# viagra.gob.ar: un asunto de seguridad nacional

*Afirmar que sitios gubernamentales argentinos comercializan viagra, cialis o copias de sistemas operativos sin licencia pero a mitad de precio sería una exageración, si no fuera posible encontrar dichos sitios a través de cualquier buscador.*

**Autor:** Lic. Cristian Borghello, CISSP-MVP
Director de www.segu-Info.com.ar
**Versión:** 1.0 (20110206)

## Introducción

La razón de que la afirmación anterior parezca correcta es la (in)seguridad que rodea a una importante cantidad de sitios GOB.AR y que permite que delincuentes de todos los rincones del mundo se beneficien, accediendo sin autorización, modificándolos e incluso poniendo en peligro los datos personales que allí podrían almacenarse, lo que constituye, al menos, una violación al artículo 9 de la Ley 25.326 de Protección de Datos Personales (Habeas Data) [1]:

ARTICULO 2° — (Definiciones)

A los fines de la presente ley se entiende por:
— **Datos personales:** Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

— **Datos sensibles:** Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

...

ARTICULO 9º — (Seguridad de los datos)
1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

## Resumen ejecutivo

En el presente artículo se pretende demostrar, apoyado con casos puntuales, actuales y comprobados, las fallas de seguridad en sitios web gubernamentales argentinos así como la necesidad de mejora y organización de la gestión y cumplimiento obligatorio de las leyes vigentes y de los convenios internacionales, a los cuales Argentina desear adherir.

Inicialmente se realiza un análisis de las leyes de Protección de Datos Personales y Delitos Informáticos y se muestran algunos casos históricos de violación a sitios gubernamentales que almacenan datos personales, financieros o fiscales de los ciudadanos.

Posteriormente se detallan algunos tipos de ciberataques actuales, los motivos económicos que persiguen y cómo las vulnerabilidades en los sitios web facilitan el trabajo de los delincuentes y crean un caldo de cultivo ideal para que esos delitos se multipliquen y arraiguen en el país y puedan ser utilizados para atacar a otros.

Finalmente se analizan las responsabilidades de los entes gubernamentales y se ofrece, humildemente y a modo de ejemplo, una posible alternativa para llevar adelante la publicación de cualquier sitio web oficial, mejorar los canales de comunicación y gestionar los riesgos e incidentes para beneficiar a sus responsables y administradores, cumpliendo la ley y demostrando al mundo que Argentina es capaz de desarrollar políticas de estado en busca de la protección y seguridad de sus ciudadanos.

## Casos resonantes

La República Argentina, como todos los países del mundo, tiene un largo historial de ataques a sus sitios web, aunque no en la medida de otros países como Rusia, Estonia, Georgia, China o Estados Unidos que ya se han visto envueltos en ciberataques (incluso ciberguerras [2]), reflejo de su enemistad política. Lo primero a destacar entonces es que detrás de los ataques que se verán a continuación no existe, en su mayoría, un motivo político de un país adversario.

Quizás uno de los casos más conocidos y resonantes fue la modificación de un discurso del entonces presidente de la nación Néstor Kirchner en marzo de 2005 [3]. Cada discurso se publica en el sitio oficial de la presidencia [4] y, lo que se hizo en esa ocasión, fue cambiar partes del mismo por frases soeces. Al momento de escribir el presente la última modificación (*defacement*[1]) al sitio presidencial, según el Zone-H[2], fue el 11 de diciembre de 2010 [5].

Otros de los casos resonantes fueron en junio de 2009, cuando en plenas elecciones legislativas, se ingresó a la base de datos del padrón electoral [6] y se agregaron leyendas ofensivas sobre algunas provincias. El sitio, perteneciente al Poder Judicial de la Nación, fue corregido pero, luego de que las primeras leyendas fueran suprimidas, volvieron a ingresar al sitio para escribir: *"aumenten la seguridad"* [7].


Imagen 1 - Ataque el sitio del padrón electoral de Argentina (26/06/2009)

A continuación se analiza el marco normativo vigente en la República Argentina y el cumplimiento obligatorio al que deberían atenerse los sitios gubernamentales.

[1] Defacement: modificación de un sitio web o parte del mismo, generalmente la página principal, para demostrar una vulnerabilidad en dicho sitio o para dejar un mensaje político, religioso, burlón, etc.

[2] Zone-H: sitio especializado en *Defacement* en donde cada persona grupo que realiza un ataque a un sitio web, lo reporta allí, lo que permite llevar un ranking de ataques

## Marco Normativo en Argentina

Más allá del supuesto "divertimento" que significa para sus autores, lo descripto representa la comisión de un delito, según la Ley 26.388 de junio de 2008 sobre Delitos Informáticos [8], que modificó el Código Penal Argentino (CPA) para incluir este tipo de ataques:

> ARTICULO 5º — Incorpórase como artículo 153 bis del Código Penal, el siguiente:
>
> Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

Este delito del artículo 153 bis del CPA, es más conocido en el ambiente como la actividad de **hacking**[3], es decir, existe sanción penal para el caso del mero acceso no autorizado a cualquier dato o sistema de **acceso restringido**.

Si bien, en el derecho comparado, otros países han optado por otros sistemas, los legisladores argentinos han remarcado esta última frase y han decidido que existirá delito siempre que el sistema o dato atacado, posea cierto nivel de seguridad, haciendo que el mismo sea considerado como restringido**.** Ahora, para el caso que no sólo se haya accedido sin autorización, sino que además se haya modificado, alterado o suprimido cualquier dato de ese sistema, existe un tipo penal más grave en cuanto a su pena, y es el caso conocido como **cracking**[4]**.**

> ARTICULO 10. — Incorpórase como segundo párrafo del artículo 183 del Código Penal, el siguiente:
>
> En la misma pena (15 días a un año de prisión) incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

En el caso de que el sistema atacado contenga **bases de datos personales** (protegidas en Argentina por la Ley 25.326 ya citada), la pena es aún mayor e incluso sin existir modificación o alteración, el delito se configura al igual que en el "hacking común", con el mero acceso indebido al sistema restringido.

> ARTICULO 8º — Sustitúyese el artículo 157 bis del Código Penal, por el siguiente:
>
> Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:
>
> 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

[3] **El término Hacking, que no debería tener una connotación maliciosa**, se ha visto bastardeado por personas no especializadas y actualmente se aplica a cualquier actividad, sea esta legal o ilegal

[4] **Cracking:** actividad dañina llevada a cabo sobre un sistema

Pero, ¿cuándo un sistema es **legalmente considerado como restringido**? Por ejemplo se lo consideraría restringido cuando cumple las normas de seguridad que exige la Autoridad de Aplicación de la Ley 25.326, la Dirección Nacional de Protección de Datos Personales (DNPDP) [9].

Según la Disposición 11/2006 (DNPDP), para el caso de las bases de datos personales, existen 3 niveles de Seguridad, de acuerdo a la clasificación de los datos personales y quién es el sujeto obligado. Las medidas serán entonces de **nivel básico, medio o crítico**.

Todo sistema donde se realice tratamiento de datos personales, deberá cumplir con el **nivel básico**, existiendo la obligación de cumplimentar con los siguientes requisitos de seguridad:

1. Funciones y obligaciones del personal.

2. Descripción de los archivos con datos de carácter personal y los sistemas de información que los tratan.

3. Descripción de las rutinas de control de datos de los programas de ingreso de datos y las acciones a seguir ante los errores detectados a efectos de su corrección. Todos los programas de ingreso de datos, cualquiera sea su modo de procesamiento (batch, interactivo, etc.), deben incluir en su diseño, rutinas de control, que minimicen la posibilidad de incorporar al sistema de información, datos ilógicos, incorrectos o faltantes.

