

Seguridad en Internet: ¿Un Problema de Seguridad Nacional?

Mariano Lizárraga Fernández · Rommel Toledo Ramírez

México, con poco más de 97 millones de habitantes de acuerdo al último censo poblacional¹, se estima que cuenta con 2.3 millones de usuarios de Internet². Y aún cuando no existe una cifra exacta, es innegable que el número de usuarios de Internet crece día con día en el país; el correo electrónico, videoconferencias, leer las noticias, verificar el estado de cuenta bancario, pago de servicios e incluso las compras cotidianas, son actividades que se desarrollan en Internet con frecuencia por muchos mexicanos.

Las instituciones educativas y la investigación científica también se han visto beneficiadas de manera significativa, lo que antes tomaba varias horas de búsqueda en una extensa biblioteca, hoy solo toma un par de minutos buscar no solo en un sitio físico, sino en miles de universidades y sitios en todo el mundo. De igual forma, las instituciones financieras han sido capaces de ofrecer más y mejores servicios, las tiendas han podido tener un mayor alcance y penetración, en fin, resulta hoy difícil encontrar una institución o un rubro que sea ajeno a las ventajas que presenta tener conectividad a Internet.

Desgraciadamente, no todo ha sido libre de problemas; ataques deliberados a instituciones financieras, comerciales, de gobierno y militares suceden día con día en todo el mundo; y aun cuando la mayoría son solamente casos en que adolescentes intentan penetrar a las redes solo para alterar el contenido de las páginas Web, también ha habido casos severos que le han costado a gobiernos y particulares miles de millones de pesos.

Pero no todos los expertos en redes son malos, ellos mismos se autocatalogan como “*Sombreros Negros*” y “*Sombreros Blancos*”, o malos y buenos; y en ambos lados de la moneda existen personas muy capaces, empleadas por gobiernos e iniciativa privada, y claro, aquellos que simplemente lo hacen por el placer de ser.

Uno de los primeros casos bien documentados de costosas intrusiones a sistemas informáticos fue el presentado por Cliff Stoll en su libro “*El Huevo del Cuckoo*”³ donde explica con lujo de detalle y a manera de novela, la persecución y captura de una serie de espías informáticos de Alemania Occidental, en pleno apogeo de la Guerra Fría.

Pero quizá el hacker “*Sombrero Negro*” más famoso de todos sea el norteamericano Kevin Mitnick, quien después de dos años de intensa persecución fue capturado gracias a la ayuda de un “*Sombrero Blanco*”: Tsutomu Shimomura, ya que el FBI había sido incapaz de seguirle la pista⁴; Kevin Mitnick fue juzgado y sentenciado a 3 años de prisión después de haber cometido fraudes y crímenes informáticos por 15 años de manera impune.

Lo preocupante en este sentido es que no hay que tener un doctorado ni capacitación muy amplia para poder lastimar seriamente a instituciones, tal es el ejemplo del adolescente de solo 17 años de edad, llamado “*mafia boy*”, que en enero del 2001, después de una intensa

búsqueda por parte de autoridades canadienses y estadounidenses, el hacker fue capturado en Canadá, donde los expertos estimaron que sus crímenes habían hecho daño a la industria (principalmente estadounidense) por mil setecientos millones de dólares; desde pequeñas compañías locales hasta los gigantes como CNN, AOL y Amazon fueron víctimas de los ataques de este adolescente⁵. Lo sorprendente de este caso, es que el muchacho tenía un escaso nivel de conocimientos técnicos y realmente solo había utilizado “programas” hechos por expertos y publicados en Internet.

Por fortuna, nuestro país no ha sido víctima de problemas de esa magnitud, pero esto es algo que no se puede, ni se debe, dejar a la suerte, es ahora el momento adecuado de reconocer, que así como las presas, plantas eléctricas, instalaciones de telecomunicaciones, etcétera son consideradas instalaciones estratégicas, el “ciberespacio” mexicano, también debe de ser considerado como un ente importante del país, el cual, así como todas las instalaciones anteriormente mencionadas, requiere de estricta vigilancia y de ser resguardado por el bien de todos los mexicanos.

Colapso del Sistema Nacional Informático, un Escenario Poco Agradable.

