Romina Garrido
http://protecciondedatospersonales.cl/
Patricia Reyes
www.bcn.cl

"Protección de datos personales e interoperabilidad en la acción del Estado"

Seminario Regional de Protección de Datos.
Montevideo, Uruguay
Junio 2010.

Desarrollo de Gobierno electrónico

Generación de planes y programas: Digitalizar procesos y documentos.

Aprobación de normativa sobre firma electrónica, comunicaciones electrónicas y mensajes de datos

"equivalencia funcional"

asegurar a las personas:

autenticidad (que sepa que la persona o el ente es en efecto quien manifiesta ser)

integridad (que la información enviada o recibida se mantenga inalterada)

no repudio, etc.


ESTOY DESESPERADO, ME TENÍA QUE ENCONTRAR POR AQUÍ CON UNA CHICA, DEJÉ EL COCHE Y ME LO ROBARON. TENÍA TODAS MIS COSAS ADENTRO
PRIMERO LLÁMALA POR TELÉFONO, TOMA MI...
NO SÉ EL NÚMERO, LO TENÍA EN LA AGENDA DEL MÓVIL
YA VENDRÁ, ¿DÓNDE SE ENCONTRABAN EXACTAMENTE?
NO SÉ, LLEGUÉ CON EL GPS
PERO SI EL ENCUENTRO ERA POR AQUÍ, QUIZÁS LA VEAS
NO LE VI NUNCA LA CARA, LA CONOCÍ EN UN CHAT
PAT

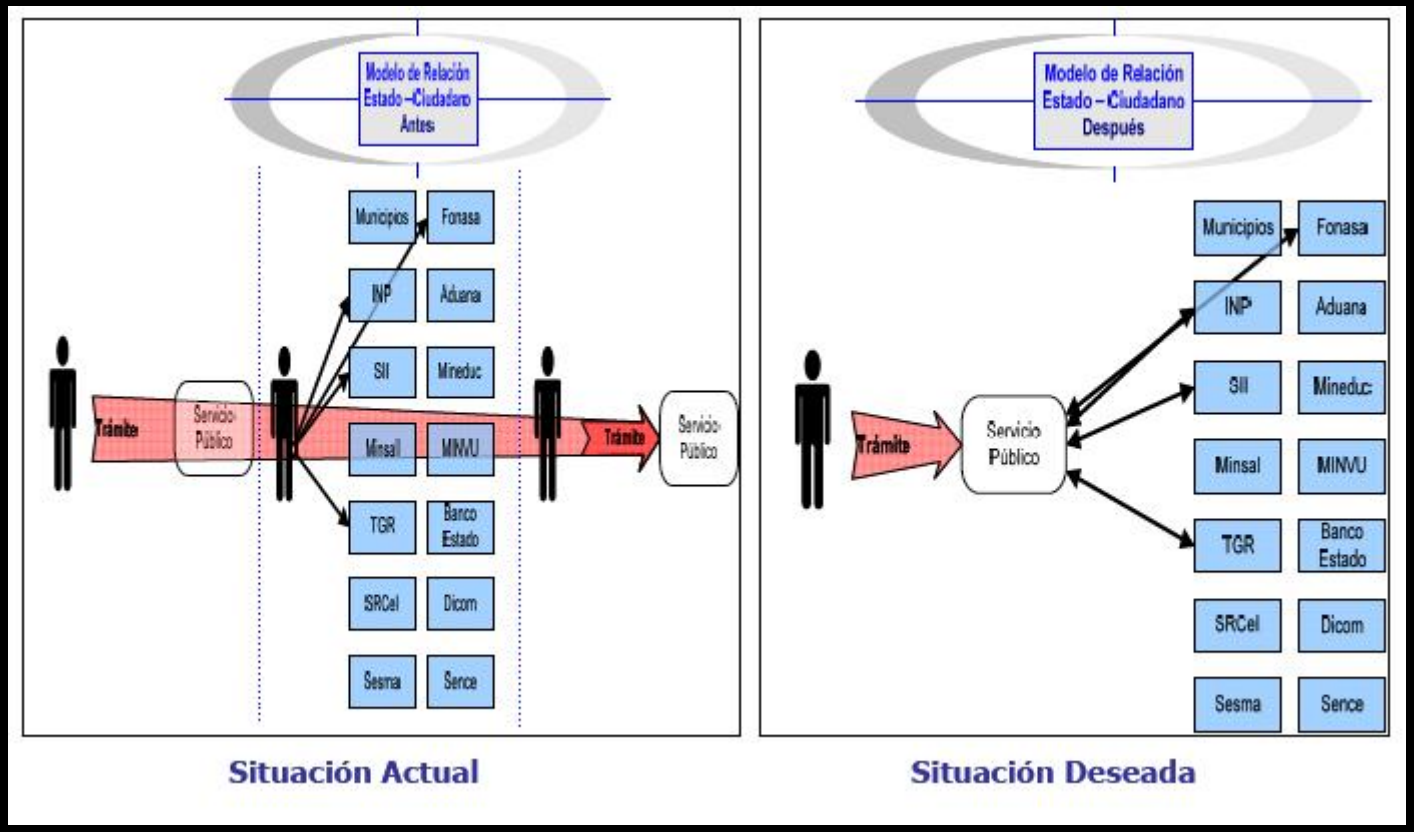
Disponibilidad, acceso e integración de la información, para hacer tangible el derecho de acceso a la información