4. Registros de incidentes de seguridad.

4.1. Notificación, gestión y respuesta ante los incidentes de seguridad.

5. Procedimientos para efectuar las copias de respaldo y de recuperación de datos.

6. Relación actualizada entre Sistemas de Información y usuarios de datos con autorización para su uso.

7. Procedimientos de identificación y autenticación de los usuarios de datos autorizados para utilizar determinados sistemas de información.

La relación entre el usuario autorizado y el/los sistemas de información a los que puede acceder debe mantenerse actualizada. En el caso en que el mecanismo de autenticación utilice contraseña, la misma será asignada por el responsable de seguridad de acuerdo a un procedimiento que garantice su confidencialidad. Este procedimiento deberá prever el cambio periódico de la contraseña (lapso máximo de vigencia) las que deberán estar almacenadas en forma ininteligible.

8. Control de acceso de usuarios a datos y recursos necesarios para la realización de sus tareas para lo cual deben estar autorizados.

9. Adoptar medidas de prevención a efectos de impedir amenazas de software malicioso (virus, troyanos, etc.) que puedan afectar archivos con datos de carácter personal. Entre otras:

1) Instalar y actualizar, con la periodicidad pertinente, software de detección y reparación de virus, ejecutándolo rutinariamente; 2) Verificar, antes de su uso, la inexistencia de virus en archivos recibidos a través de la web, correo electrónico y otros cuyos orígenes sean inciertos.

10. Procedimiento que garantice una adecuada Gestión de los Soportes que contengan datos de carácter personal (identificación del tipo de información que contienen, almacenamiento en lugares de acceso restringidos, inventarios, autorización para su salida fuera del local en que están ubicados, destrucción de la información en desuso, etc.).

Para los casos tratados en el presente (.GOB.AR), al ser sistemas administrados por Organismos Públicos, de acuerdo a la Disposición 11/2006 (Anexo I) y Disposición 7/2008 [9] deberán siempre cumplimentar con el **nivel de seguridad medio**, de manera que además de cumplir con todos los requisitos del nivel básico, deberán tener:

1. El Instructivo de seguridad deberá identificar al Responsable (u órgano específico) de Seguridad.

2. Realización de auditorías (internas o externas) que verifiquen el cumplimiento de los procedimientos e instrucciones vigentes en materia de seguridad para datos personales.

Los informes de auditoría pertinentes, serán presentados al Responsable del Archivo a efectos de que se adopten las medidas correctivas que correspondan. La Dirección Nacional de Protección de Datos Personales, en las inspecciones que realice, deberá considerar obligatoriamente, con carácter no vinculante, los resultados de las auditorías referidas precedentemente, siempre que las mismas hayan sido realizadas dentro de un período máximo de un año.

3. Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

4. Se establecerá un control de acceso físico a los locales donde se encuentren situados los sistemas de información con datos de carácter personal.

5. Gestión de Soportes e información contenida en ellos, 5.1. Se dispondrá de un registro de entradas y salidas de los soportes informáticos de manera de identificar, día y hora de entrada y salida del soporte, receptor, emisor, forma de envío, etc.

5.2. Se adoptarán las medidas necesarias para impedir cualquier recuperación de la información con posterioridad a que un soporte vaya a ser desechado o reutilizado, o que la información deba ser destruida, por la causa que correspondiere.

Asimismo se deberán adoptar similares medidas cuando los soportes, o la información (ej.: cuando se hacen copias de respaldo a través de una red de transmisión de datos, la información sale de un soporte local y viaja hasta otro remoto vía dicha red.), vaya a salir fuera de los locales en que se encuentren ubicados, 5.3. Deberá disponerse de un procedimiento de recuperación de la información de respaldo y de tratamiento de la misma en caso de contingencias que pongan no operativo el/los equipos de procesamiento habituales.

6. Los registros de incidentes de seguridad, en el caso de tener que recuperar datos, deberán identificar la persona que recuperó y/o modificó dichos datos. Será necesaria la autorización en forma fehaciente del responsable del archivo informatizado.

7. Las pruebas de funcionamiento de los sistemas de información, realizadas con anterioridad a su puesta operativa no se realizarán con datos/archivos reales, a menos que se aseguren los niveles de seguridad correspondientes al tipo de datos informatizados tratados.

Por último, para el caso que los datos personales que posea el Estado sean sensibles según la Ley 25.326, se deberá cumplir con el nivel más alto de seguridad, **el nivel crítico**. Es decir que aparte de cumplimentar con todas las medidas del nivel básico y medio, deberán además:

1. Distribución de soportes: cuando se distribuyan soportes que contengan archivos con datos de carácter personal —incluidas las copias de respaldo—, se deberán cifrar dichos datos (o utilizar cualquier otro mecanismo) a fin de garantizar que no puedan ser leídos o manipulados durante su transporte.

2. Registro de accesos: se deberá disponer de un registro de accesos con información que identifique al usuario que accedió, cuando lo hizo (fecha y hora), tipo de acceso y si ha sido autorizado o denegado. En el caso que el acceso haya sido autorizado se deberá identificar el dato accedido y el tratamiento que se le dio al mismo (baja, rectificación, etc.). Este registro de accesos deberá ser analizado periódicamente por el responsable de seguridad y deberá ser conservado como minino por el término de un TRES (3) años.

3. Copias de respaldo: además de las que se mantengan en la localización donde residan los datos deberán implementarse copias de resguardo externas, situadas fuera de la localización, en caja ignífuga y a prueba de gases o bien en una caja de seguridad bancaria, cualquiera de ellas situadas a prudencial distancia de la aludida localización. Deberá disponerse de un procedimiento de recuperación de esa información y de tratamiento de la misma en caso de contingencias que pongan no operativo el/los equipos de procesamiento habituales.

4. Transmisión de datos: los datos de carácter personal que se transmitan a través de redes de comunicación (1), deberán serlo cifrados o utilizando cualquier otro mecanismo que impida su lectura y/o tratamiento por parte de personas no autorizadas.

Estos requisitos de seguridad, son legalmente una referencia para poder responder al interrogante planteado anteriormente: **en Argentina un sistema será considerado restringido cuando mínimamente cumpla con esos requisitos de seguridad**.

Entonces, queda claro que desde el punto de vista del ciudadano, cualquiera de estas actividades mencionadas anteriormente **es un delito** pero, desde el punto de vista de los responsables y administradores de los sitios gubernamentales vulnerados, la negligencia, ¿no debería ser al menos una infracción o contravención? ¿Quién evalúa la gravedad de la información expuesta y el daño que se causa a las organizaciones y a los ciudadanos?

**¿Cumple el Estado Argentino con las medidas de seguridad que son obligatorias según la ley?**

## Motivos económicos detrás de un ataque

Ampliando ahora la búsqueda de posibilidades por las cuales es posible ingresar a un sitio web, sus servidores o sus bases de datos, se procede a analizar los distintos tipos de ataques y los objetivos, principalmente económicos, que existen detrás.

Una vulnerabilidad se define como una debilidad que puede proveer al atacante de un acceso no autorizado a un determinado lugar, red, datos, etc. También puede caracterizarse por la ausencia de una contramedida lo cual, en última instancia, permite el mismo acceso no autorizado. Simplificando, se puede decir que una puerta con la cerradura rota es una vulnerabilidad pero también lo es no destinar un guardia a dicha puerta para cuidarla mientras se repara la cerradura.

