD DE ACCESO



SEGURIDAD REACTIVA



INFRAESTRUCTURA + DATOS

=

SEGURIDAD

Mitos

- Software Infalible
- Escenarios simples y pocos
- Robo de información sólo a nivel de red
- Asegurar el "end-point" resuelve el problema
- Comportamiento del usuario es seguro

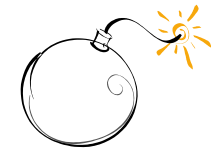
PRINCIPIOS GENERALES DE SEGURIDAD

 *Ponderación del Riesgo*



AMENAZAS

Vs.



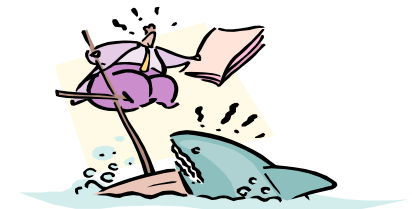
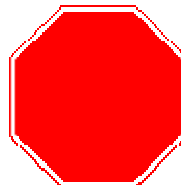
VULNERABILIDADES

 *Políticas de seguridad "customizadas"*

 *Condiciones de Éxito*

- (i) Utilidad
- (ii) Coherencia
- (iii) Practicable
- (iv) Adecuada culturalmente

 *Obligaciones del responsable*





SEGURIDAD: PROBLEMAS Y SOLUCIONES

Problemas

Fuga de Datos



Fraudes y Daños Informáticos



SEGURIDAD COMO PROYECTO



Concepto

Conductas Antijurídicas

Realizadas mediante el uso de recursos informáticos o telemáticos

Dirigidas contra recursos, medios o sistemas informáticos o telemáticos



- Derecho Penal no permite analogía
- ¿Necesidad de Tipos Específicos?
- Prudencia en la redacción
- Evitar interferencias de Mercado

Descripción Delitos

- Contra la Integridad Sexual
 - Pornografía Infantil
 - Acoso Sexual
- Contra el Honor
 - Injurias / Derecho a la Imagen
 - Inserción Datos Personales Falsos
- Contra la Privacidad
 - Intercepción Comunicaciones
 - Acceso a Bases de Datos
 - Escuchas / Intercepción
 - SPAM
- Contra la Propiedad
 - Hurto/Robo de Información
 - Estafas y Defraudaciones
 - Daños a Sistemas de Información
- Contra las Comunicaciones
 - Entorpecimiento / Interrupción
- Violación de Documentos
 - Falsificación Documento Electrónico
 - Falsificación Firma Digital
 - Alteración Pruebas



Pérdida de Información por distintos medios (Internet, intranet, dispositivos externos)



Hackers: adolescentes con conocimientos informáticos. Sin intereses económicos



Crackers: anonimato limitado. Intereses económicos



Phishing: redes de crimen organizado.

Vishing:



- E-mail con número de teléfono
- Llamado que emula la central telefónica del banco

Pharming:

- Manipulación de DNS del PC para desviar a páginas falsas
- Se utilizan gusanos y troyanos

Scam:

- Ofrecimiento vía e-mail de trabajo desde el hogar
- Se utiliza para blanquear dinero

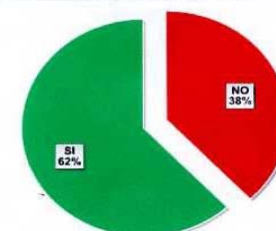
ALGO DE ESTADÍSTICAS ...

Un 44% de las páginas web bancarias españolas favorecen el phishing

Seguridad básica en sistemas de autenticación de los servicios de banca electrónica