Interoperabilidad

Concreta derecho de acceso a la información pública, posibilitando la navegación transparente de los ciudadanos a través de los portales públicos y/o la interrelación entre los servicios públicos para un mejor y más eficiente servicio.

En la practica, acceso desde una plataforma común a distintos documentos electrónicos relacionados, aunque éstos se encuentren en distintas bases de datos.

estándares de almacenamiento + tecnologías a los procesos en las organizaciones públicas.


Modelo de Relación Estado – Ciudadano Antes
Municipios
Fonasa
INP
Aduana
SII
Mineduc
Minsal
MINVU
TGR
Banco Estado
SRCel
Dicom
Sesma
Serce
Trámite
Servicio Público
Trámite
Servicio Público
Situación Actual
Modelo de Relación Estado – Ciudadano Después
Municipios
Fonasa
INP
Aduana
SII
Mineduc
Minsal
MINVU
TGR
Banco Estado
SRCel
Dicom
Sesma
Serce
Trámite
Servicio Público
Situación Deseada

Documentación electrónica e Interoperabilidad

Chile

Instalar el Gobierno Electrónico en el país, tiene sus orígenes en el primer Comité interministerial de modernización de la gestión pública en 1998, hoy un comité estable denominado "Estrategia para el desarrollo digital", desde febrero de 2007.

Estrategia digital es el responsable de diseñar y ejecutar una política pública que permita desarrollar acciones en pos de un uso más profundo e intensivo de las tecnologías de información y comunicaciones por parte de los ciudadanos, empresas y el propio Estado.

Marco normativo
a considerar

1. Ley de Firma Electrónica N° 19.799 regula los documentos electrónicos y sus efectos legales y la utilización en ellos de firma electrónica. Los actos, contratos y documentos de los órganos del Estado, suscritos mediante firma electrónica (por tanto documentación electrónica), serán válidos de la misma manera y producirán los mismos efectos que los expedidos por escrito y en soporte de papel.

2. Decreto 181 MINECON 2002, Reglamento de la Ley crea el Comité de Normas para el Documento Electrónico, cuya función principal refiere a asesorar al Presidente de la República con respecto a la fijación de normas técnicas que deberán seguir los órganos de la Administración del Estado para garantizar la compatibilidad de los distintos tipos de documentos electrónicos.

3. Decreto 77 SEGPRES 2004 sobre Eficiencia de Comunicaciones Electrónicas, que reguló este tipo de comunicación entre las dependencias gubernamentales y los ciudadanos.

