

Fraudes en los Sistemas de Registro

Lic. Cristian Borghello, CISSP – CSSK – MVP

www.segu-info.com.ar

info@segu-info.com.ar

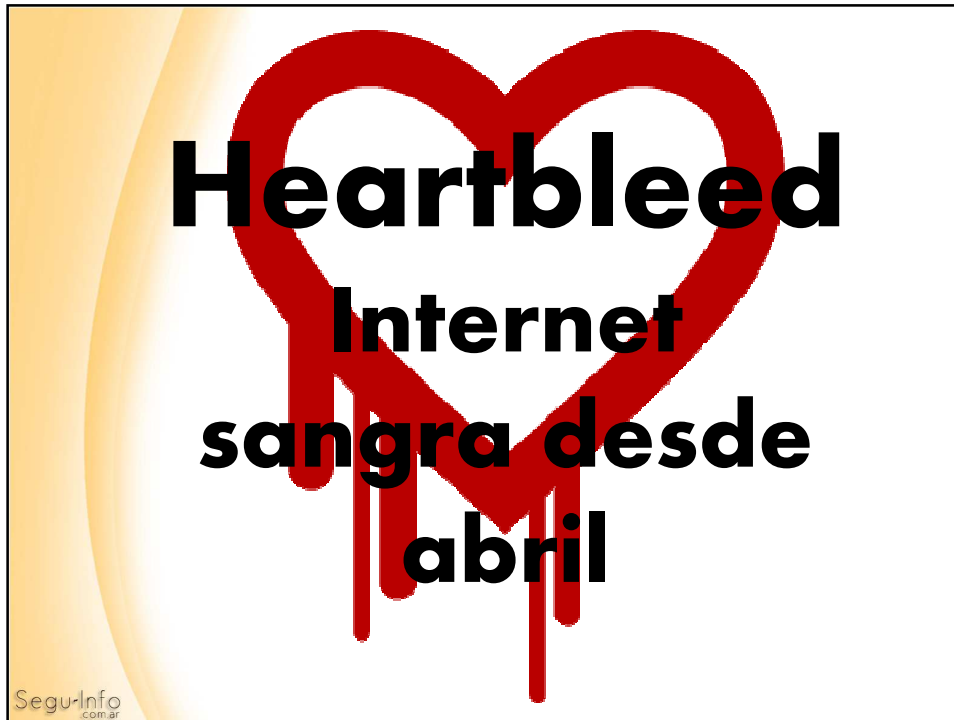
@SeguInfo



Sobre Cristian Borghello

- Licenciado en Sistemas UTN desde 2000
- Desarrollador desde los 8 años
- CISSP (Certified Information Systems Security Professional) desde 2008
- Microsoft MVP Security (Most Valuable Professional) desde 2010
- CCSK (Certificate Cloud Security Knowledge) desde 2014
- Creador y Director de **Segu-Info**
- Consultor independiente en Seguridad de la Información

Segu-Info
com.ar



Canadá apaga sus web públicas por problema informático 'Heartbleed'

Wn.com

El Gobierno canadiense ordenó a todos sus departamentos que "desconecten inmediatamente" todas sus páginas de internet que operan con versiones del software OpenSSL afectadas por la vulnerabilidad conocida como "Heartbleed". La directiva fue comunicada en la noche del jueves a los departamentos federales canadienses y anunciada por el Secretario del Consejo del Tesoro de Canadá, Tony Clement, a través de Twitter. "He aprobado la directiva para INHABILITAR todas las páginas públicas del Gobierno de Canadá que funcionan con la versión antigua de OpenSSL debido a la amenaza de Heartbleed", dijo Clement. [El...more »](#)

Segu-Info.com.ar



Ley de Protección de Datos Personales N° 25.326, Seguridad del Art. 9 inc. 1:

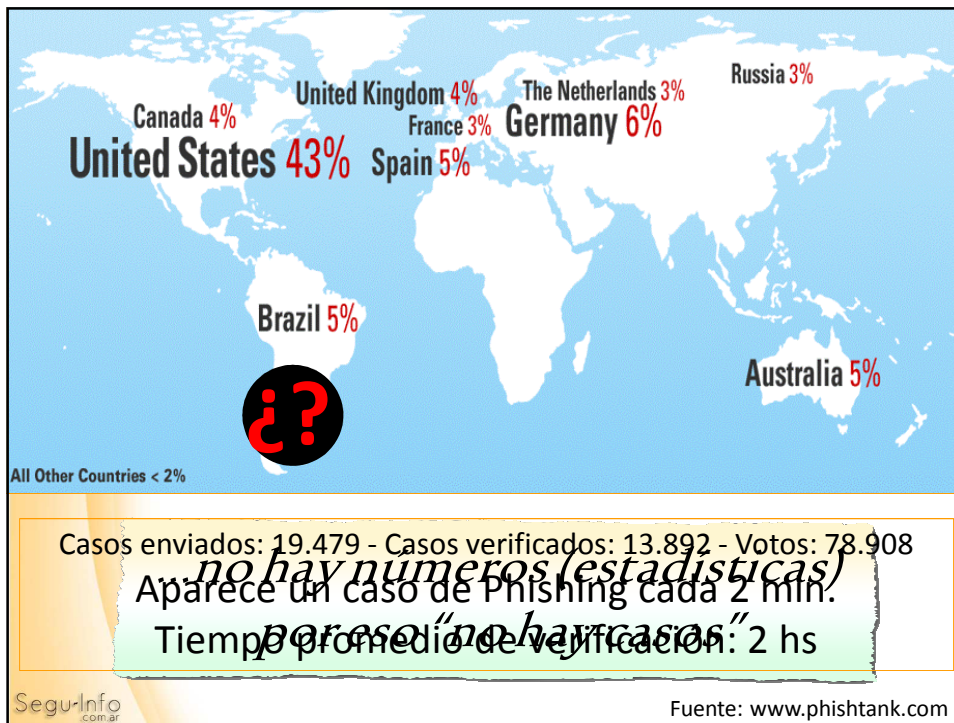
"El responsable de los datos debe adoptar las medidas para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no..."

```

[ ] .218:443 - Printable info leaked. SL: fFqBm;all:pe
l, application/vnd.ms-powerpoint, application/msword, /*Referer:
s/reportes.doAccept-Language: es-ARUser-Agent: Mozilla/4.0 (compat
LCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729;
ateHost: ebanking.banco.com.arConnection: Keep-AliveCooki
EsWe{z8^r$+4D91441B36066563B16F-F8AB9j1;[xjno-cacheCookie: JSESSION
&password= Sir=IngresarQ\<03eYnta0rigen=&id0bjetc
Name=veps&refreshList=&form=form0{Ju\=%24view.objetosrz+yZaAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

```

Segu-Info.com.ar



https://servicios1.afip.gov.ar/clavefiscal/aceptabiometricos/frmDatosBiometricos... AFIP - Administración Fed...

Aceptación de Datos Biométricos

Bienvenido Usuario SUSANA [014-7]

www.finanzas.gov.ar/fondorh/iconos/a.php

Hacked by [redacted] & [redacted]

Seguir a @

Si te dicen, "alto en nombre de la ley". Corre en nombre de la libertad.

Subida ROBO COI

miércoles, 01 de mayo de 2013

mayo de 2013						
do	lu	ma	mi	ju	vi	sá
28	29	30	31	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	1

MANDRI... AR, administrac... otana.com.ar

SURRA... BERTO, administ... n@dlagos.com..

Mato S... n Eduardo, api-... pi-rio.com.ar... stracion@edfan..

Schwar... Damian, adminis... ion@isladeles...

Segu-Info.com.ar



*Hay dos tipos de compañías: aquellas
 "Mienten un fábulo de sus servicios
 no auxiliares en el desarrollo"*

PODER JU
 REPÚBL
 Excmo. Cáb

Google site:gov.ar "cheap viagra"

diniece.me.gov.ar/index.php?option=

www.argentina.gov.ar

www.argentina.gov.ar

La conexión ha sido reiniciada

La conexión al servidor fue reiniciada mientras la página se cargaba.