	dirección URL	https en página de login	Validez del certificado	Visualización de url	Calificación
Bancaja	http://www.bancaja.es/	no		si	incorrecto
Banco Atlántico	http://www.batlantico.es/	no		si	incorrecto
Banco Cetelem	http://www.bancocetelem.es	si	si	si	correcto
Banco de Valencia	www.bancadevalencia.es	si	si	si	correcto
Banco Finantia Sofintoc	http://www.bancoesfinge.es/	no		no	incorrecto
Banco Gallego	www.bancogallego.es	si	si	si	correcto
Banco Guipuzcoano	http://www.bancogui.es/	si	si	si	correcto
Banco Herrero	http://www.bancoherrero.es	no		si	incorrecto
Banco Pastor	http://www.bancopastor.es/	si	si	no	incorrecto
Banco Popular	http://www.bancopopular.es/	si	si	si	correcto
Banco Sabadell Atlantico	www.sabadellatlantico.com/	no	si	si	incorrecto
Banco Urquijo	http://www.bancourquijo.es/	si	si	si	correcto
Banco Zaragozano	www.bancozaragozano.es/	si	si	si	correcto
Banesto	www.banesto.es	si	si	si	correcto
Bankinter	http://www.bankinter.com/	no		si	incorrecto
Bankoa	www.bankoa.es	si	si	si	correcto
Bankpyme	http://www.bankpyme.es/	no		si	incorrecto
BankpymeNet	www.bankpymenet.com	si	si	si	correcto
Barclays	http://www.barclays.es/	si	si	si	correcto
BBK	www.bbk.es	si	si	si	correcto
BBVA	http://www.bbvanet.com	si	si	si	correcto
BSCH	www.santandercentralhispano.es	no		si	incorrecto
Caixa Catalunya	http://www.caixacatalunya.es	no		si	incorrecto
Caixa Galicia	http://www.caixagalicia.es	si	si	si	correcto
Caixa Sabadell	http://www.caixasabadell.es	si	si	si	correcto
Caja Duero	http://www.cajaduero.es	no		no	incorrecto
Caja España	http://www.cajaespana.es	si	si	si	correcto
Caja Inmaculada (CAI)	http://www.cai.es/	no		si	incorrecto
CAI Online	http://caionline.cai.es	si	si	si	correcto
Caja Laboral	http://www.cajalaboral.es/	si	si	si	correcto
Caja Madrid	http://www.cajamadrid.es	si	si	si	correcto
Caja Rioja	http://www.cajarioja.es/	no		si	incorrecto
Caja Rural Vasca	www.cajaruralvasca.es	si	si	si	correcto
Caja Vital	www.cajavital.es	no		si	incorrecto
Cajamar	www.cajamar.es	si	si	si	correcto
Citybank	http://www.citybank.es	si	si	si	correcto
Deutsche Bank	www.deutsche-bank.es	no		si	incorrecto
Hispaner	http://www.hispamer.es/	si	si	si	correcto
ibanesto.com	http://www.ibanesto.com/	si	si	no	incorrecto
Ibercaja	www.ibercaja.es	si	si	si	correcto
ING direct	http://www.ingdirect.es	si	si	si	incorrecto
Inversis	http://www.inversis.es	no		si	incorrecto
Kutxa	www.kutxa.es	si	si	no	incorrecto
La Caixa	http://www.lacaixa.es	no		si	incorrecto
La Caja de Canarias	http://www.lacajadecanarias.es/	no		si	incorrecto
Lloyds TSB Bank	http://www.lloydsbank.es/	si	si	si	correcto
Patagon	http://www.patagon.es	si	si	si	correcto
RuralVia	http://www.ruralvia.com/	no		si	incorrecto
unicaja	http://www.unicaja.es	si	si	si	correcto
Uno-e	https://www.uno-e.com	si	si	si	correcto
Total		19		5	22

HTTPS en página de login



Diseño de los sistemas de autenticación en banca online española



Fuente: Hispasec Sistemas-Parque tecnológico de Andalucía -

Estudio sobre debilidades de diseño en páginas web de bancos on-line que favorecen ataques de phishing 16/11/04

SPAM - CONCEPTOS GENERALES

DEFINICIÓN

- ➔ "Spam": correo electrónico no solicitado (Junk mail)
- ➔ "Spamming": acción de enviar mensajes de correo electrónico a varias personas con fines primariamente publicitarios



ORIGEN

- ➔ Año 1999
- ➔ Abogados especialistas en migraciones Canter & Siegel
- ➔ Ofrecimiento de servicios