Llevando el mismo ejemplo al mundo tecnológico, publicar un servidor y un sitio web en Internet, sin contar con las normas y medidas de seguridad recomendadas y sin un administrador que lleve adelante dichas medidas deja abierto el paso para que, tarde o temprano, un atacante encuentre una debilidad y pueda acceder sin autorización. Luego podrá, por ejemplo, modificar un discurso presidencial o una base de datos personal y, si lo deseara, publicar información de cómo comprar viagra a mitad de precio.

Este procedimiento, ineficiente y negligente, es llevado a cabo en forma constante en Internet y lamentablemente también en sitios gubernamentales. Como resultado visible, por ejemplo, las búsquedas para comprar ciertas drogas o productos (falsos) en sitios GOB.AR arrojan los siguientes resultados:

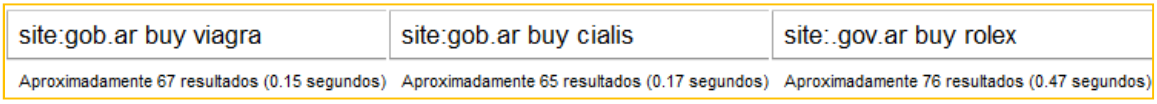


Imagen 2 - Búsqueda de productos (falsos) en sitios gubernamentales argentinos (29/01/2011)

**Nota 1:** la búsqueda se realiza en inglés porque en estos casos los delincuentes son por lo general, extranjeros y, además, de esta manera, se excluyen artículos científicos y oficiales sobre los productos buscados. Las búsquedas GOV.AR y GOB.AR arrojan resultados distintos.

Los resultados indican que los sitios que aparecen listados, ya han sido vulnerados y modificados por los delincuentes con el objeto de ofrecer distintos tipos de productos a quienes visiten los mismos.

El objetivo de estos ataques es lograr encontrar la mayor cantidad posible de sitios vulnerables para poder incluir en ellos la promoción de sus productos. Cuanto mayor sea la cantidad, mayor es la publicidad y más rentable se vuelve el negocio. Es importante aclarar que este tipo de ataques son llevados a cabo en su mayoría por procesos automatizados, lo que descarta que sean dirigidos a sitios específicos, aunque puede darse el caso.

No es objeto de este artículo analizar las técnicas utilizadas para realizar estos ataques pero es necesario enunciar al menos el conocido como **Black Hat SEO**, en el que se busca posicionar en las primeros lugares de un buscador cientos o miles de sitios, con el propósito de que cualquier búsqueda que realice el usuario, lo lleve a uno de ellos, en donde podrá resultar infectado con un malware o se le podrá ofrecer productos (generalmente falsos o adulterados) a "precios inigualables".

En el caso de acceder a un sitio gubernamental, el logro es aún mayor porque ¿quién desconfía de este tipo de sitios? Si la información está allí, debería ser oficial y real.

Por ejemplo, el siguiente caso muestra el sitio de la Comisión Federal de Impuestos [10], en donde se ha creado un subdominio "buy-viagra" para promocionar el producto mencionado (y "sin prescripción médica"):


Imagen 3 - Búsqueda que devuelve sitios gubernamentales modificados (29/01/2011)

Estas páginas que aparecen en la imagen redireccionan a un sitio farmacéutico, que puede variar dependiendo el momento en el que se ingrese.

En la siguiente imagen se puede ver el código fuente del sitio web vulnerado y cómo se realiza la redirección:

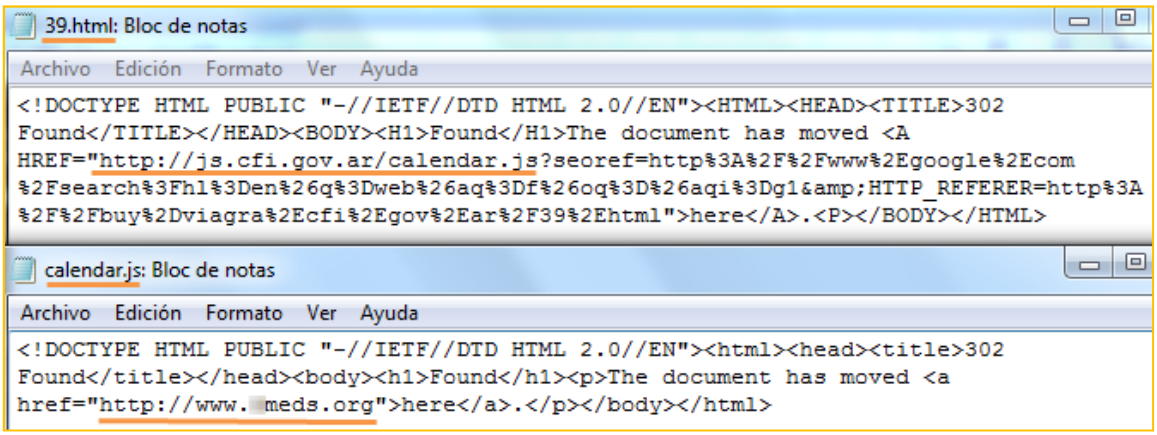


Imagen 4 - Código fuente de los sitios modificados (29/01/2011)

Entonces, si el usuario hace clic sobre los enlaces devueltos por la búsqueda, terminará viendo el siguiente sitio web, que incluso detecta de qué país proviene el visitante para ajustar el idioma. Nuevamente, el sitio puede variar dependiendo el momento en que se ingrese.


Imagen 5 - Sitio con productos farmacéuticos al cual se arriba luego de la búsqueda (29/01/2011)

Otro caso que vale la pena analizar es la modificación de un sitio web para agregar miles de enlaces al mismo sitio dañino (texto oculto[5], *Spamming Keywords*[6] y *Keyword Stuffing*[7]), con el objetivo de "engañar" a los buscadores que, al "ver" este sitio enlazado muchas veces, pueden interpretar que el mismo es popular y por lo tanto mostrarlo en las primeras posiciones.

[5] Texto oculto: colocar palabras claves y enlaces en una página web, con el mismo color de fondo u ocultas, de modo que pasen desapercibida para el usuario, pero no para el buscador

[6] Spamming Keywords: formar frases con palabras claves para que se hagan populares

[7] Keyword Stuffing: abusar de ciertas palabras claves dentro del contenido para hacerlas populares

Esta es la técnica de la cual se valieron los delincuentes para modificar el sitio de la Agencia Nacional de Promoción Científica y Tecnológica [11]. En la siguiente imagen se aprecia que, si bien los enlaces dañinos pasan desapercibidos para el ojo humano, si se analiza el código fuente se pueden encontrar y, por lo tanto serán indexados por los buscadores:


Imagen 6 - Sitio modificado para agregar enlaces ocultos (29/01/2011)

En este caso había 1.538 enlaces ocultos ,y si bien los buscadores implementan técnicas para evitar este tipo de técnicas fraudulentas, de todos modos su utilización aún es masiva por parte de los delincuentes, lo que indica que les sigue resultando beneficiosa.

## Técnicas utilizadas y sus consecuencias

Una vez analizados algunos casos, las consecuencias a las que puede llevar el acceso a un sitio web gubernamental pueden ser algunas de las siguientes:

- Promoción de productos ilegales, para hacer pensar al visitante del sitio que el producto es oficial
- Mensajes políticos, religiosos o discriminatorios
- Daño a la imagen gubernamental o incluso generar problemas políticos internacionales a través de mensajes falsos
- Acceso a bases de datos personales, financieras o fiscales con la consecuente violación a la Ley de Habeas Data y la posible comisión de **delitos de fraude, estafa y robo de identidad**, ya que el delincuente cuenta con información privilegiada y exacta que facilita su "trabajo" posterior.