- El sitio podría estar no disponible temporalmente o demasiado ocupado. Vuelva a intentarlo en unos momentos.
- Si no puede cargar ninguna página, compruebe la conexión de red de su equipo.
- Si su equipo o red están protegidos por un cortafuegos o proxy, asegúrese de que Firefox tiene permiso para acceder a la web.

Reintentar

senado.gov.ar DOWN OR NOT?

SENADO.GOV.AR IS DOWN!

“Nuevas aplicaciones para la fibra de lana” volvió a Chos Malal

``

SeguInfo.com.ar

http://www.master-consultas.com.ar/

SOCIOS • COMERCIOS • EMPRESAS
CONSULTAS POR EMAIL • SEGURIDAD • SALIR

Martes 19 de Abril de 2011

Rellene el formulario
Al registrarse, deberá proveer datos personales de la tarjeta y su resumen de cuenta, por lo tanto le recomendamos tener a la vista esta información.

> **Por favor complete la siguiente información:**

Ingresar Nombre de Usuario:	<input type="text"/>
Ingresar Contraseña:	<input type="password"/>
Número de Tarjeta:	<input type="text"/> - <input type="text"/> - <input type="text"/>
Fecha de Expiración:	04 - 2011
Código de Seguridad Cvv (3 digitos):	<input type="text"/>

También puede comunicarse a los siguientes teléfonos:
Argentina: (011) 4348-7000 las 24 horas.
Uruguay: (02) 902 4900 de Lun. a Vie. de 9 a 21 Hs.

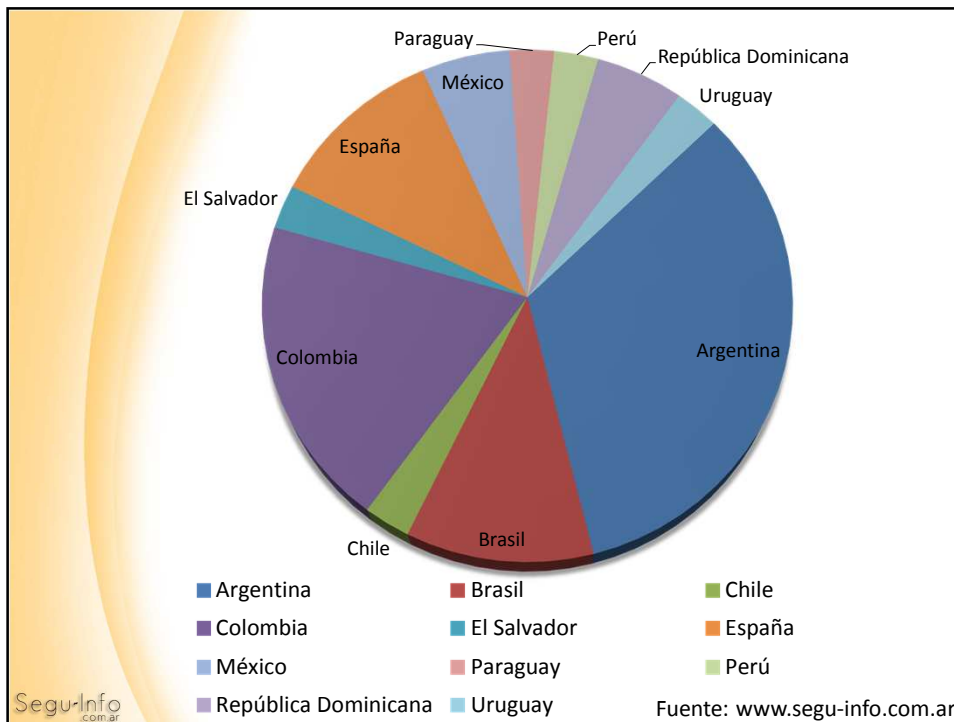
[CONTINUAR >>](#) [¿NECESITA AYUDA? ?](#)

Sugerencia: Presione Tab para pasar de un campo al siguiente

Visite: www.masterconsultas.com.ar | www.masterconsultas.com.uy

Segu-Info.com.ar

First Data Cono Sur S.R.L. Todos los derechos reservados. Se recomienda utilizar Internet Explorer 5.5 o superior, Netscape 4.9 o superior, Firefox 1.0 superior, Opera 5.02 o superior configurando su navegador con soporte para cookies, Java y JavaScript. Operar con MasterConsultas implica aceptar los Términos y Condiciones en los que se funda.