Año con año, el Centro de Estudios Superiores Navales, lleva a cabo una serie de estudios y ejercicios donde contemplan las posibilidades de hostilidades con naciones “hipotéticas”: en citado ejercicio, y de manera imaginaria, tropas se movilizan, unidades aéreas y navales conducen operaciones para tomar el control de la imaginaria nación enemiga, miles de marinos y soldados son movilizados en el ejercicio y, después de una semana, el ejercicio termina; esta práctica, que marca la culminación de los cursos de Mando y Diplomado de Estado Mayor, son un saludable ejercicio que permite a los cursantes ver el panorama general de todos los conocimientos adquiridos durante un año.

Sin embargo, una extensa operación militar como la simulada en el CESNAV no es la única forma en la que una nación puede sufrir notables pérdidas, el siguiente, es solo un escenario extremo que demuestra cuán vulnerable puede ser un país, si éste no está preparado para reaccionar de manera adecuada ante emergencias informáticas:

Un día al azar...

- 08:00 Empieza un Ataque distribuido de Negación de Servicios⁶ a las páginas de Internet de los principales bancos mexicanos, éstos se ven obligados a cerrar sus portales. Los bancos no se comunican entre ellos, cada Web master piensa que es un evento aislado.
- 09:30 Un correo electrónico masivo es enviado a miles de usuarios mexicanos con títulos como “Banca Electrónica Temporalmente Cerrada”, con remitentes ficticios de cuentas robadas de los principales proveedores de Internet. Todos aquellos usuarios que abren el correo son infectados con un nuevo virus que a su vez se reenvía a toda la agenda de direcciones de Outlook. La mayoría de los usuarios no se dan cuenta.

- 10:00 Miles de personas acostumbradas a hacer sus transacciones diarias en los bancos por Internet acuden a sucursales físicas a realizar las transacciones; la capacidad de las sucursales en cuestión de horas son sobrepasadas por la cantidad de clientes.
- 11:00 Las paginas de las compañías de teléfonos, telefonía celular y de energía son alteradas para mostrar los saldos inflados en 45% a los usuarios que los consultan por Internet, no hay daño ni penetración a la red de datos de estas compañías, pero los centros de atención telefónica son prácticamente paralizados por la cantidad de usuarios que llama al servicio a clientes para preguntar respecto a su saldo.
- 12:00 La mayoría de los portales de Internet de las secretarías de estado son o alterados o atacados mediante Negación de Servicios; los Web master deciden sacar de publicación sus sitios. No se comunican entre ellos, piensan que es un caso aislado.
- 14:00 Todos aquellos usuarios que han sido infectados con el virus de Outlook, envían un correo electrónico a una de las cuatro tiendas en línea más importantes de México; las tiendas se ven inundadas de correos de miles de usuarios; se ven obligadas a cerrar transacciones.
- 15:00 La seguridad de uno de los bancos es penetrada y miles de números de tarjetas de crédito son robados en cuestión de minutos. El banco se da cuenta y cierra operaciones por completo, cajeros y sucursales se quedan sin “sistema”. La Policía Federal Preventiva es notificada.
- 16:00 Los números de tarjetas de crédito son usados en compras en dos sitios de subastas de México para comprar subastas de particulares; el envío y las insatisfacciones de clientes le costara al sitio miles de pesos y le llevara más de dos meses esclarecerlas.
- 18:00 La Policía Federal Preventiva cae en cuenta de que no es solo un hecho aislado el ataque al banco, y emite una emergencia general a las instituciones financieras, de comunicaciones y de gobierno; prácticamente las operaciones con computadoras en el país se paralizan.

Aún cuando este escenario no deja de ser ficticio, es factible y lo más sorprendente de todo es que para que algo así suceda en el país, lo único que se requiere es que un grupo de no más de 10 Hackers se decidan a hacerlo.

Y, en contra de la idea general, este tipo de crímenes no son crímenes exclusivos de los países desarrollados, y lo alarmante de la situación es que a criterio de la autoridad competente, en este caso la PFP, cada día más Hackers utilizan al país como plataforma para realizar sus ataques⁷, crímenes tales como el robo y fraude a clientes de bancos mexicanos⁸ y el posible robo de información fiscal desde las computadoras de los contribuyentes⁹ han sido reportados recientemente por periódicos nacionales.