Un ejemplo de lo citado en los puntos anteriores es el ataque al sitio web del diario de las Islas Malvinas [12], que si bien no es un sitio gubernamental pone en evidencia que la publicación de noticias falsas podría desencadenar un conflicto internacional.

Otra situación similar es la modificación no autorizada del sitio web perteneciente al Instituto Nacional contra la Discriminación y la Xenofobia de Argentina (INADI) que incluyó un mensaje pidiendo la muerte de la familia presidencial y, paradójicamente, un texto discriminatorio hacia ciudadanos peruanos y bolivianos [13].

Pero, más allá de la gravedad de los hechos anteriores, el **acceso indebido a bases de datos personales**, como el ya analizado caso del padrón electoral, constituye en sí mismo la **violación más grave porque se ven involucrados todos los ciudadanos argentinos**.

Un ejemplo de lo mencionado es la posibilidad que tuvieron los delincuentes de acceder a datos de todos los contribuyentes (7 millones) a través del sitio web de la Administración Federal de Ingresos Públicos (AFIP) el pasado 31 de diciembre de 2010 [14]. A través de un fallo en la validación de datos, era posible acceder al documento nacional de identidad (DNI) escaneado, huella digital, fotografía y firma holográfica de cualquier contribuyente.

Meses antes, el jefe de AFIP había afirmado públicamente que la política de digitalizar los datos de los contribuyentes tenía el objetivo de *"brindar mayor seguridad jurídica"* y evitar que terceros utilicen sus claves [15].

> "Esto estará protegido por el secreto fiscal; es la tendencia de otros países de la región y desarrollados. Además, evitará que otra persona diferente del titular del CUIT pueda utilizar esa clave".

La vulnerabilidad fue reportada a la delegación por un blogger argentino y solucionada por AFIP unos días después, sin informar oficialmente en ningún momento sobre la existencia del fallo ni de su posterior solución. Se debe recordar que la institución actúa como custodio de los datos personales y fiscales de sus contribuyentes y, al no protegerlos debidamente, genera una contradicción con la transparencia con la cual debieran manejarse este tipo de situaciones.

Las técnicas utilizadas para vulnerar cualquier tipo de sitio van desde el simple acceso a través de usuarios y contraseñas débiles hasta la utilización de intrusiones avanzadas y, comúnmente utilizadas luego del análisis de la estructura del sitio y de sus posibles vulnerabilidades.

Para analizar algunos casos y demostrar que los atacantes no diferencian razas, credos o creencias políticas, en mayo y en junio de 2009, fueron modificados los sitios oficiales de UCR y PJ, los dos partidos políticos mayoritarios del país (ambos ORG.AR). Si bien en esos caso no se trata de sitios gubernametales, sí lo es el Ministerio de Defensa argentino [16], cuyo sitio fue modificado en enero de 2011.

A continuación se tomará un listado de sitios gubernamentales vulnerables [17] y que fueron denunciados por **Segu-Info** en agosto de 2009 a sus respectivos administradores y a ArCERT [18], la Oficina de Coordinación de Emergencia y Redes Teleinformáticas.

**Tabla 1: sitios vulnerables atacados por desconocidos en agosto de 2009**

| | |
|---|---|
| www.agro.misiones.gov.ar | www.buenosaires.gov.ar |
| www.catamarca.gov.ar | www.ccpm.misiones.gov.ar |
| www.cedit.misiones.gov.ar | www.entrerios.gov.ar |
| www.gobierno.misiones.gov.ar | www.hacienda.catamarca.gov.ar |
| www.hacienda.jujuy.gov.ar | www.ips.misiones.gov.ar |
| www.issp.gov.ar | www.mdsjujuy.gov.ar |
| www.municipios.jujuy.gov.ar | www.policia.misiones.gov.ar |
| www.policiadejujuy.gov.ar | www.propap.jujuy.gov.ar |
| www.proveedores.jujuy.gov.ar | www.registroinmobiliario.catamarca.gov.ar |
| www.salud.catamarca.gov.ar | www.sanjavier.misiones.gov.ar |
| www.softwarelibre.misiones.gov.ar | www.trabajo.jujuy.gov.ar |
| www.turismo.jujuy.gov.ar | www.turismo.misiones.gov.ar |
| www.usigobierno.catamarca.gov.ar | www.vialidad.jujuy.gov.ar |
| www.viedma.gov.ar | |

**Nota 2:** todas las denuncias realizadas desde **Segu-Info** a ArCERT han sido a través de su correo electrónico oficial, destinado a tal fin: mailinfo@arcert.gov.ar. Con respecto a las denuncias realizadas a los responsables de los sitios, al no contar con un correo oficial de denuncias de este tipo, las mismas han sido enviadas a webmaster@sitio.gob.ar y a contacto@sitio.gob.ar.

Luego del ataque, los sitios lucían un mensaje en contra de una disposición fiscal del momento, un impuesto adicional a productos electrónicos fabricados fuera del país, conocido como “impuestazo tecnológico” [19]:


Imagen 7 - Sitios gubernamentales atacados (25/08/2009)

En enero de este año, desde **Segu-Info** nuevamente hemos reportado otros sitios vulnerables a sus responsables y a ArCERT, sin obtener en ningún caso respuesta oficial hasta el momento. Los sitios reportados han sido:

**Tabla 2: sitios vulnerables reportados por Segu-Info el 10 de enero de 2011**

| Localidad | Sitio vulnerable |
|---|---|
| Municipalidad de Puerto General San Martin (Buenos Aires) | http://login.mpgsm.gov.ar |
| Municipalidad de Saladillo (Buenos Aires) | http://www.saladillo.gov.ar |
| CONICET | http://www.imhicihu-conicet.gov.ar |
| Turismo en Tucumán | http://www.tucumanturismo.gov.ar |
| Auditoria General de la Ciudad de Buenos Aires | http://www.agcba.gov.ar |
| Ministerio de Relaciones Exteriores, Comercio Internacional y Culto (Cancillería) | http://prensa.cancilleria.gov.ar |
| Municipalidad de La Cumbre (córdoba) | http://www.lacumbre.gov.ar |

Actualmente, si se busca en Zone-H sitios gubernamentales siendo atacados y modificados, se puede ver que en **los últimos 60 días ha habido 51 ingresos no autorizados** (casi una intrusión al día):