Consecuencias

- Fue juzgado como una acción negativa por la sociedad
- Cancelación del servicio Internet
- Desafiliación como "*barristers*" en el Estado de Arizona
- Ganancias por la publicación del libro

CLASES

- ➔ Como medio válido y lícito de marketing
- ➔ Como medio fraudulento y engañoso (SPAM)

SIST. ARGENTINO

- ➔ Bases de Datos en general: Principio "OPT-IN"
- ➔ Bases de Datos de Marketing: Principio "OPT-OUT"

CARACTERISTICAS

- Multiplicidad de destinatarios
- No fue solicitado previamente
- Utilizan Internet como medio de envío
- El envío se hace desde direcciones no válidas
- Contiene generalmente títulos engañosos
- Genera costos
- Medios de obtención de la direcciones (bases de datos ilegales, robots que "scannean" paginas web, etc)

QUIÉN LOS ASUME?

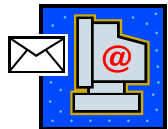
DESDE EL ISP

- ➔ Costos operativos en RR.HH y tecnológicos:
 - atención de reclamos
 - saturación de redes y servidores
 - filtrado de mails

DESDE EL USUARIO

- ➔ Tiempo de lectura
- ➔ Tiempo de conexión
- ➔ Realizar quejas
- ➔ Solicitud infructuosa de OPT-OUT

SOLUCIONES ?




TÉCNICAS Y FÍSICAS (listas blancas y listas negras)



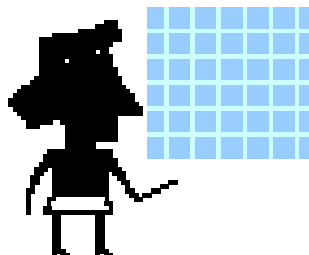
JURIDICAS

 Regulación

 Auto -regulación

OTRA VEZ ALGUNOS NÚMEROS ...

El Spam sigue creciendo inmune a cualquier medida en su contra



Año	2006	2005 ... 2003	2002
Período	1° Q	4° Q ... Julio	Diciembre
	62%	57% ... 50%	40%



Variaciones

2005-2006 → 5%

2003-2006 → 12%

Temáticas del Spam

42% sexo y pornografía

- ✓ Hipotecas y Préstamos
- ✓ Medicamentos
- ✓ Software pirata
- ✓ Lotería y Juegos

PROYECTOS DE LEY

Áreas que Regulan

Inclusión de nuevos tipos penales o adaptación de los existentes a los nuevos medios informáticos

Medidas tendientes a combatir los delitos informáticos o evitar su comisión

- Balance entre la protección de los usuarios y una Internet libre y abierta
- Medida al imponer obligaciones a los ISPs y otros operadores
- Desde el 2000 hay más de 30 proyectos presentados
- Leyes 23.741, 25.326 y 25.506 ya modificaron el Código Penal

ALGUNOS PROYECTOS PRESENTADOS

→ Jenefes (Exp. 520/07)

- Regula: Daño Informático
- Presentado: Al Senado el 27/03/2007
- Estado: Tratamiento en Comisiones

→ Bortolozzi (Exp. 4417/06)

- Regula: Privacidad comunicaciones electrónicas, pornografía infantil, escuchas e interceptación de comunicaciones, acceso y daño a sistemas de Información.
- Presentado: Al Senado el 05/12/2006
- Estado: Tratamiento en Comisiones

→ Nemirovski y otros (Exp. 5864-D-2006)

- Regula: pornografía infantil, privacidad comunicaciones electrónicas, secreto, escuchas e interceptación de comunicaciones, acceso, daño a sistemas de Información, fraude y alteración de pruebas.
- Presentado: A Diputados el 04/10/2006
- Estado: media sanción en Diputados, tratamiento en comisiones en el Senado

→ Lovaglio y otros (Exp. 5484-D-2006)

- Regula: Acceso, Fraude, Pornografía, Daño Informático
- Presentado: A Diputados el 05/09/2006
- Estado: Tratamiento en comisiones en Diputados