Y desde luego, que en el resto del mundo la situación no es diferente, los Hackers astutamente han cambiado su estrategia para atacar equipos de computo, ahora no crean virus, sino que encuentran vulnerabilidades y las ponen al acceso de todos en Internet¹⁰.

Otra cifra alarmante es por ejemplo el caso de los ataques al Departamento de Defensa de Estados Unidos, donde El Pentágono aseguro en el año de 1996 recibir 250000 ciber ataques al año, y que de estos solo uno de cada 150 era detectado y reportado¹¹.

Quizá uno de los más importantes golpes que han recibido las instituciones bancarias fue atestado por un Hacker, en febrero de este año, cuando tuvo acceso a 5.6 millones de cuentas de tarjetas de crédito¹², lo cual, simplemente en el monto de reemplazo de tarjetas plásticas a los afectados, asumiendo un costo de 2 dólares por tarjeta, el monto se va a la alarmante cantidad de 11.2 millones de dólares.

Esta es la realidad hoy en el en el ciberespacio, un sitio “inexistente”, no físicamente palpable, pero que así como trae enormes ventajas a sus usuarios, también trae consigo riesgos.

Autoridades Competentes en el Ciberespacio Mexicano.

Si alguno de los escenarios arriba planteados llegasen a suceder en nuestro país, la capacidad de respuesta de las autoridades es más bien escasa, esto debido a que la legislación actual no contempla en la mayor parte de los casos los llamados “delitos informáticos”. Y es debido a esto que en la mayor parte de los casos se carece de un “plan de contingencia informática”.

En nuestro país la autoridad competente en delitos informáticos es la Policía Federal Preventiva (PFP), con la recién creada “policía cibernética”.¹³

Esta llamada policía cibernética, cuyo nombre oficial es: ***Unidad de policía Cibernética y Delitos Contra Menores***”, es dependiente de la Policía Federal Preventiva de la Secretaria de Seguridad Publica. De acuerdo a la información difundida en su sitio, sus misiones son:

- Identificación y desarticulación de organizaciones dedicadas al robo, lenocinio, tráfico y corrupción de menores, así como la elaboración, distribución y promoción de pornografía infantil, por cualquier medio.
- Localización y puesta a disposición ante autoridades ministeriales de personas dedicadas a cometer delitos informáticos.
- Realización de operaciones de patrullaje anti Hacker, utilizando Internet como un instrumento para detectar a delincuentes que cometen fraudes, intrusiones y organizan sus actividades delictivas en Internet.
- Análisis y desarrollo de investigaciones en campo sobre actividades de organizaciones locales e internacionales de pedofilia, así como de redes de prostitución infantil.

Esta policía esta conformada por 40 elementos cuyas edades oscilan entre los 20 y 23 años, que son especialistas en el manejo de computadoras, psicología y criminalística. Mismos que se encargan de “patrullar” la red, en búsqueda de personas que busquen, generen,

proporcionen u ofrezcan pornografía infantil o turismo sexual de menores. Asimismo buscan prevenir el ataque a paginas del gobierno federal y otros ilícitos relacionados.

Esta dependencia es además la responsable ante el Gobierno Federal de la **Secretaría Técnica del Grupo de Combate Interinstitucional de Delitos Cibernéticos en México**, misma que fue creada en diciembre del 2002 y que esta formada por:

La Policía Federal Preventiva, La Procuraduría General de la Republica, las Secretarías de la Defensa Nacional y de Relaciones Exteriores, el Centro de Investigación y Seguridad Nacional (CISEN), autoridades de los gobiernos estatales de Jalisco y Estado de México, del Distrito Federal, del Poder Legislativo, Instituciones Académicas, compañías prestadoras de servicios de Internet y de la Embajada de Estados Unidos en México.

Este organismo trabaja también en colaboración con el Servicio Secreto y de Aduanas de los Estados Unidos en el intercambio de información y sesiona cada mes.

Los delitos con mayor incidencia en el ciberespacio mexicano según la Secretaria Técnica son: pornografía infantil, fraude por transacciones no finalizadas y amenazas tanto a instalaciones estratégicas como a particulares.