4. Decreto 81 MINECON 2004 Normas para el Documento Electrónico,

5. Ley de Procedimientos Administrativos, N° 19.880, establece que los servicios públicos no pueden solicitar a un ciudadano que hace un trámite, ningún documento que otra dependencia debe tener. Los órganos gubernamentales deben poder intercambiar y/o validar la información entre ellos.

Características del Documento electrónico

Decreto 81

Fijó el estándar XML

Flexible

Multiplataforma

Permanente

Interoperable

Seguridad de las comunicaciones y documentos electrónicos

Decreto 83

Fija características mínimas obligatorias de seguridad y confidencialidad

Aplicable a todo documento electrónico, que se generen, intercambien, transporten y almacenen en o entre los diferentes organismos de la Administración del Estado y entre éstos y los particulares.

La norma busca garantizar un estándar mínimo de seguridad en el uso, almacenamiento, acceso y distribución del documento electrónico

Cumplimiento de la norma por etapas

Nivel básico de seguridad: año 2004.

Garantizar las condiciones mínimas de seguridad y confidencialidad en los documentos electrónicos que se generan, envían, reciben, procesan y almacenan entre los órganos de la Administración del Estado;.

Condiciones mínimas: política de seguridad en la organización, un encargado de la seguridad de los documentos electrónicos, clasificación de grado de protección de los documentos y su procedimiento de manipulación seguridad física, seguridad del personal, controles de acceso, etc.

Nivel avanzado de seguridad: año 2009.

Para este nivel, se exige la adopción de la norma, ISO NCh-ISO 27002 declarada norma oficial de la república en septiembre de 2009

Soluciones de interoperabilidad y protección de datos

1. Estado es el principal tenedor de información personal

Por razones de planificación, gestión, orden público almacena y registra hechos, documentos que constituyen información personal de los ciudadanos

2. Estado realiza tratamiento de datos personales

Elaboración de políticas públicas y funcionamiento de ciertos servicios públicos requiere manejo y procesamiento de esta información

3. Estado trata datos sensibles

Es deber de los servicios de clasificar el grado de protección de los documentos y establecer los procedimientos de manipulación, en razón del contenido de la información que se almacena y se trata.

A consecuencia de dicha clasificación, y al tratarse de datos de propiedad de terceras personas manipulados por el Estado, se hace más exigente la adopción de medidas de seguridad sobre los documentos que los contienen.

La protección de los documentos, no se justifica en sí misma, sino en virtud de la protección de su contenido.

Guía Modelo de Políticas de Privacidad para la protección de los datos personales.

Mantener adoptar y declarar una política de privacidad es obligatorio en el primer nivel de cumplimiento de la norma técnica para el desarrollo de sitios Web de servicios de los órganos de la administración del estado.

La inclusión de una política de privacidad, apunta a conferir certidumbre a la ciudadanía respecto del tratamiento de datos personales que se verificará en el sitio, así como los derechos de que se es titular y el modo en que puede ejercerlos, anticipando su conocimiento al uso mismo de los recursos disponible en línea

Ley 19.628

Cuando los organismos del Estado tratan datos sólo deben hacerlo respecto a materias de su competencia, de esta manera no requieren consentimiento de su titular

Respeto a los principios informadores del tratamiento de datos

- Finalidad
- Confidencialidad
- Debida diligencia
- Calidad
- Seguridad en el tratamiento

Respeto a los derechos de los titulares de datos

- Acceso e información
- Modificación, cancelación y bloqueo
- Gratuidad
- Habeas data

