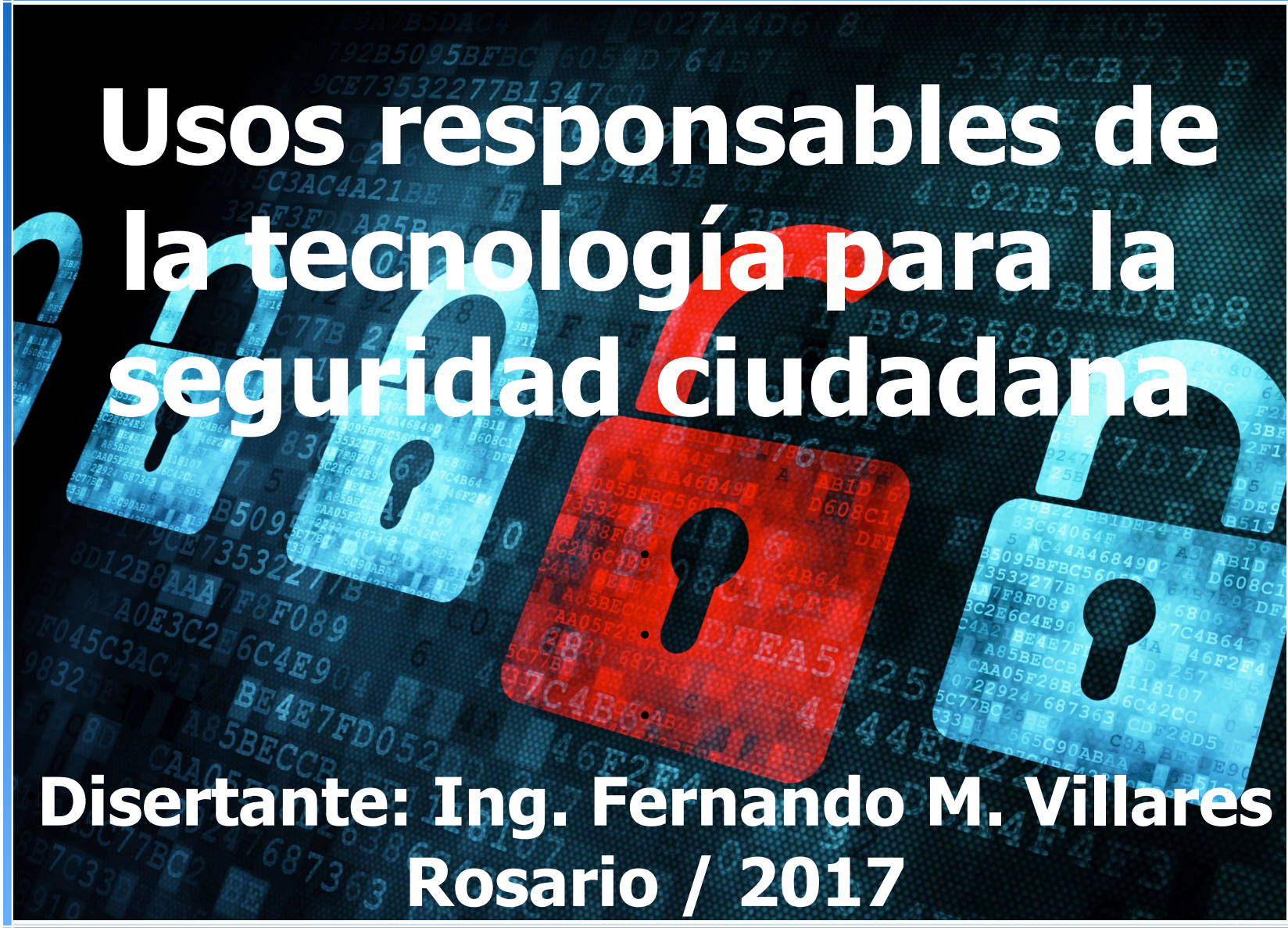
Usos responsables de la tecnología para la seguridad ciudadana



Disertante: Ing. Fernando M. Villares

Rosario / 2017

Glosario Previo

- **Cracking**: Figura cuya conducta típica consiste en acceder a sistemas informáticos de forma no autorizada, y con una finalidad clara: menoscabar la integridad, disponibilidad y acceso a la información del sistema.