SEGURIDAD EN INTERNET

“Un recorrido por los aspectos clave”

AGENDA



La Protección de Datos y de la Propiedad Intelectual en la Sociedad de la Información

- ✓ *Concepto y Características*
- ✓ *Aspectos relevantes de la Ley 25.326*
- ✓ *Situación Argentina y resto del Mundo*
- ✓ *El Servicio WHOIS: concepto, posturas y criterios. El Debate*
- ✓ *La Protección de la Propiedad Intelectual en Internet*

CONCEPTO Y CARACTERÍSTICAS



Dato = Información



Sociedad

Flujo de información entre sus integrantes que se realiza en tiempo real

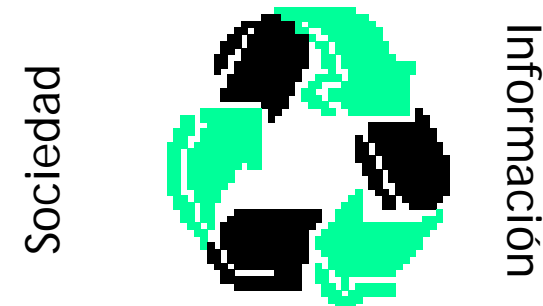
Dato Personal

Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables (Art. 2 - Ley 25.326)



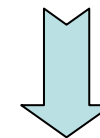
- ✓ Información
- ✓ Asociación en forma directa o indirecta a una persona física
- ✓ DATO PERSONAL

Dato Personal



Flujo

.....
Dato Personal



**AUTODETERMINACION
INFORMATIVA**

Derecho a la Intimidad se relaciona con:



Autodeterminación
Informativa



Anonimato

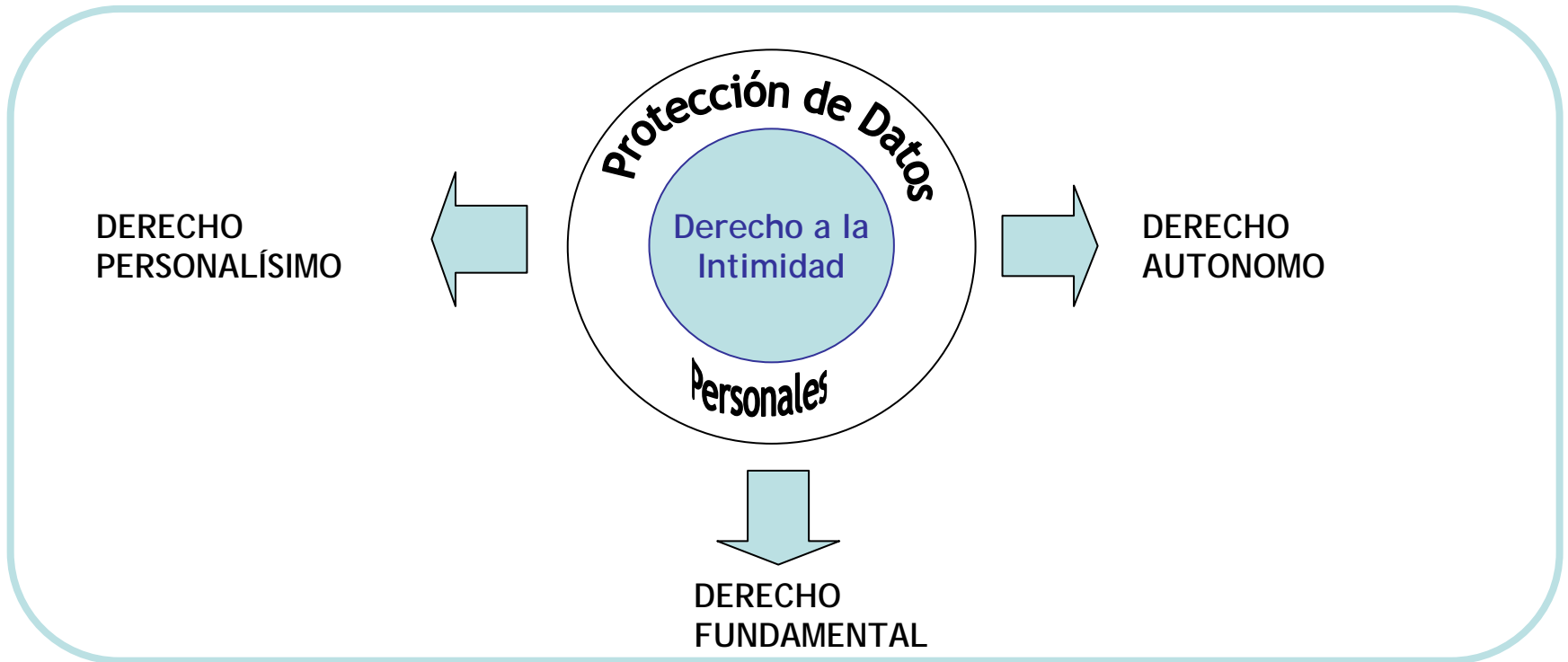


Posibilidad de controlar la información referida así misma que una determinada persona quiere compartir con los otros

Artículo 19 C.N.

“ Las acciones privadas de los hombres que de ningún modo ofendan al orden y la moral pública ni perjudiquen a un tercero, están reservadas a Dios y exenta de la autoridad de los magistrados ...”

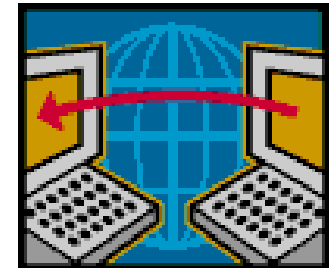
DERECHO A LA INTIMIDAD VS. PROTECCIÓN DE DATOS



Derecho a ser dejado a solas






Defensa de la intimidad en la S.I



LA DIRECCIÓN IP COMO DATO PERSONAL

ELEMENTOS DEL "DATO PERSONAL"

-  Referido a personas identificadas o **identificables**
-  Comprende información de **carácter numérico**
-  Tratamiento de datos



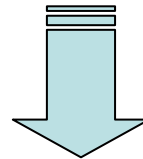
Dirección IP:
información numérica



Entidad tratante



Relacionarla con una
persona física



DATO PERSONAL

OBLIGACIONES

- ➔ REGISTRO del Banco de Datos (BD) como condición de licitud (Arts. 3, 21 y 24)
- ➔ ADECUACION del BD a la Ley (Art. 3)
- ➔ CALIDAD de los Datos Personales (Art. 4)
- ➔ CONSENTIMIENTO INFORMADO del titular de los datos (Arts. 5 y 6)
- ➔ SEGURIDAD de los datos (Art. 9)
- ➔ CONFIDENCIALIDAD de los datos (Art. 10)
- ➔ CESIÓN de datos personales (Art. 10)
- ➔ TRANSFERENCIA INTERNACIONAL (Art. 12)
- ➔ RESPETO Derechos Titulares (Arts. 13-16)



- ➔ La Ley plantea un nuevo marco de responsabilidad.
- ➔ La Ley crea la acción de protección de los datos personales
- ➔ La Ley crea nuevos tipos penales

DESCRIPCIÓN

- ➔ Registro Nacional de Bases de Datos
- ➔ Revisión de procesos, prácticas y Políticas
- ➔ Datos ciertos, adecuados, pertinentes, no excesivos, exactos y actuales
- ➔ Informar al titular sobre la finalidad de recolección y sus destinatarios
- ➔ Tomar medidas técnicas y organizativas para garantizar la seguridad y confidencialidad
- ➔ Secreto Profesional sobre los datos
- ➔ Requiere consentimiento del titular y es revocable
- ➔ Limitaciones para la transferencia internacional de datos personales
- ➔ Garantizar los derechos de información, acceso, rectificación, actualización o supresión