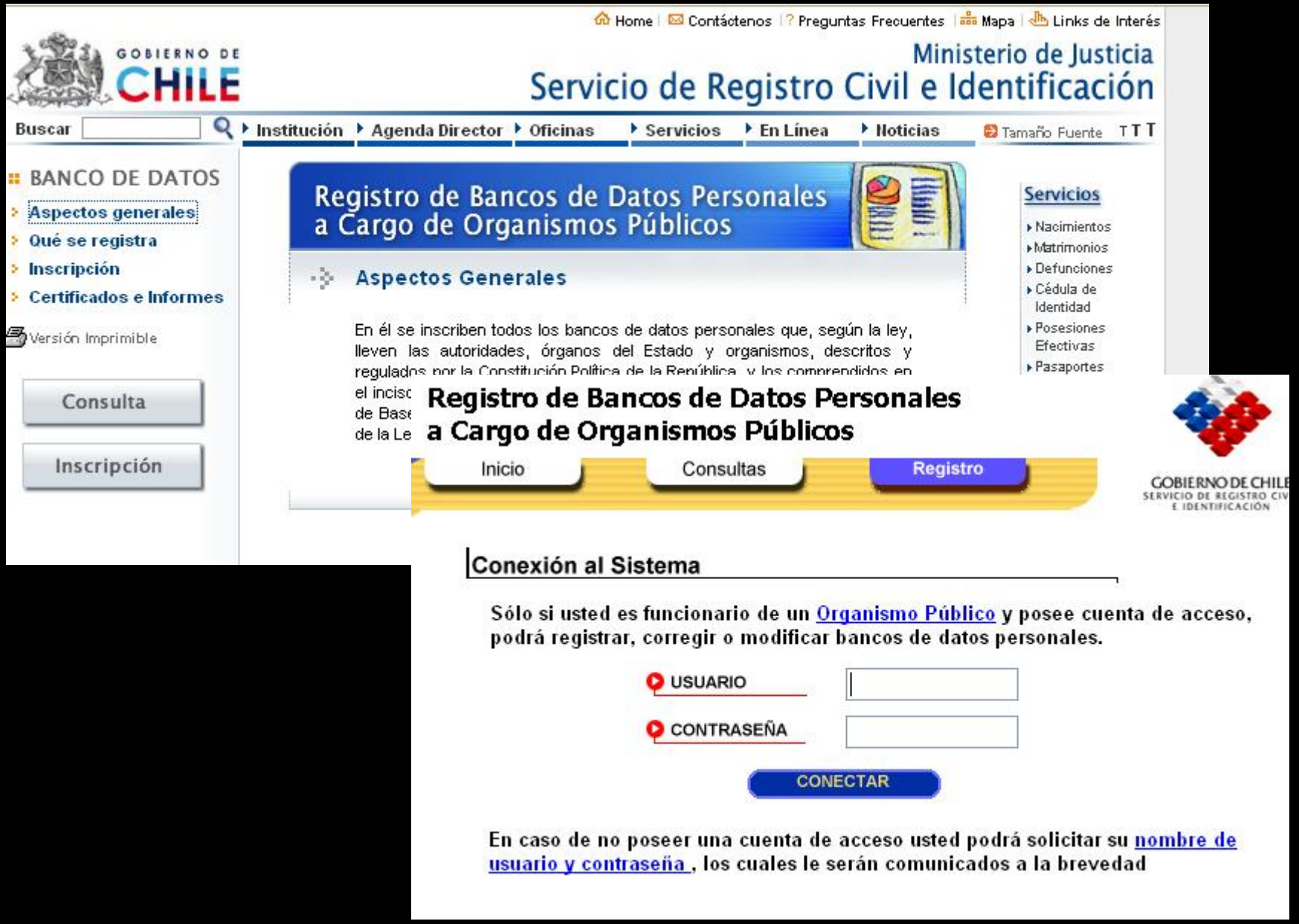
De esta manera, el tratamiento de datos por organismos públicos, no necesita el consentimiento del titular.

Cuando los organismos del Estado tratan datos tienen la obligación legal de registrar su base de datos en el registro civil

Decreto Nº 779 de agosto de 2000 del Ministerio de Justicia. El Registro de Bases de Datos es público y, accesible en línea.

¿Que se registra?