- El cracking **IMPLICA** por definición la concreción de un **DELITO**

Glosario Previo

- **Delitos informáticos:** Ciber-crimen, o ciber-delicuencia es toda aquella acción, típica, anti-jurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Debido a que la informática se mueve más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como delito, según la "Teoría del delito", por lo cual se definen como abusos informáticos, y parte de la criminalidad informática y sobre todo cuando se viola un sistema.

Glosario Previo

- **Grooming:** Acoso o acercamiento a un menor ejercido por un adulto con fines sexuales. Concretamente, se refiere a acciones realizadas deliberadamente para establecer una relación y un control emocional sobre un niño o niña con el fin de preparar el terreno para el abuso sexual del menor, incluyéndose en este desde el contacto físico hasta las relaciones virtuales y la obtención de pornografía infantil.

Glosario Previo

- **Sexting:** es un anglicismo que se refiere al envío de mensajes sexuales (eróticos o pornográficos), por medio de teléfonos móviles. Inicialmente hacía referencia únicamente al envío de SMS de naturaleza sexual, pero después comenzó a aludir también al envío de material pornográfico (fotos y videos) a través de teléfonos celulares y computadoras.

Glosario Previo

- **Pornovenganza:** Contenido sexual explícito que se publica en internet sin el consentimiento del individuo que aparece representado. Realizado tanto por exparejas como por desconocidos con acceso no autorizado a imágenes y grabaciones íntimas de la víctima. Muchas de las fotografías son tomadas por las propias personas que aparecen en ella. El contenido suele ir acompañado de información personal, enlaces a sus perfiles, etc. Se considera violencia sexual y/o de género.

Glosario Previo

- **MALWARE:** También llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario. El término virus informático suele aplicarse de forma incorrecta para referirse a todos los tipos de malware, incluidos los virus verdaderos

Glosario Previo

- **PHISHING:** Estafa cometida a través de medios informáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc) de forma fraudulenta.

- El estafador o phisher **suplanta la identidad** de una persona o empresa de confianza para que el receptor de una comunicación electrónica aparentemente oficial (vía e-mail, fax, sms o telefónicamente) crea en su veracidad y facilite, de este modo, los datos privados que resultan de interés para el estafador.

Glosario Previo

- **Defacement/Defacing:** es una palabra inglesa que significa desfiguración y es un término usado en informática para hacer referencia a la deformación o cambio producido de manera intencionada en una página web por un atacante que haya obtenido algún tipo de acceso a ella, bien por algún error de programación de la página, por algún bug en el propio servidor o por una mala administración de este. El autor de un defacement se denomina defacer.

Glosario Previo

- **SPAM:** Correo no deseado recibido por el destinatario, procedente de un envío automatizado y masivo por parte del emisor. El spam generalmente se asocia al correo electrónico personal, pero no sólo afecta a los correos electrónicos personales, sino también a foros, blogs y grupos de noticias.

Glosario Previo

- **SUPLANTACIÓN DE IDENTIDAD:**

Ocurre cuando una parte adquiere, transfiere, posee o utiliza información personal de una persona física o jurídica de forma no autorizada, con la intención de cometer fraude u otros delitos relacionados. También es conocido como Robo de identidad.

Glosario Previo

- **Eavesdropping:** Término utilizado para referirse a escuchar secretamente, se ha utilizado tradicionalmente en ámbitos relacionados con la seguridad, como escuchar llamadas telefónicas. Se ha convertido en parte de la jerga habitual en criptografía y se refiere a ataques de escuchas, tanto sobre medios con información cifrada, como no cifrada.

Glosario Previo

- **Tampering:** Término referido a diversas formas de sabotaje, normalmente referido a modificaciones de forma intencional a diversos productos de forma que pudieran causar algun tipo de daño o perjuicio al consumidor.

Ej: celulares chinos con badware / pendrives con firmwares alterados, Red Stuxnet

Glosario Previo

- **Botnet:** es un término que hace referencia a un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota.
- **DDoS:** Ataque de denegación de servicio distribuido, el cual se lleva a cabo generando un gran flujo de información desde varios puntos de conexión.