Es importante reconocer el esfuerzo que el país ha hecho en esta dirección, solo Alemania, España, Holanda, Rusia, Australia, Estados Unidos y México cuentan con organismos de este tipo y existe una colaboración entre los gobiernos de estos países para el intercambio de información y datos de los delincuentes o posibles infractores; sin embargo, queda todavía mucho por hacer para mejorar la seguridad del ciberespacio mexicano.

Entidades Educativas

Existen además en México dos grupos de respuesta a emergencias informáticas: el **Equipo de Respuesta de Emergencias Informáticas Mexicano** MxCERTⁱ establecido en el Instituto Tecnológico de Estudios Superiores de Monterrey (ITESM), y el **UNAM-CERT**, de la Universidad Nacional Autónoma de México, mismos que hacen esfuerzos por promover la importancia de la seguridad informática en el país.

Cabe destacar que el Equipo Mx-CERT cuenta con un Sitio en Internet¹⁴ mismo que al momento de escribir este artículo se encuentra “caído”, además de que el Sitio “Hackers Mexicanos”¹⁵ se jacta de haber “hackeado” el Sitio de Mx-CERT¹⁶

En cuanto al UNAM-CERT¹⁷, está localizado en el Departamento de Seguridad en Cómputo (DSC) de la Dirección General de Servicios de Cómputo Académico (DGSCA) de la UNAM.

ⁱ Por sus Siglas en Ingles: Mexican Computer Emergency Response Team

El UNAM-CERT se encarga de proveer el servicio de respuesta a incidentes de seguridad en cómputo a sitios que han sido víctimas de algún “ataque” así como de publicar información respecto a vulnerabilidades de seguridad, alertas de la misma índole y realizar investigaciones de la amplia área del cómputo y así ayudar a mejorar la seguridad de los sitios.¹⁸

Marco Legal Mexicano

Actualmente las únicas leyes que contemplan algunos de los innumerables aspectos del uso del ciberespacio son:

El Código Penal Federal, Código Civil Federal, el Código Federal de Procedimientos Civiles, el Código de Comercio y la Ley Federal de Protección al Consumidor.

A continuación se explican en resumen las consideraciones que hacen los distintos preceptos legales a razón del uso del ciberespacio o de medios electrónicos y/u ópticos.

- Código Penal Federal: Establece las penas para todos aquellos que exhiban pornografía infantil en cualquier medio electrónico (Art. 201 bis), también las penas al que se introduzca y altere o dañe la información contenida en sistemas de cómputo protegidos por cualquier medio, ya sean estos privados o de gobierno (Art. 211 Bis), así como a los que reproduzcan software o creen programas para desactivar la protección del software. (Art. 424 bis).
- Código Civil Federal: Establece la validez de los contratos electrónicos (Titulo Primero, Capitulo I, diversos artículos).
- Código Federal de Procedimientos Civiles: Establece la validez de las pruebas presentadas en medios electrónicos y/u ópticos (Art. 210-A).
- Código de Comercio: Establece la Inscripción de Actos mercantiles en formato electrónico, así como la validez de los Contratos Mercantiles (Diversos artículos).
- Ley Federal de Protección al Consumidor: Establece los derechos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. (Art. 76).

De los documentos estudiados no se encontró ninguno que penalizara el acceso a sistemas de cómputo sin previa autorización. Solo se encontró la siguiente referencia en el Boletín de Prensa 2000/179 del 27 de agosto del 2000 de la pagina del Senado de la Republica.¹⁹

- “Mediante estas modificaciones, se prevé elevar las sanciones, y hacer más rígidos los mecanismos de aplicación y ejecución de las penas en las conductas antisociales como las que atentan contra los derechos de la propiedad intelectual y contra los

derechos industriales; el robo de vehículos y el acceso a sistemas de cómputo sin previa autorización”.

- “En lo referente a la prevención general, se plantea el aumento de las sanciones penales para que los potenciales delincuentes, se abstengan de cometer ilícitos o bien evitar su reincidencia. Además, será objeto de penalización el acceso, sin autorización, a sistemas de cómputo y equipos de informática protegidos por algún mecanismo de seguridad de empresas e instituciones públicas.”