- Organismo Público responsable.
- Nombre del banco de datos personales.
- Fundamento jurídico de su existencia.
- Finalidad.
- El o los tipos de datos almacenados en dicho banco.
- Descripción del universo de personas que comprende.


Home | Contáctenos | Preguntas Frecuentes | Mapa | Links de Interés
GOBIERNO DE CHILE
Ministerio de Justicia
Servicio de Registro Civil e Identificación
Buscar
Institución | Agenda Director | Oficinas | Servicios | En Línea | Noticias
Tamaño Fuente T T T
BANCO DE DATOS
Aspectos generales
Qué se registra
Inscripción
Certificados e Informes
Versión Imprimible
Consulta
Inscripción
Registro de Bancos de Datos Personales a Cargo de Organismos Públicos
Aspectos Generales
En él se inscriben todos los bancos de datos personales que, según la ley, lleven las autoridades, órganos del Estado y organismos, descritos y
Servicios
Nacimientos
Matrimonios
Defunciones
Cédula de Identidad
Posesiones Efectivas
Pasaportes
Registro de Bancos de Datos Personales a Cargo de Organismos Públicos
Inicio
Consultas
Registro
GOBIERNO DE CHILE
SERVICIO DE REGISTRO CIVIL E IDENTIFICACIÓN
Conexión al Sistema
Sólo si usted es funcionario de un Organismo Público y posee cuenta de acceso, podrá registrar, corregir o modificar bancos de datos personales.
USUARIO
CONTRASEÑA
CONECTAR
En caso de no poseer una cuenta de acceso usted podrá solicitar su nombre de usuario y contraseña , los cuales le serán comunicados a la brevedad

Encuesta Consejo para la transparencia

618 organismos públicos,

Desde el 28 de enero al 19 de marzo, (cantidad y tipo de bases de datos personales administradas por el organismo, su marco legal y el tratamiento de los datos; incluyendo si el servicio tiene contratos o convenios de entrega de dichos datos personales. Asimismo, se requería información sobre negativas, modificaciones, eliminación y recursos ante la justicia por parte de los titulares de los datos)

258 organismos públicos

responden encuesta de protección de datos

Objetivo: elaborar recomendaciones o instrucciones en materia de Protección de Datos Personales.

Las transferencias electrónicas de datos personales, entre organismos públicos, deben cautelar los derechos de los titulares y guardar concordancia con las tareas y finalidades de los organismos participantes

El responsable del tratamiento tiene la obligación de dejar constancia de:

a) La individualización del requirente;

b) El motivo y el propósito del requerimiento, y

c) El tipo de datos que se transmiten.

La admisibilidad del requerimiento de transferencia electrónica de datos será evaluada por el responsable del banco de datos que lo recibe, pero la responsabilidad por dicha petición será de quien la haga, es decir del servicio solicitante.

La ley chilena no contempla al encargado del tratamiento que como tal tiene responsabilidades en la actividad de transferencia

En la práctica

[redacted]

El Mercurio, 02 de junio, 2009
Cuerpo A. p. 11

Información nacional de acceso público:

Buscador de personas reabre el debate sobre datos privados

El sitio **trywho.com** identifica a un individuo y da desde su fecha de nacimiento hasta sus bienes raíces. Un proyecto de ley busca frenar la entrega de antecedentes para usos no consentidos.

[redacted]

[redacted]

El Mercurio, 12 de mayo, 2008
Cuerpo C. p. 9

Aparición en internet de datos personales de seis millones de chilenos:

Cibercrimen indaga cómo se filtraron las bases de datos de tres organismos públicos

[redacted]

Diario Financiero, 15 de mayo, 2008. p. 26

LA INDUSTRIA INFORMÁTICA ESTÁ DIVIDIDA, PERO COINCIDE EN QUE EL PELIGRO NO ESTÁ AFUERA

Robo de datos: ¿Qué tan seguros son los sistemas de protección del aparato estatal?