Glosario Previo

- **Zero Day Attack/Exploit:** Es un ataque contra una aplicación o sistema que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de vulnerabilidades que, por lo general, son desconocidas para la gente y el fabricante del producto.
- **CVE:** Lista de información registrada sobre vulnerabilidades reportadas de seguridad, donde cada referencia tiene un número de identificación único.

Glosario Previo

- **Cifrado:** Conjunto de métodos que permiten aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para decodificarlo.

- **Esteganografía:** estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia.

Glosario Previo

- **Hacker:** Todo individuo que se dedica a programar de forma entusiasta, o sea un experto entusiasta de cualquier tipo, que considera que poner la información y el conocimiento al alcance de todos constituye un extraordinario bien.

  Ej: Leonardo Da Vinci...

Glosario Previo

- **Virus:** Tipo de malware que tiene por objetivo alterar el funcionamiento normal del ordenador, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo producen molestias.

Glosario Previo

- **Ransomware:** Tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate.

Glosario Previo

- **Internet Profunda:** Se conoce también con otros nombres como deep web, dark web, internet invisible o internet oculta, al contenido de internet que no es indexado por los motores de búsqueda convencionales, debido a diversos factores. Normalmente se accede a ella a través de accesos cifrados anónimos como ToR, i2p, FreeNet, Riffle, etc.

El puntapié inicial hacia una noción de seguridad.

- ¿Han sufrido o conocen sobre algún tipo de ataque o acoso por medios electrónicos ?
- ¿Desde donde espero recibir un ataque?
- ¿Sus comunicaciones son SEGURAS?
  - ¿Es segura su información privada?
  - ¿Qué conoce ud. de su información pública?
- Análisis Inicial:
  - ¿Sabemos algo?
  - ¿Podemos hacer algo al respecto?

Formas de obtener información personal y OSINT

- ✔ **Los usuarios**
- ✔ **Los dispositivos**
- ✔ **Los canales de comunicación**
- ✔ **Las redes sociales**
- ✔ **Venta de datos**
- ✔ **INTERNET (datos públicos)**

El presente, nuestro mayor problema...

Formas de prevención o mitigación de daños.

- ✔ **Contraseñas fuertes y diferentes para cada servicio, uso de gestores para administrar su complejidad creciente.**
- ✔ **Uso de software libre vs. Software privativo.**
- ✔ **Uso de email cifrado, pdf con claves, navegadores web con bloqueos de publicidad y privacidad.**
- ✔ **NO ejecutar o UTILIZAR SOFTWARE proveniente de DUDOSAS FUENTES o ilegal.**
- ✔ **Jamas compartir pendrives o dispositivos en computadoras que no sean de confianza, no utilizar servicios sensibles en redes públicas.**

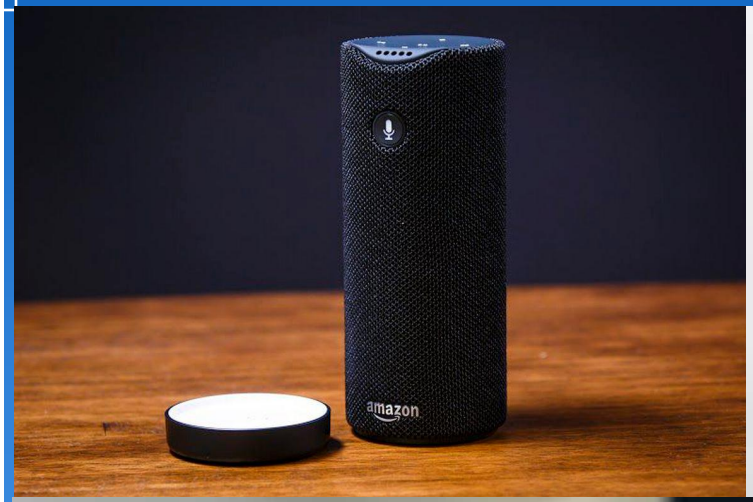
Formas de prevención o mitigación de daños.