El 85% de las organizaciones han sufrido fugas de información por parte de sus empleados, clientes o proveedores en los últimos dos años

Ponemon Institute

...el 100% de las organizaciones ha perdido información, pero aún no lo saben

Segu-Info
com.ar

www.mercadolibre.com/pla/maileaser.php

onde co...

mercado Libre

Registración Preguntas Home **Vender** Mi Cuenta Mapa del Sitio Entrar

Navegar Vender Buscar Mi MercadoLibre MercadoPago Comunidad Ayuda

Buscar: Ir

Ingresar a MercadoLibre [Ayuda](#)

Coloca tu apodo o e-mail y tu clave para ingresar

Apodo o e-mail:

Clave:

Continuar

¿No estás registrado?

Para comprar y vender debes estar registrado ¡Hazlo ahora!

Regístrate

Recuerda que tu clave es confidencial y que MercadoLibre NUNCA solicita datos de cuenta, clave o de medios de pago vía e-mail.

Recuerda confirmar luego tu registración desde tu casilla de e-mail.

Segu-Info
com.ar

Stream Content

```

POST /ProtocolGw/protocol/commands HTTP/1.1
Accept: application/json
Content-Type: application/json
Content-Length: 626
Host: www. webmobile.com
Connection: Keep-Alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)

{"initiationType":"schedule","needsSpecificParameters":true,"applicationDetails":
{"applicationId":"325842966#752469853","build":
{"brand":"generic","device":"generic","manufacturer":"unknown","model":"sdk","versionRelease":
"4.0.4","versionSDKInt":15,"deviceId":"0000000000000000","displayMetrics":
{"density":1.5,"densityDpi":240,"heightPixels":800,"scaledDensity":1.5,"widthPixels":480,
"xdpi":240.0,"ydpi":240.0},"locale":"en-US","protocolVersion":"0.0.2","userAgent":"Mozilla
a/5.0 (Linux; U; Android 4.0.4; en-us; sdk Build/MRI) AppleWebKit/534.30 (KHTML, like
Gecko) Version/4.0 Mobile Safari/534.30","userId":"NOT IN USE!!!"}}HTTP/1.1 200 OK
Content-Type: application/json
Date: Tue, 08 May 2012 14:58:11 GMT
Server: Apache-Coyote/1.1
Content-Length: 177
Accept-Ranges: bytes
Cache-Control: no-store
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
x-cdn: Served by Cotendo - dynamic
Connection: Keep-Alive

{"commands":[{"id":"44e82092-ed1c-4354-8156-
f088a6b3192f","parameters":null,"command":"TERMINATE"}
],"commandsInterval":259200,"parameters":{"abTest":null,"validResponse":true}]
    
```

Segu-Info.com.ar

com.ar

Usuario:
 Contraseña:

```

<form action="/First.htm" method="post" target="_parent"
<table border="0" width="30%">
<tr>
    
```

Segu-Info.com.ar

Modulo Control Temperatura Camaras / Heladeras / Freezer

- Modulo Control Ambiente Deposito Drogueria y ANMAT
- Modulo Control Temperatura Heladeras
- Modulo Control Temperatura Camaras / Heladeras / Freezer**
- Modulo Control Temperatura Freezer Varios
- Modulo Control Ambiente Alto Costo

7.5 °C
2.5 °C
10.0 °C
-35.0 °C
7.5 °C
2.5 °C
7.5 °C
2.5 °C

Alarmas Activas
21/11/2011 09:48:47
Más...

Heladera 2 Puertas: 5.1 °C
Preparación: -16.4 °C
Freezer Tapa Vidrio: °C
Camara Secundaria: 4.2 °C
Camara Principal: 2.8 °C

Segu-Info.com.ar

Se desea actualizar e integrar sistemas antiguos con instalaciones modernas y... ¡se los conecta a Internet!