Otros preceptos legales Internacionales firmados por nuestro país que pudiesen ser de aplicación son:

- Convención sobre la propiedad intelectual de Estocolmo.
- Convención para la protección y producción de fonogramas.
- Estudio de la OCDE para armonizar leyes penales internacionales contra el uso indebido de programas de computación.
- Informe 1986 de la OCDE sobre Delitos de informática: Análisis de la normatividad.
- Normas de la OCDE en 1992 para la seguridad de los sistemas de información.
- Reporte del Congreso sobre prevención del delito y Justicia de la Habana, Cuba en 1990, de la ONU.

Estado Actual de la Seguridad en los Sistemas Informáticos del Gobierno Mexicano.

La mayor parte de los sistemas informáticos del país tienen grandes problemas de seguridad, en un estudio de vulnerabilidades efectuado en el año 2001²⁰, se encontraron 436 vulnerabilidades en un total de 242 sitios del Gobierno Federal, Estatales y entidades Educativas evaluados.

De estas el 40.37% eran “Vulnerabilidades de Alto Riesgo”, 49.08% de “Medio Riesgo” y 10.55% de “Bajo Riesgo”ⁱⁱ.

Las dependencias que mostraron menor seguridad en sus Sistemas de acuerdo al porcentaje de Vulnerabilidades de Alto Riesgo encontradas, por sector de actividad son:

ⁱⁱ Son consideradas de “Alto Riesgo” las que permiten obtener servicios de Administrador en el Sistema infiltrado. De “Medio Riesgo” las que permiten obtener información del Sistema tal como cuentas de usuarios, y de “Bajo Riesgo” las que no ponen en peligro el Sistema estudiado.

- Las de Turismo con 70%
- Las de educación con 61%
- Las de Energía con 60% y
- Las de Gobiernos Estatales y Municipales con 56%.

Todo lo anterior nos habla de la baja conciencia que existe en cuanto a la seguridad informática y peor aun al grado de vulnerabilidad que presentan los infraestructura informática del Gobierno y las Instalaciones estratégicas del país ante un ataque como el descrito en la primera parte de este artículo.

Acciones Tomadas en Otros países

En algunos países, ya se han tomado acciones contundentes para atraer la atención de los poderes legislativo y judicial en este aspecto, por ejemplo, en Estados Unidos, desde el año de 1996 ya se hablaba de cómo los ataques informáticos eran un asunto de Seguridad Nacional²¹, y la conciencia de esta amenaza es tal, que recientemente el director de la CIA ha puesto al nivel de las armas de destrucción masiva (nucleares, biológicas y químicas) a este tipo de ataques.

Ese país también ha creado la “Estrategia Nacional para un Ciberespacio Seguro”, emitida por el Departamento de Seguridad Interna en la que destacan cinco prioridades nacionales²²:

1. Creación de un Sistema de Respuesta Nacional de Seguridad del Ciberespacio.
2. Creación de un Programa Nacional de Reducción de Vulnerabilidades y Riesgos de la Seguridad del Ciberespacio.
3. Creación de un Programa Nacional de Entrenamiento y Alerta de Seguridad del Ciberespacio.
4. Asegurar el Ciberespacio del Gobierno, y
5. Cooperación en Seguridad del Ciberespacio Internacional y Seguridad Nacional.

Cada uno los puntos anteriores se subdivide en diversas estrategias para llegar a su cometido, entre las cuales destaca una que trata de promover una “Cultura de Seguridad” global. Eso es debido a que su infraestructura informática está directamente enlazada con Canadá, México, Europa, Asia y Sudamérica. Aquí se destaca también que la gran mayoría de los ciber ataques se originan y pasan a través de sistemas que se encuentran fuera de sus fronteras y que requieren de investigación y cooperación internacionales para ser detenidos.

En ese mismo documento se establece que los Estados Unidos trabajarán en conjunto con Canadá y México para crear una “Ciber Zona Segura”, de modo que identifiquen y aseguren

redes informáticas críticas comunes, tales como: telecomunicaciones, energía, transportes, banca y sistemas financieros, servicio de emergencia, alimentación, salud pública y sistemas de agua potable.

La Unión Europea, también ha iniciado pasos contundentes en contra de este tipo de crímenes, en Noviembre del 2001 se llevo a cabo en Budapest la “Convención de Crímenes Cibernéticos”²³, de la cual se origino un tratado el cual, de acuerdo a su declaración tiene como objetivo: “Establecer un preámbulo y conseguir una política criminalística común, orientada a la protección de la sociedad en contra de ciber crímenes, especialmente adoptando legislación adecuada y fomentando la cooperación internacional”.