MARCO DE RESPONSABILIDAD

Organizaciones y Empresas

Deber de Adecuación
a la Ley

Responsabilidad
Patrimonial

por demandas
por sanciones
administrativas

Responsabilidad
en Cascada

Solidaria e ilimitada
entre quienes se
cedan o traten datos

Responsabilidad
Penal

Por inserción de datos falsos
Por datos Falsos
Por acceso ilegítimo a BD
Por violación confidencialidad



- ➔ Sanciones que van de multas de \$ 1000 a \$ 100.000
- ➔ Demandas patrimoniales de múltiples damnificados
- ➔ Penas de 1 mes a 4 años y medio de prisión

Órgano de Aplicación

<http://www.jus.gov.ar/dnppdpnew>



**Dirección Nacional de
Protección de Datos Personales**

CÓDIGOS DE CONDUCTA (Art. 30)

Asociaciones o Entidades Representativas

Elaborar Códigos de Conducta de Práctica Profesional

Establecer

Normas de Tratamiento de Datos

Asegurar y Mejorar

Condiciones de operación de sistemas de Información

Lograr un Balance

Entre la protección de los derechos de los titulares y los servicios prestados por los diferentes proveedores



Sujeto a la Aprobación de



**Dirección Nacional de
Protección de Datos Personales**

SITUACIÓN ARGENTINA Y RESTO DEL MUNDO

UNIÓN EUROPEA

- ➔ 1º Legislación Europea: "Convenio del Consejo de Europa de protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981"
- ➔ Directiva 95/46/CE
- ➔ Directiva 97/66/CE
- ➔ Directiva 2002/58/CE



LATINOAMERICA

- ➔ Leyes que regulan el tratamiento de datos personales: Chile y Paraguay
- ➔ Proyecto de Ley en discusión: Brasil

ESTADOS UNIDOS

- ➔ Sistema "SAFE HARBOUR"
- Basado en la protección referida al consumo de sectores determinados
- Órgano de Control: FTC

Argentina

- Sistema jurídico mixto (Consumo + Derecho Humano)
- Ley general con protecciones específicas
- Único país en Latinoamérica con adecuación internacional

EL SERVICIO WHOIS

Significado básico: Servicio de informar datos sobre un nombre de dominio

Polémica

- Qué datos se debe pedir al solicitante
- Qué datos se deben poner a disposición del público y como hacerlo

Ejemplos de los datos a que se refiere el WHOIS Service







- Nombre, dirección, e mail y teléfono del titular del dominio
- Nombre y datos de la entidad servidora de ese dominio (primario y secundario)
- Fecha de creación del dominio
- Fecha de expiración del dominio
- Contacto de facturación
- Contacto técnico
- Contacto Administrativo

Definición Técnica del Whois

Definición de WHOIS recomendada por el Consejo General sobre Nombres de Dominio de ICANN (al 12 de Abril de 2006)

El propósito del servicio de WHOIS es el de proveer suficiente información para contactar a la persona responsable de un nombre de dominio que pueda resolver o, que sea responsable de transmitir a quien pueda resolver, cuestiones relativas a la configuración de los archivos asociados a ese nombre de dominio en un servidor de dominios

Grupos de incumbencias o "Constituencies" en ICANN que opinan para esta definición

-  Grupo de usuarios comerciales y de negocios
-  Grupo de propiedad intelectual
-  Grupo de proveedores de servicios y conectividad
-  Grupo de titulares de registros de dominios
-  Grupo de registradores de dominios
-  Grupo de usuarios no comerciales

FUTURO DEL WHOIS I

Grupo de trabajo o Task Force para aconsejar a ICANN en la implementación del WHOIS Service.

Recomienda en Abril 2007 la creación del OPoC





Punto operacional de contacto (OPoC) (Operational Point of Contact)


- El OPoC debe asegurar contacto con el titular del nombre de dominio en un plazo breve
- El OPoC debe tener responsabilidades específicas en notificar comunicaciones, incluidas las de tipo legal a los titulares de dominios
- El sistema debe tener procedimientos claros, consistentes, puntuales y predecibles para obtener acceso a datos no publicados.