[redacted]

Sin culpables se cierra caso por publicación de bases de datos en internet

El Ministerio Público archivó el viernes la causa, a raíz de que fue imposible dar con el paradero del supuesto *hacker* y que los sistemas informáticos no fueron vulnerados.

Andrés López

Tras cuatro meses de investigación, el fiscal José Ignacio Escobar resolvió archivar sin culpables el caso referente a la publicación en internet de cinco bases de datos con información personal de seis millones de chilenos, al determinar que no es posible rastrear al *hacker* que subió los archivos en una página *web* el 10 de mayo.

Una de las razones para tomar esta decisión se basa en que el informe elaborado por la Brigada del Cibercrimen de Investigaciones concluyó que los sistemas informáticos del Servicio Electoral (Servel), la Dirección General de Movilización Nacional (DGMN), el Departamento de Evaluación, Medición y Registro Educacional (Demre) y la Junta Nacional de Auxilio Escolar y Becas (Junaeb) no fueron vulnerados en los períodos cercanos a la fecha en que estalló el caso.

Tras el análisis de la información, los policías descubrieron que su data fluctuaba entre 2004 y 2006, que en algún momento fue de acceso público, por lo que no vulneraba la privacidad de los afectados. Por ejemplo, una de ellas correspondía al llamado al Servicio Militar efectuado a los estudiantes nacidos en 1988.

"FRED"
sería el nombre del supuesto hacker que publicó la información.

La única base de datos cuyo origen no fue develado es la guía telefónica que estaba en los archivos, puesto que nunca se determinó si estos teléfonos eran verdaderos o inventados. Escobar fue designado dos días después de descubierto el hecho que creó alarma pública, luego de que llegara la denuncia a la Fiscalía Centro Norte.

Consultado por **La Tercera**, el fiscal confirmó esta información y explicó que el archivo de la causa durará hasta que no existan mayores antecedentes.

Pero las diligencias no sólo fueron realizadas en Santiago, puesto que en Temuco se interrogó a un testigo que aseguró conocer al culpable de publicar las bases en internet.

Según su versión, un supuesto hacker de nombre "Fred" se contactó con él y comenzaron a dialogar sobre la vulnerabilidad de los sistemas computacionales de los servicios públicos. A medida que seguían conversando vía *email* le confesó ser el responsable y que actuó con un afán "educador", y era una advertencia sobre la fragilidad en el resguardo de la información privada en el país.

Tras el análisis de las direcciones virtuales (IP) no se logró dar con el lugar físico donde operó "Fred" a raíz de que utilizó IP enmascaradas que ocultaban su verdadera ubicación. Por ejemplo, los mensajes provenían supuestamente de China, Alemania, Estados Unidos y Rusia.

3
archivos comprimidos contenían la información.

Dirección falsa
utilizó el supuesto hacker.