LOCATION

HOME MESSAGE NETWORK LOCATION About SCADA

Last Update
Upstream Downstream

Last Update
Upstream

Last Update
Upstream Downstream

Last Update
Upstream

Last Update
Upstream Downstream

Last Update
Upstream Downstream

Last Update
Upstream Downstream

Segu-Info.com.ar

WEB Scada

Measurement Counters Events Alarms **Parameters**

Controller Configuration		Electrical Parameters			
LCD Contrast []	39	Set	Mains Voltage High [V]	200	Set
Screen Scroll Timer [sec.]	10	Set	Mains Volt.FailTimer [sec.]	1	Set
Language Selection []	0	Set	Instant MainsDropOut [s]	0.0	Set
Genset Default Disp. []	0	Set	Mains Frequency Low [Hz]	100	Set
Status PromptsEnable	0	Set	Mains Frequency High [Hz]	100	Set
Fault Holdoff Timer [sec.]	20	Set	Mains Freq.FailTimer [sec.]	1	Set
Alarm Relay Timer [sec.]	60	Set	Load Shedding LowLim [kW]	0	Set
Intermittent Alm Rly	0	Set	Load SheddingHighLim [kW]	0	Set
SMS Enable	0	Set	Load Add Delay [sec.]	0	Set
GPRS Connection En.	1	Set	Engine Parameters		
Web Programming En.	1	Set	Engine Start Delay [sec.]	1	Set
Web Control Enable	1	Set	Preheat Timer [sec.]	0	Set
			Engine Heating Timer [sec.]	4	Set

SeguInfo.com.ar





Análisis de seguridad

Se siguen los mismos pasos que podría seguir un atacante real pero con un contrato de servicio. Se entrega un informe de lo hallado y recomendaciones

Penetration Test: identificación de servicios disponibles y vulnerabilidades en los sistemas

Ethical Hacking: el objetivo es más amplio y se analiza el todo del sistema de información (factor humano + técnico + físico)

Segu-Info
com.ar

Nuevo Código Penal

ART. 123.- Acceso ilegítimo a información

1. Será reprimido con multa de 10 a 100 días, el que a sabiendas accediere por cualquier medio, sin autorización, a un sistema o dato informático de acceso restringido

2. La pena será de 6 meses a 2 años de prisión cuando el acceso fuere en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos, de salud o financieros. Si el hecho se cometiere con el fin de obtener información sensible a la defensa nacional, el máximo de la pena de prisión se elevará a 4 años

Segu-Info
com.ar

Nuevo Código Penal

3. Será penado con prisión de 6 meses a 2 años el que:

a) A sabiendas y violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales

...

d) Mediante cualquier ardid o engaño determinare a otro a proveer datos personales, financieros o confidenciales

...

f) Utilizare la identidad de una persona física o jurídica que no le perteneciere, a través de cualquier medio electrónico, con el propósito de causar perjuicio

Segu-Info
com.ar

Conclusiones (I)


- Si un atacante es capaz de infiltrarse en la red, tendrá "la suerte" de visualizar y controlar todas las fuentes de información
- Los ataques no se limitan a robar información financiera
- Es obligatorio realizar análisis de riesgos
- Realizar auditorias de seguridad *-Ethical Hacking y Penetration Test-* para conocer el estado de la seguridad y las recomendaciones

Segu-Info
com.ar

Conclusiones (II)

- Anualmente se pierden millones de \$ por falta de previsión y protección
- La información es un activo que puede valuarse, conocerse y clasificarse
- Existen controles que deben ser implementados para conservar la CID de la información y evitar su fuga
- Es necesario legislar adecuadamente los "viejos" delitos que utilizan las "nuevas"

Segu-Info.com.ar tecnologías



[Sobre nosotros](#)
[Servicios](#)
[Denunciar](#)
[Contacto](#)

BUSCAR PHISHING ACTIVOS

Palabra clave:

Entidad: Todas las entidades

Período: Días

¿Recibió un correo sospechoso?
 ¿Cree que puede ser Phishing?
¡DENÚNCIELO!