| Time | Notifier | H | M | R | Domain | OS |
|---|---|---|---|---|---|---|
| 2011/01/27 | [M]entes[C]riminales | H | M | R | plannacer.msaludsgo.gov.ar | Linux |
| 2011/01/27 | [M]entes[C]riminales | H | | R | www.msaludsgo.gov.ar | Linux |
| 2011/01/27 | [M]entes[C]riminales | H | M | R | intranet.msaludsgo.gov.ar | Linux |
| 2011/01/26 | T0r3x | | | R | www.sanjuandgr.gov.ar/tor.txt | Win 2003 |
| 2011/01/25 | [M]entes[C]riminales | H | M | | www.buenavista.gov.ar | Linux |
| 2011/01/25 | [M]entes[C]riminales | H | M | | www.herradura.gov.ar | Linux |
| 2011/01/25 | [M]entes[C]riminales | H | M | | www.lagunanaineck.gov.ar | Linux |
| 2011/01/23 | Unknown Core | | | | www.mindef.gov.ar/cgi-bin/ | Win 2000 |
| 2011/01/19 | virus3033 | | M | | www.almafuerte.gov.ar/tribunal/ | Linux |
| 2011/01/15 | CyberHaxors | | M | | defensorsantafe.gov.ar/ch.html | Linux |
| 2011/01/15 | virus3033 | | M | | www.hernando.gov.ar/virus3033.php | Linux |
| 2011/01/15 | virus3033 | | M | | www.municipioembalse.gov.ar/fo... | Linux |
| 2011/01/14 | By_aGReSiF | H | M | | www.saltogrande.gov.ar | Win 2000 |
| 2011/01/14 | By_aGReSiF | | M | | concejoriogrande.gov.ar/agre.html | Linux |
| 2011/01/14 | By_aGReSiF | | M | | lafrancia.gov.ar/agre.html | Linux |
| 2010/12/30 | LatinHackTeam | | | R | www.loteriacorrentina.gov.ar/n... | Linux |
| 2010/12/28 | GHoST61 | | M | | parquesnacionales.gov.ar/gh.html | Linux |
| 2010/12/28 | GHoST61 | | M | | tclarioja.gov.ar/gh.html | Linux |
| 2010/12/28 | GHoST61 | | M | R | dposs.gov.ar/gh.html | Linux |
| 2010/12/28 | GHoST61 | | M | | 700escuelas.gov.ar/gh.html | Linux |
| 2010/12/28 | GHoST61 | | M | R | innovacionrn.gov.ar/gh.html | Linux |
| 2010/12/28 | ulow | | | | rig.tucuman.gov.ar/rfc/ | Linux |
| 2010/12/28 | king511 | | | | www.ic.gba.gov.ar/comedia/ | Linux |
| 2010/12/28 | team-s.b | | | | www.zarate.mun.gba.gov.ar/viej... | Linux |
| 2010/12/20 | xugurx | H | M | | mardelplata-conicet.gov.ar | Linux |

**51 defacement en los últimos 60 días**

Imagen 8 - *Defacement* realizados en los últimos 60 días (29/01/2011)

La siguiente imagen muestra el primer sitio de la lista correspondiente al Ministerio de Salud de una provincia argentina (actualmente eliminado), en una captura según Zone-H:

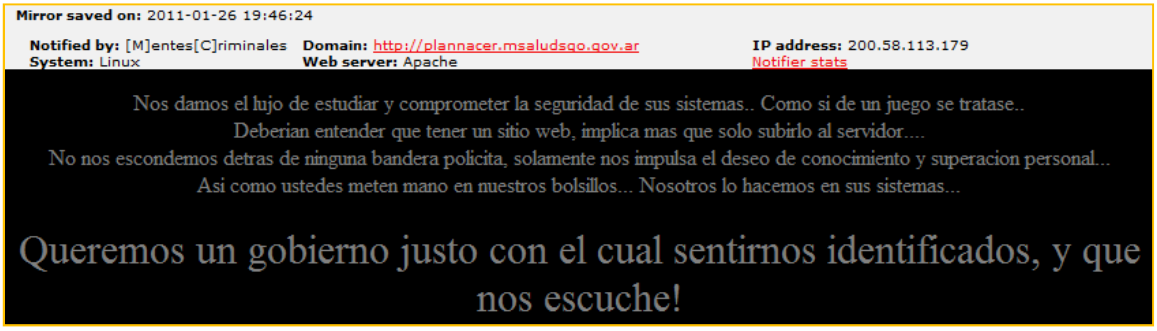


Imagen 9 - Sitio atacado y modificado según la imagen de Zone-H (29/01/2011)

Al momento de desarrollar el presente informe, un año y cuatro meses después del primer reporte, en algunos de los sitios listados en la **Tabla 1** aún se puede "comprar viagra" o "adquirir licencias ilegales de distintos sistemas operativos":


Imagen 10 - Sitio provincial modificado (29/01/2011)

Se debe tener en cuenta que estos resultados son sólo parte de la realidad ya que miles de intrusiones diarias no se reportan y, por lo tanto pasan desapercibidas, sobre todo si persiguen objetivos económicos, como los casos analizados previamente, porque al ocultarlos pueden permanecer en línea más tiempo y se pueden lograr mayores ingresos.

Tal y como muestra la siguiente estadística de Zone-H [21], las técnicas más utilizadas por lo atacantes son el ingreso no autorizado a los servidores, a través de servicios web, TELNET y FTP[8] vulnerables o incorrectamente configurados:

| Attack Method | Total 2008 | Total 2009 | Total 2010 |
|---|---|---|---|
| Attack against the administrator/user (password stealing/sniffing) | 33.141 | 24.386 | 10.918 |
| Shares misconfiguration | 72.192 | 87.313 | 55.725 |
| File Inclusion | 90.801 | 95.405 | 115.574 |
| SQL Injection | 32.275 | 57.797 | 33.920 |
| Access credentials through Man In the Middle attack | 37.526 | 7.385 | 1.005 |
| Other Web Application bug | 36.832 | 99.546 | 42.874 |
| FTP Server intrusion | 32.521 | 11.749 | 5.138 |
| Web Server intrusion | 8.334 | 9.820 | 7.400 |

Imagen 11 - Estadística de tipos ataques de Zone-H

Si aún se utilizan estos servicios, los mismos deberian ser reemplazados por otros más seguros y si, además no son configurados adecuadamente, pueden adolescer de muchas vulnerabilidades propias de su antiguedad o de la utilización de contraseñas débiles.

Estos errores de configuración permiten a cualquier atacante modificar archivos existentes en el servidor o almacenar otros creados por ellos (*File Inclusion*[9]) para realizar una acción (dañina) en particular.

Otras de las técnicas utilizadas es el aprovechamiento de debilidades en las aplicaciones publicadas en los sitios web como causa de desarrollos que carecen de pruebas de seguridad y de calidad mínimas, que serían capaces de detectarlas y corregirlas a tiempo. Por ejemplo, en el caso de la **imagen 10**, seguramente se utilizó una vulnerabilidad de *SQL Injection*[10] para modificar la base de datos donde se alojan las noticias que deben ser publicadas en ese sitio web, haciendo aparecer publicidad de un supuesto producto legítimo.

[8] TELNET y FTP: protocolos de comunicación inseguros creados en los 70 (cuando la seguridad no era una prioridad) y que generalmente se utilizan para acceder a un servidor y administrarlo

[9] File Inclusion: vulnerabilidad que permite incluir llamadas a archivos locales o remotos para que el sitio vulnerado realice una acción distinta a la original

[10] SQL Injection: ataque que consiste en aprovecharse de una vulnerabilidad en un aplicación (generalmente un sitio web) para acceder o modificar una base de datos de la entidad atacada

La Biblioteca Nacional de Maestros [22] también fue víctima de esta vulnerabilidad hace tiempo y el sitio fue modificado, tal y como se ve a continuación (a través de la utilización de la cache del Google):


Imagen 12 - Sitio modificado para alojar publicidad no deseada (29/01/2011)

Sitios tales como la Honorable cámara de Senadores y Diputados argentinos [23] tienen vulnerabilidades similares y otras que permiten la explotación de errores de *Cross Site Scripting* (XSS)[11]. Dichas debilidades fueron reportadas por **Segu-Info** a ArCERT el 14 de noviembre de 2009 y, aunque en este caso sí se recibió respuesta, algunas de ellas aún persisten:

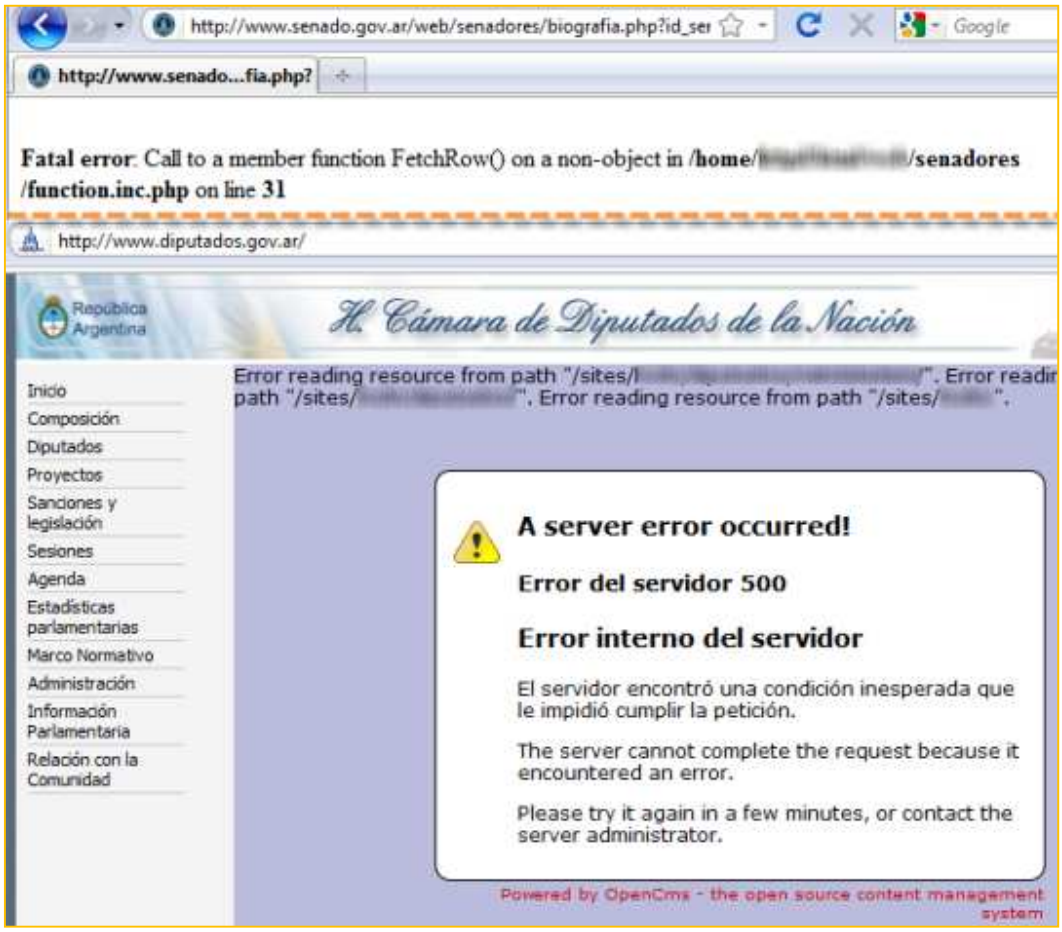


Imagen 13 - Sitios de Senadores y Diputados vulnerables

Si bien existen infinidad de tipos de ataques que se pueden realizar sobre una infraestructura no apropiadamente asegurada, **sólo aplicando los ataques mencionados, se puede causar mucho daño a la imagen gubernamental y a los datos personales de los ciudadanos, sin mencionar el incumplimiento de la ley vigente por parte del estado.**

[11] Cross Site Scripting (XSS): ataque que permite la manipulación de la página web para mostrar contenido o realizar acciones para la cual no fue creada originalmente

## Responsabilidades

Un problema común asociado a todos los citados es la descentralización del gobierno federal que imposibilita que todos los sitios nacionales, provinciales y municipales cuenten con una sóla entidad que las agrupe y administre. **Queda en evidencia la necesidad de que haya una delegación o secretaría que se encargue de analizar las posibles vulnerabilidades, administre los incidentes y facilite su solución.**

Como primer análisis, la entidad que cumple con estos requisitos es la ya mencionada ArCERT [16], dependiente de la Oficina Nacional de Tecnologías de Información (ONTI) [24] de la Secretaria de Gestión Pública [25] de la Jefatura de Gabinete de Ministros, es decir del Poder Ejecutivo Nacional.

El concepto de CSIRT/CERT (*Computer Emergency Response Team*) [26] inicialmente creado en 1988 por la Universidad de Carnegie Mellon como respuesta al gusano de Internet Morris:

> … es un centro de respuesta a incidentes de seguridad en tecnologías de la información. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información. Un CERT estudia el estado de seguridad global de redes y ordenadores y proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red, publica alertas relativas a amenazas y vulnerabilidades y ofrece información que ayude a mejorar la seguridad de estos sistemas.

Existen diferentes CERT públicos y privados en muchos países y, según FIRST (*Forum of Incident Response and Security Teams*) [27], la entidad que actualmente agrupa y coordina los CERT Internacionales, en Argentina existen dos CSIRT/CERT afiliados: ArCERT orientado Administración Pública Nacional (APN) y CSIRT-BANELCO para entidades bancarias privadas.

Según la Resolución 81/99 [28], ArCERT fue planteado como un organismo de asesoramiento, de orientación, de soporte y consulta para centralizar y coordinar los esfuerzos en el manejo de los incidentes de seguridad que afecten los recursos informáticos en el ámbito de la APN y en su política [29] y explicación de su existencia se lee:

> En este sitio encontrará las principales acciones que se están llevando a cabo, para la implementación de Políticas de Seguridad de la Información, en el ámbito de la Administración Pública Nacional de la República Argentina.
>
> …
>
> También difunde información con el fin de neutralizar dichos incidentes, en forma preventiva o correctiva, y capacita al personal técnico afectado a las redes de los organismos del Sector Público Nacional. **ArCERT** comenzó a funcionar en mayo de 1999 en el ámbito de la Subsecretaría de la Gestión Pública, siendo sus principales funciones:
>
> - Centralizar los reportes sobre incidentes de seguridad ocurridos en la APN y facilitar el intercambio de información para afrontarlos.

- Proveer un servicio especializado de asesoramiento en seguridad de redes.
- Promover la coordinación entre los organismos de la APN para prevenir, detectar, manejar y recuperar incidentes de seguridad.
- Actuar como repositorio de toda la información sobre incidentes de seguridad, herramientas y técnicas de defensa"

En un país federal, cada provincia decide sus políticas incluso en materia del uso de la tecnología y, entonces para formar parte en forma gratuita de ArCERT, cada entidad debe solicitar, en forma voluntaria, una membresía. Si bien los beneficios son similares en cada una de ellas, los organismos nacionales pueden solicitar una "membresía plena" y los organismos provinciales o municipales, una "membresía simple" [30].

En paralelo, recientemente Argentina ha solicitado formalmente adherir a la Convención de Cibercriminalidad, conocido como el Convenio de Budapest [31], una iniciativa de la Unión Europea que busca crear lazos de cooperación para combatir la delincuencia informática.

Esta Convención es, por el momento, el único instrumento legal internacional que consagra estándares mínimos en la materia, sentando los lineamientos básicos entorno a tres cuestiones de vital importancia: la tipificación de los delitos informáticos, en la que se basó buena parte de la Ley 26.388 argentina; los aspectos procesales implicados en la investigación de estos delitos, y las cuestiones relativas a la cooperación internacional, teniendo en cuenta que estas conductas no reconocen fronteras políticas, territoriales, ni legales.