Se publicó en un foro

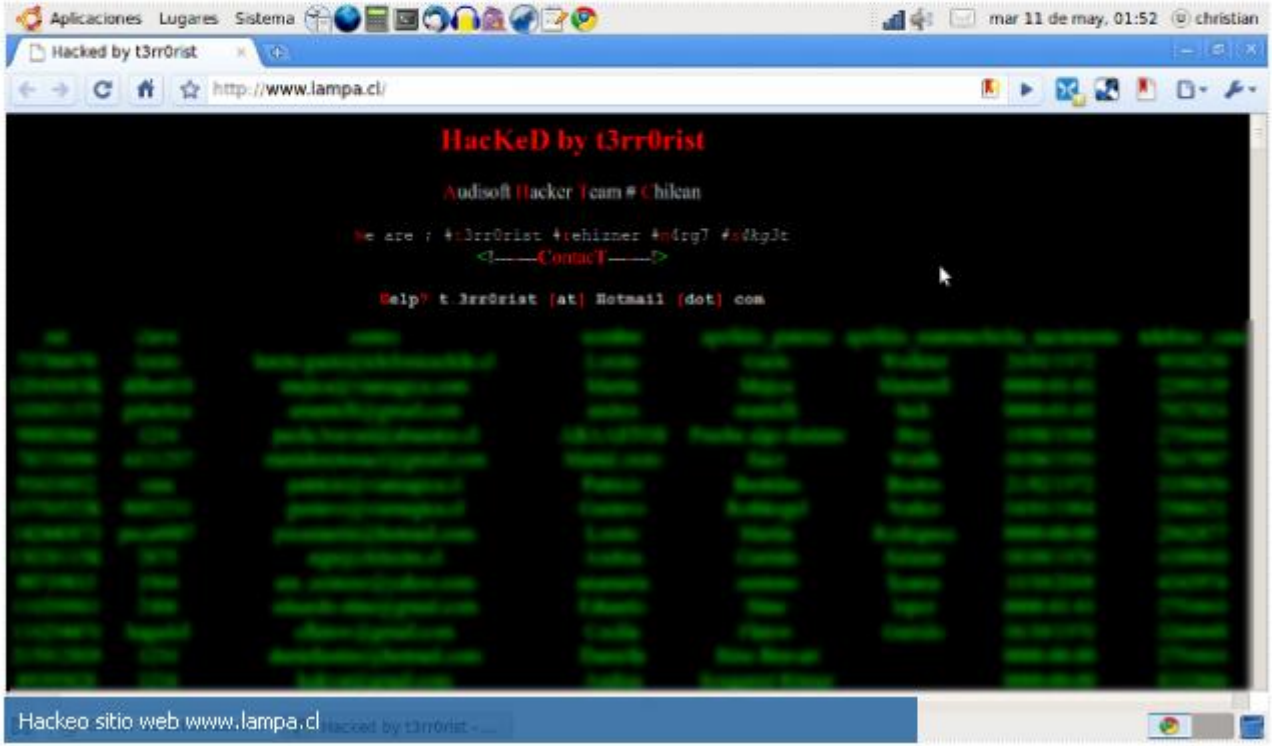
El hecho fue denunciado a la policía por los miembros del *staff* del sitio *fayerwayer.com* tras descubrir que en su foro había tres links que contenían las bases de datos con teléfonos, cédulas de identidad, nombres, direcciones y correos electrónicos.

Martes 11 Mayo 2010 | 2:47

Hackeo a sitios web de Mun. de Lampa y del Serviu de Magallanes expone datos de más de 500 usuarios

Publicado por Alberto Gonzalez • 1,372 visitas

Enviar por correo




Humor12.com
SÍ, CLARO QUE ESCUCHÉ DE LOS HACKERS... SON PERSONAS QUE A TRAVÉS DE LA RED SE PUEDEN METER EN TU COMPUTADORA

Temas

pendientes

responsabilidades difusas. No hay infracciones, ni sanciones efectivas y directas, ni un **órgano de control** por sobre la actividad de aquellos que tratan datos en Chile. El ajuste a la legalidad no puede formar parte de la buena voluntad de los organismos públicos que tratan datos.

no existe uniforme incorporación de las tecnologías de la información a los procesos, generando en definitiva asimetrías en el ejercicio de los derechos de acceso a la información por un lado y habeas data por otro.

Determinación clara sobre la matriz de competencias de los organismos del Estado para tratar datos personales: ¿Donde está la raíz que autoriza a cualquier organismo público para tratar datos personales, generar y mantener bases de datos ¿dónde deben estar explicitadas estas competencias?

Garantizar los niveles de seguridad adecuados en el acceso y las transacciones cuando éstas involucren tratamiento de datos
Seguridad significa inversión de recursos públicos

ciudadanos concientes del valor de sus datos, que demanden la existencia de un estándar real de seguridad y protección.

Romina Garrido
romina.garrido@gmail.com
http://protecciondedatospersonales.cl/

Patricia Reyes
preyes@bcn.cl
www.leychile.cl
www.bcn.cl