ÚLTIMOS CASOS DE PHISHING REPORTADOS

Sólo se muestran los últimos 4 casos. Contáctese con nosotros para mayor información

Entidad	Dominio y URL	Fecha
PayPal	http://[flashyreview.[DOMINIO.TLD]/www.paypal.[DOMINIO.TLD]/us/cgi-bin/webscr.htm?cmd=_login-run	02/05 - 18:53:48
Google	https://docs.[DOMINIO.TLD]/spreadsheet/viewform?formkey=dGVvcTlsbzlCcUtdR0FudGtKRvJzNGc6MQ	02/05 - 18:50:24
PayPal	http://paypal.[DOMINIO.TLD]/ID-Number-PP-001-230-377-124/b064ef76cedf78645ba5940d19821f03/	02/05 - 18:49:44
PayPal	http://gogiveblood.[DOMINIO.TLD]/httpd.www.paypal.[DOMINIO.TLD]/us/cgi-bin/webscr.htm	02/05 - 18:41:26

[Ver más casos](#)

SERVICIOS

AyRO: seguimiento y baja de casos de Phishing; detección en forma temprana de incidentes que atentan contra la reputación de su organización.

EDUCACIÓN

Capacitación, concientización y entrenamiento de la organización sobre delitos informáticos.

[Conocer más...](#)

2-05-12

PHISHING A VISA EN MÚLTIPLES DOMINIOS

Varios usuarios nos han reportado nuevos casos de Phishing a VISA que utilizan varios dominios vulnerados para robar las credenciales del usuario y sus datos de tarjetas de crédito. El correo electrónico que llega al usuario es el clásico engaño: Si el usuario hace clic sobre el enlace ingresará al primer sitio...

[Continuar leyendo...](#)

Antiphishing.com.ar | [En un entorno seguro de Root-Secure](#) | [Segu-Info](#) | [Aviso Legal](#) y [Política de Privacidad](#)


CRUZADA POR LA
IDENTIDAD DIGITAL
PROYECTOS S-1312/12 Y S-2257/11
ARGENTINA 2012

[Cruzada](#) [Proyectos](#) [Id.Digital](#) [Noticias](#)



CRUZADA POR LA
IDENTIDAD DIGITAL
PROYECTOS S-1312/12 Y S-2257/11
ARGENTINA 2012


SEGU-INFO
CONSULTORÍA Y EDUCACIÓN EN
SEGURIDAD DE LA INFORMACIÓN

RED IBEROAMERICANA
ELDERECHOInformático.com
Asesoría en Derecho Informático y Seguridad de la Información

En vistas del incremento exponencial de los casos de Suplantación de Identidad Digital y Phishing, [Segu-Info](#) y [La Red El Derecho Informático](#) se han unido para generar la Primera **Cruzada por la Identidad Digital - Argentina 2012**.


La Cruzada posee como bases dos Proyectos de Ley presentados ante el Senado de la Nación, impulsados por la **Senadora Nacional María de los Ángeles Higonet** y el **Senador Nacional Carlos Verna**.

En la redacción y detalles de ambos proyectos han participado el **Abog. Marcelo Temperini** y el **Lic. Cristian Borghello**, junto al equipo de asesores de la Senadora Higonet, desde donde se busca avanzar hacia un mejor y más adecuado marco legal para combatir el cibercrimen en Argentina.


El primero de los proyectos fue presentado bajo el **N° de Expediente S-2257/11 - Proyecto de Ley para tipificar el Phishing o Captación Ilegítima de Datos**, ingresado en fecha 19 de Septiembre de 2011 y desde el cual se busca combatir las diferentes técnicas de obtención ilegítima de información personal.

<http://cruzada.elderechoinformatico.com>





Pensar *“a mí no me va a pasar”*
es el principio del fracaso



Agradecimientos

A la Comunidad de [Segu-Info](http://www.segu-info.com.ar)
que todos los días [nos] aporta
conocimiento a través de los
distintos grupos de discusión

Lic. Cristian Borghello, CISSP – CSSK – MVP

www.segu-info.com.ar

info@segu-info.com.ar

@SeguInfo