En esta llamada Era de la Información, la mayor fuente de riqueza y bienestar tanto de una empresa civil como de un gobierno es su información. Por lo que ésta y los sistemas que la gestionan son los blancos principales de los nuevos enemigos del estado y de los criminales.

Por todo lo anterior es tiempo de que en nuestro país se tomen medidas serias y efectivas en contra de esta nueva amenaza a nuestra Seguridad Nacional y a la nueva forma de vida que nos ha traído la tecnología. De modo que podamos asegurar que Internet y el ciberespacio sean aprovechados de la mejor manera para el engrandecimiento en nuestro país y asimismo haciéndolo cada vez más seguro como una herramienta del Desarrollo Nacional.

Referencias

- ¹ Instituto Nacional de Estadística, Geografía e Informática; <http://www.inegi.gob.mx/difusion/espanol/fietab.html> .
- ² Ciber Atlas de Internet; http://cyberatlas.internet.com/big_picture/geographics/article/0,1323,5911_151151,00.html .
- ³ Stoll, Cliff.- “The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage”, Pocket Books, Julio de 1995; http://www.amazon.com/exec/obidos/ASIN/0671726889/ref=ase_hadelnet/104-9293199-4052739 .
- ⁴ Takedown, la Historia de Tsotomu Shimomura; <http://www.takedown.com> .
- ⁵ “El Hacker Mafiaboy encarcelado”, BBC News, <http://news.bbc.co.uk/1/hi/sci/tech/1541252.stm> .
- ⁶ Descripción de Ataques de Negación de Servicios; <http://www.unam-cert.unam.mx/negacion.html> .
- ⁷ “Llevar Hackers a México al octavo lugar”, Periódico Reforma <http://www.reforma.com/ciudademexico/articulo/281531/default.htm>
- ⁸ “Interponen demanda por Hacker”, Periódico Reforma, <http://www.reforma.com/economiayfinanzas/articulo/285796/default.htm>
- ⁹ “La red, un riesgo para contribuyentes”, Periódico Reforma <http://www.reforma.com/economiayfinanzas/articulo/273042/default.htm>
- ¹⁰ “Cambian Hackers estrategia”, Periódico Reforma <http://www.reforma.com/tecnologia/articulo/256006/default.htm>
- ¹¹ “40 Millones de Potenciales Espías”, Cadena de Noticias CNN <http://www.cnn.com/US/9605/23/internet.spying/index.html>
- ¹² “Hacker gana acceso a 5.6 Millones de Tarjetas de Crédito”, Cadena de Noticias CNN <http://www.cnn.com/2003/TECH/02/17/creditcard.hack/index.html>
- ¹³ Sitio Oficial de la Policía Cibernética; http://www.ssp.gob.mx/_c_programas/p_cibernetica/INDEX.htm .
- ¹⁴ Sitio Oficial del MxCERT; <http://www.mxcert.org.mx/> .
- ¹⁵ Sitio Oficial de los Hackers Mexicanos; <http://hackers.com.mx> .
- ¹⁶ Sitio que Afirma haber tirado el servicio de Mx-CERT; <http://hackers.com.mx/mirrors/team/mxcert.org.mx/> .
- ¹⁷ Sitio oficial del Equipo de Respuesta a Incidentes de Seguridad en Computo; <http://www.unam-cert.unam.mx/> .
- ¹⁸ Fuente UNAM-CERT.
- ¹⁹ Resumen De Trabajo LVII Legislatura, México, D.F., 27 de Agosto del 2000; <http://www.senado.gob.mx/comunicacion/boletines/2000/b27agosto.html> .

²⁰ Un estudio sobre el estado de la seguridad informática en México, SekureIT, Consultores en Seguridad Informática; <http://www.sekureit.com>.

²¹ “Ciber Ataques Amenazan la Seguridad Nacional, dice el Jefe de la CIA” , Cadena de Noticias CNN <http://www.cnn.com/TECH/9606/25/comp.security/>

²² “Estrategia Nacional para un Ciberespacio Seguro”, La Casa Blanca <http://www.whitehouse.gov/pcipb/>

²³ “Convención de Crímenes Cibernéticos ETS No. 185” Budapest, Noviembre del 2001 <http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185>