FUTURO DEL WHOIS II

Principales áreas a discutir en la propuesta OPoC

1. Qué datos serán publicados en el WHOIS de los Registros
2. Qué datos serán publicados por los registradores
3. Qué mecanismos se usarán para corregir datos incorrectos
4. Cómo será el mecanismo de transferencia de datos entre los registradores que pierden un nombre de dominio y el que lo gane.

-  Conflictos existentes en el mundo inmaterial (pero con grandes consecuencias materiales)
-  Interesados en Derechos de Propiedad Intelectual. Rango de grupo incumbente o Constituency en ICANN
-  Marcas versus Sistema de nombres de dominio (Domain Name System)
-  Derecho de Autor (Copyright), Patentes y Secretos versus Posibilidad exponencial de copiado y difusión anónima de obras de autor.

-  El único derecho claro que tiene el dueño de un derecho intelectual es la posibilidad de excluir a otros de su uso, reproducción y difusión

MARCAS (y nombres personales, comerciales, geográficos, científicos, etc)
Versus Nombres de Dominio (el choque de dos mundos)







Ejemplos de infracciones

- ➔ Piratería de nombres de dominio (cybersquatting)
- ➔ Vinculación indebida (linking o framing). Metavinculos
- ➔ Metavinculación (Metatagging)
- ➔ Venta de palabras claves (Keywords)

La solución legal en Argentina

- ➔ Caso Fredo, PSA, Xenical. Artículo 50 del TRIP's
- ➔ Desviación fraudulenta de clientela o infracción a la ley de consumidor o lealtad comercial
- ➔ Principios generales del derecho

Derechos de Autor, Patentes, Secretos Industriales e Internet versus reproducción y difusión anónima y masiva

-  Música, Cine y Televisión y Software
-  Caso de la Iglesia Cientológica
-  Caso Napster
-  Motion Picture Association
-  Digital Millennium Copyright Act
-  Casos de modelos contra Google y Yahoo en Argentina

ORGANISMOS, TRATADOS Y HERRAMIENTAS CLAVES

ICANN

IPC (Intellectual Property Contituecy)

Desarrollo del WHOIS Service

Sistema Uniforme de resolución de disputas (UDRP)

OMPI (WIPO)

ADPIC (TRIP's)



SEGURIDAD EN INTERNET

“Un recorrido por los aspectos clave”



ISOC.Ar
Capítulo
Argentina

AGENDA

- ➔ *Aspectos de la Seguridad en Internet*
- ➔ *La Protección de Datos y de la Propiedad Intelectual en la Sociedad de la Información*
- ➔ *Conclusiones y Propuestas de ISOC.Ar*
- ➔ *Preguntas*

CONCLUSIONES Y PROPUESTAS

CONCLUSIONES

- ➔ Mesura y racionalidad al imponer obligaciones a los proveedores de servicios de información y telecomunicación para la protección eficaz de los usuarios.
- ➔ El principio de autodeterminación informativa es un elemento esencial de la protección a la intimidad.
- ➔ Una política de seguridad debe considerar tanto la infraestructura como la información.
- ➔ Delitos informáticos son actividades profesionalizadas



PROPUESTAS

- ➔ Lograr un balance entre la protección de los usuarios y una Internet libre y abierta
- ➔ Establecer consenso en torno a la forma de regular los Delitos Informáticos
- ➔ Generar un ámbito de debate para la búsqueda de mejores soluciones sin interferencias de mercado
- ➔ Ser un canal para la elaboración de propuestas que favorezcan la aplicación de los Principios Rectores



SEGURIDAD EN INTERNET

“Un recorrido por los aspectos clave”



ISOC.Ar
Capítulo
Argentina

AGENDA

- ➔ *Aspectos de la Seguridad en Internet*
- ➔ *La Protección de Datos y de la Propiedad Intelectual en la Sociedad de la Información*
- ➔ *Conclusiones y Propuestas de ISOC.Ar*
- ➔ *Preguntas*



¡ Muchas Gracias !



ISOC.Ar
Capítulo
Argentina

Muchas gracias por participar y
lo invitamos a formar parte de nuestra organización