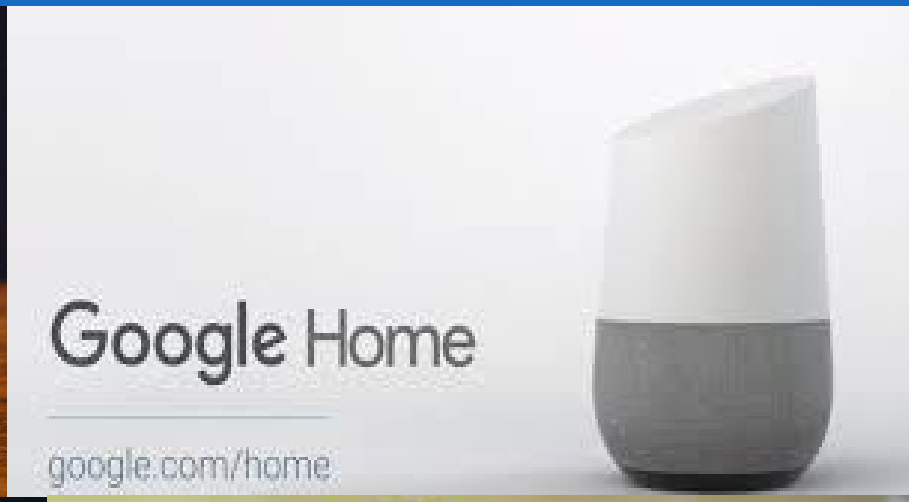
- ✔ **Tener backups de forma regular y permanente de su información sensible.**
- ✔ **Proteger su información y PC mas sensibles con cifrado de discos, revisar periódicamente las claves y accesos de wifi y a la red, actualizar los dispositivos electrónicos (IoT).**
- ✔ **CUIDADO con la información que se comparte por redes sociales, chats de whats app, telegram, o almacenamiento en la nube como dropbox, etc.**
- ✔ **Siempre tener actualizados los Sistemas Operativos, TODAS las aplicaciones que se usen regularmente y el antivirus en caso de usar celulares Android(r) y SO Windows(r)**

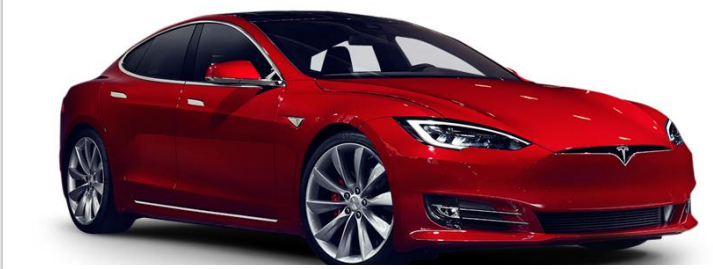
El futuro…

- ✔ **TODO posee una computadora HOY en DÍA…lamentablemente el hecho de decir, yo soy de otra generación, no me interesa aprender, la computación no es lo mio etc., va a generar en el corto plazo una generación de analfabetos digitales segregados y en riesgo en la actual sociedad digital.**
- ✔ **El software privativo debe ser evitado ya que al no saber que hace exactamente pone en riesgo a toda la sociedad (obsolescencia programada, vigilancia masiva, soberanía tecnológica).**

1984 = IA + BIG DATA en las actividades diarias...







BIBLIOGRAFÍA CONSULTADA

- *Internet Engineering Task Force - www.ietf.org)*
- *Seguridad en Voip - Saúl Ibarra Corretgé - www.saghul.net*
- *Blog Segu Info – Christian Borghello– www.segu-info.com.ar*
- *Observ. Del. Inf. LatAm - www.odila.org*
- *Wikipedia – es.wikipédia.org*
- *Antisec Security – antisec-security.blogspot.com.ar*
- *Tor Project – www.torproject.org*
- *Defensa personal del email – emailselfdefense.fsf.org/es/*
- *Free Software Foundation - https://www.fsf.org/es*
- *Open VPN Software - https://openvpn.net/*
- *Libre office suite - https://es.libreoffice.org/*
- *Ubuntu GNU LINUX http://www.ubuntu.com/*
- *Foxit PDF reader - www.foxitsoftware.com/products/pdf-reader/*
- *Common vulnerabilities and Exposures - https://cve.mitre.org/*

¡GRACIAS POR SU PARTICIPACIÓN!

[IN] telix
Ingenieria & Telecomunicaciones

Autor: Ing. Fernando M. Villares Terán - 2017

Consultas: contacto@intelix.com.ar
www.intelix.com.ar