Entre los requisitos que debería cumplir Argentina para poder ser parte del Convenio, se encuentra el siguiente:

> Artículo 35. Red 24/7
>
> 1. **Los Estados designarán un punto de contacto localizable las 24 horas del día, y los siete días de la semana, con el fin de asegurar la asistencia inmediata en la investigación de infracciones penales llevadas a cabo a través de sistemas y datos informáticos o en la recogida de pruebas electrónicas de una infracción penal**.
> Esta asistencia comprenderá, si lo permite el derecho y la práctica interna, facilitar la aplicación directa de las siguientes medidas:
>
> a. aportación de consejos técnicos.
> b. conservación de datos según lo dispuesto en los artículos 29 y 30; y
> c. recogida de pruebas, aportación de información de carácter jurídico y localización de sospechosos.
>
> 2. a. Un mismo punto de contacto podrá ser coincidente para dos Estados, siguiendo para ello un procedimiento acelerado.
> b. Si el punto de contacto designado por un Estado no depende de su autoridad o autoridades responsables de la colaboración internacional o de la extradición, deberá velarse para que ambas autoridades actúen coordinadamente mediante la adopción de un procedimiento acelerado.
>
> 3. Los Estados dispondrán de personal formado y dotado a fin de facilitar el funcionamiento de la red.

Sin perjuicio de lo expresado, el mismo CERT, cuando se refiere a los afiliados nacionales (página 4, traducción libre) [32] menciona:

> Internet en sí mismo se ha vuelto una infraestructura crítica que debe ser protegida. Continúa expandiéndose y hay un movimiento continuo hacia configuraciones distribuidas heterogéneas cliente-servidor. Así como la tecnología está distribuida, a menudo se da el caso que la administración de la tecnología también es distribuida.

Lamentablemente esa autonomía y distribución mal entendida e implementada, genera el inconveniente de que cada delegación se crea capaz de administrar su tecnología de forma individual. De allí que no sea homogéneo el nivel de calidad de la administración, incluyendo la seguridad de la información y, en el futuro cercano, la posible evaluación por organismos internacionales que harán énfasis en las deficiencias mencionadas.

## ¿Una idea?

Analizando las normas nacionales e internacionales anteriores y, de desear una "política nacional" que cubra a todos los sitios gubernamentales, parece lógico pensar que las membresías de ArcERT deberían ser obligatorias para cada sitio GOB.AR y de esta forma el organismo podría dar soporte a cada delegación.

Pero, ¿cómo controlar dicha participación en una administración descentralizada como la detallada? La respuesta a ese interrogante debería venir de la mano de NIC Argentina [33] dependiente del Ministerio de Relaciones Exteriores, Comercio Internacional y Culto [34], es decir también del Poder Ejecutivo Nacional.

**Nota 3:** paradójicamente, el sitio de este Ministerio figura en la **Tabla 2** como uno de los reportados como vulnerables por **Segu-Info.**

Según la normativa de NIC.ar, para registrar un dominio gubernamental (o militar), cada entidad debe realizar un trámite formal ante la institución, previa a su autorización:

> - Denominaciones bajo el subdominio GOB.AR: sólo podrán registrar nombres dentro del subdominio GOB.AR las entidades que pertenezcan al Gobierno Nacional, Provincial o Municipal de la República Argentina que cumplan con lo establecido en la Regla 7, in fine.
>
> ...
>
> 7. Las denominaciones que contengan las palabras, letras, o nombres distintivos que usen o deban usar la Nación, las provincias y los municipios, sólo podrán ser registradas por las entidades públicas que correspondan. Las denominaciones bajo GOB.AR sólo se registrarán a nombre de organismos de gobierno que pertenezcan a los Poderes Ejecutivo, Legislativo o Judicial nacionales, provinciales o municipales. La solicitud de registro de un nombre de dominio, en los términos expuestos precedentemente, podrá tener aceptación definitiva cuando la autoridad competente del organismo registrante, tras completar el trámite de registro pertinente vía Internet, haga llegar a NIC Argentina una nota oficial, con membrete de la dependencia, firma original y sello del funcionario a cargo de la misma, en la que se solicite el nombre de dominio en cuestión para dicho organismo.

Entonces, si NIC.ar conoce de la existencia de cada dominio gubernamental (no de los subdominios creados *a posteriori*), incluso antes de su creación efectiva, ¿por qué no es posible controlar la seguridad de los sitios web antes de su publicación, cuando lo que se pone en juego son los datos de los ciudadanos? (aunque muchas veces un sitio web gubernamental sólo se utilice para campañas políticas del gobierno de turno).

Seguramente la respuesta a esas preguntas puedan estar asociadas al presupuesto y los recursos de los cuales se dispone pero, por otro lado, todo parece indicar que existen los canales oficiales para como para llevar adelante una mejora sustancial (comparado con lo actual), suponiendo que el "desarrollo e innovación tecnológica" sea un asunto de estado, tal y como lo enuncia la Resolución de 1999, cuando se creó ArCERT.

## Conclusiones

Actualmente las vulnerabilidades en sitios gubernamentales existen, son muchas y variadas y, como se mencionó al principio, el objeto del presente es hacer un llamado de atención con fines de información y educación en materia de Seguridad de la Información. Un llamado que deben atender especialmente aquellos profesionales que son personal responsable y autorizado de los sistemas del Estado Argentino pero, sobre todo, el mismo Estado Argentino.

Estas vulnerabilidades han permitido a lo largo del tiempo que delincuentes con distintos intereses se hagan con la administración de los sitios web y puedan desde modificar una página con un mensaje alegórico, hasta la venta de productos ilegales o la modificación de datos personales de los ciudadanos argentinos.

Más allá de los errores de infraestructura, diseño y programación y de las técnicas utilizadas para vulnerar un sitio web, sus archivos o sus bases de datos, los desafíos que el Estado Nacional debería plantear para los sitios gubernamentales son:

- Mejora de la gestión y administración eficiente de la seguridad de la información.
- Capacidad para analizar los riesgos a los cuales se expone el sitio web y la información que el mismo posee.
- Poner a disposisicón recursos, tiempo y capacitación del personal involucrado.
- Desarrollos de aplicaciones seguras para evitar vulnerabilidades ampliamente conocidas por los delincuentes, lo que las hace aún más susceptibles de ataques.
- Evaluación de herramientas para evitar que los atacantes puedan realizar desde un simple cambio en una página hasta el acceso a una base de datos con información sensible.
- Auditorias y análisis de penetración y de vulnerabilidades realizado por personal autorizado y capacitado, con el fin de hallar errores en la infraestructura y sus aplicaciones.
- Creación de equipos de gestión de crisis para lograr trabajar eficaz y eficientemente en momentos que exigen celeridad.
- Seguimiento de incidentes, de forma tal que cuando se reporta y soluciona una vulnerabilidad, se analicen otras amenazas similares y también se solucionen.
- Análisis exhaustivo de la normativa nacional e internacional que obliga a cumplimentar acciones responsables sobre la información del Estado.
- Ningún sistema es 100% seguro, es necesaria la creación de áreas que reciban las denuncias sobre las posibles vulnerabilidades, para solucionarlas en el menor tiempo posible.
- Solucionar incongruencias tales como que existen sitios GOV.AR y GOB.AR o desarrollos sobre software libre y software pago, sin un lineamiento claro al respecto, más alla de los recursos propios con los que cuenta cada delegación.

- Procesos y procedimientos oficiales que cualquier organización gubernamental debería seguir para crear su estructura de red, base de datos y sitios webs. En caso de que dicha normativa exista, los casos demuestran que no se están aplicando.
- Mayor coordinación entre diferentes organismos para llevar adelante la publicación responsable de cualquier sitio gubernamental.
- Aplicación federal de políticas de seguridad de la información que deban ser cumplidas por cualquier delegación nacional al momento de registrar un dominio y de publicar un sitio web.

Muchas de estos puntos son, en definitiva, efectos de la falta de planeamiento y aplicación de un verdadero Sistema de Gestión de la Seguridad de la Información (SGSI), con la responsabilidad que merecen los sistemas informáticos del Estado Nacional.

En un país dividido por diferentes motivos sociales, económicos y políticos, ¿es posible pensar en seguridad de la información y en seguridad nacional? o ¿seguirá siendo posible comprar viagra en sitios gubernamentales?

**Agradecimientos**

A los que cada día colaboran para que la Comunidad de **Segu-Info** siga creciendo y ayudando a que los sistemas y vidas de miles de personas sean más seguras.

Especialmente a EJ, FM, MT, OG y RB por su colaboración y aportes invalorables para este artículo.

## Referencias

**Todos los enlaces a continuación fueron visitados el 29 de enero de 2011.**

[1] Ley 25.326 de Protección de Datos Personales
http://infoleg.mecon.gov.ar/infolegInternet/anexos/135000-139999/136121/norma.htm

[2] Informe de ciberguerra de la OCDE
http://blog.segu-info.com.ar/2011/01/informe-de-ciberguerra-de-la-ocde.html

[3] Atacan sitio oficial de la Presidencia de la Nación Argentina
http://www.pergaminovirtual.com.ar/revista/cgi-bin/hoy/archivos/00001914.shtml
http://www.chacabucoya.com.ar/noticias/30007434-hackearon-la-pagina-web-de-la-presidencia-de-la-nacion.htm

[4] Sitio oficial de la Presidencia Argentina y discurso (original) del presidente Néstor Kirchner
http://www.presidencia.gob.ar
http://www.casarosada.gov.ar/index.php?option=com_content&task=view&id=1921&Itemid=71

[5] Ingreso al sitio web presidencial en diciembre de 2010
http://www.zone-h.net/mirror/id/12686576

[6] Sitio del padrón electoral perteneciente al Poder Judicial de la Nación
http://www.padrones.gov.ar/

[7] Ataque al sitio del padrón electoral
http://blog.segu-info.com.ar/2009/06/argentina-atacaron-la-pagina-oficial.html
http://edant.clarin.com/diario/2009/06/26/um/m-01947145.htm
http://gomobile.com.ar/2009/06/acerca-del-hack-al-padron-electoral/

[8] Ley 26.388 de Delitos Informáticos
http://www.segu-info.com.ar/boletin/boletin-113-080607.htm
http://www.infoleg.gov.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

[9] Dirección Nacional de Protección de Datos Personales (DNPDP) y Disposición 11/2006
http://www.jus.gob.ar/datos-personales.aspx
http://www1.hcdn.gov.ar/dependencias/dip/textos%20actualizados/25326.010408.pdf
www.jus.gov.ar/media/33445/disp_2006_11.pdf
www.jus.gov.ar/media/33466/disp_2008_09.pdf

[10] Comisión Federal de Impuestos
http://www.cfi.gov.ar/

[11] Agencia Nacional de Promoción Científica y Tecnológica
http://www.agencia.mincyt.gob.ar/

[12] Defacing a diario Kelper
http://blog.segu-info.com.ar/2010/02/defacing-diario-kelper.html
http://www.penguin-news.com/
http://www.zone-h.org/mirror/id/10281468

[13] 'Hackean' página del Gobierno argentino y piden muerte para peruanos

http://www.larepublica.pe/30-04-2010/039hackean039-pagina-del-gobierno-argentino-y-piden-muerte-para-peruanos

[14] Filtración de información privada en AFIP (solucionado)
http://blog.segu-info.com.ar/2011/01/filtracion-de-informacion-privada-en.html
http://www.fernando.com.ar/2011/afip-filtra-informacion-privada/
http://www.fernando.com.ar/2011/arreglado-el-problema-en-afip/

[15] Los contribuyentes con CUIT deberán reinscribirse en 2010
http://www.lanacion.com.ar/nota.asp?nota_id=1200777

[16] Ataques a sitios de UCR, PJ y Ministerio de Defensa
http://blog.segu-info.com.ar/2009/05/defacing-al-sitio-oficial-de-la-ucr-en.html
http://blog.segu-info.com.ar/2009/06/defacing-al-sitio-web-del-pj.html
http://blog.segu-info.com.ar/2011/01/sitio-del-ministerio-de-defensa.html
http://www.zone-h.org/mirror/id/8941153
http://www.zone-h.org/mirror/id/12945183

[17] Ataque simultáneo de sitios gubernamentales argentinos
http://blog.segu-info.com.ar/2009/08/deface-simultaneo-de-sitios.html
http://blog.segu-info.com.ar/2009/08/mas-sitios-gubernamentales-argentinos.html

[18] ArCERT
http://www.arcert.gov.ar/

[19] Impuestazo tecnológico o la modificación a la Ley de Impuestos Internos
http://www.infobae.com/contenidos/464638-101275-0-Diputados-aprob%C3%B3-el-pol%C3%A9mico-impuestazo-tecnol%C3%B3gico
http://tecnologia.infobaeprofesional.com/notas/85575-Avanza-el-proteccionismo-el-impuestazo-tecnologico-ya-tiene-media-sancion.html
http://www.lanacion.com.ar/nota.asp?nota_id=1158931&pid=7031262&toi=6258

[20] Sitio modificado y atacado
http://www.zone-h.org/mirror/id/12970049

[21] Estadística de ataques de Zone-H
http://www.zone-h.net/news/id/4735

[22] Biblioteca Nacional de Maestros
http://www.bnm.me.gov.ar/

[23] Honorable Cámara de Diputados y Senadores
http://www.senado.gov.ar/
http://www1.hcdn.gov.ar/

[24] La Oficina Nacional de Tecnologías de Información (ONTI)
http://www.sgp.gov.ar/contenidos/onti/quienes/quienes.html

[25] Secretaria de Gestión Pública de la Nación
http://www.sgp.gob.ar/

[26] CERT
http://es.wikipedia.org/wiki/CERT

[27] National CSIRT (2004)
http://www.cert.org/archive/pdf/NationalCSIRTs.pdf

[28] Resolución 81/99 para formación de ArCERT
http://www.arcert.gov.ar/documentos/resarcert.pdf
http://www.sgp.gov.ar/contenidos/onti/productos/arcert.html

[29] Política de ArCERT
http://www.arcert.gov.ar/politica/
http://www.arcert.gov.ar/webs/que_es_arcert.html

[30] Membresías en ArCERT
http://www.arcert.gov.ar/webs/pre_asociarse.htm

[31] Convenio sobre Cibercriminalidad de Budapest
http://blog.segu-info.com.ar/2010/03/que-es-el-convenio-sobre.html
http://www1.hcdn.gov.ar/proyxml/expediente.asp?fundamentos=si&numexp=0890-D-2009
http://conventions.coe.int/Treaty/en/Treaties/html/185-SPA.htm

[32] CERT miembros de FIRST en Argentina
http://www.first.org/members/map/
http://www.arcert.gov.ar/webs/tramiteq.html

[33] NIC Argentina
http://www.nic.ar/normativa.html

[34] Ministerio de Relaciones Exteriores, Comercio Internacional y Culto
http://www.mrecic.gov.ar/