

**CONCEPTOS DE CIBERSEGURIDAD**

FUERZA AÉREA ARGENTINA – JORNADA DE CONCIENTIZACION EN CIBERSEGURIDAD

[www.ba-csirt.gob.ar](http://www.ba-csirt.gob.ar)



**BA-CSIRT**

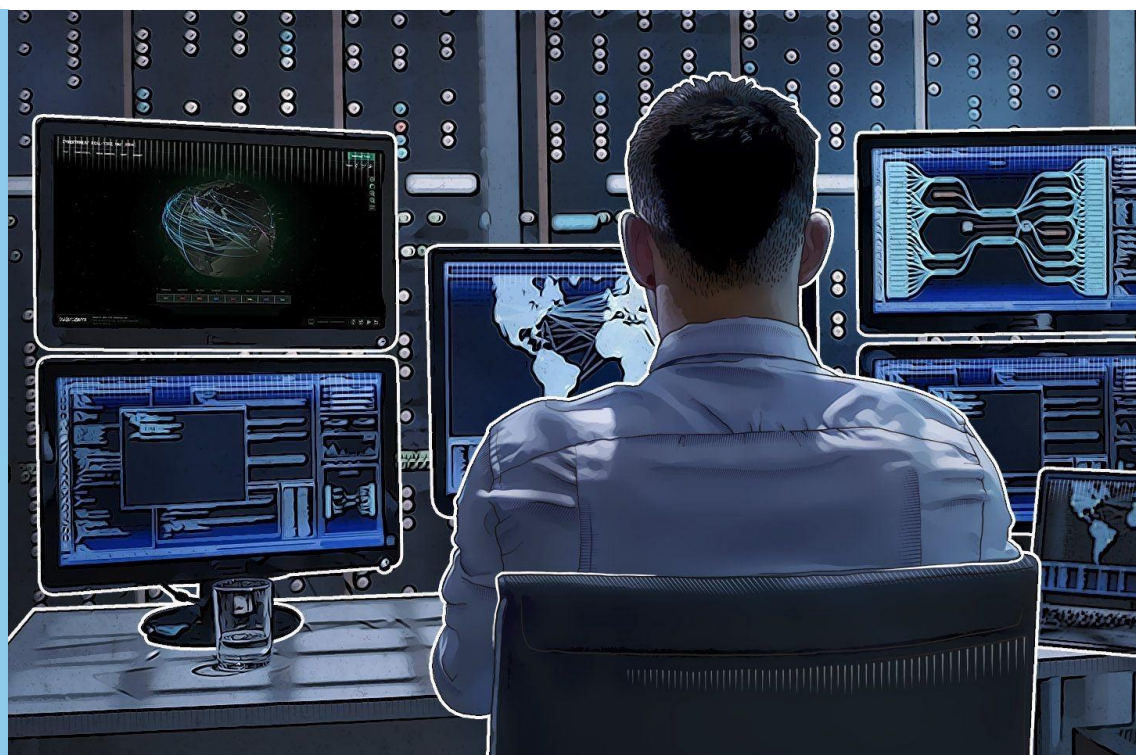
**CHARLAS DE CONCIENTIZACIÓN**

# BA-CSIRT | CENTRO DE CIBERSEGURIDAD

SOBRE NOSOTROS

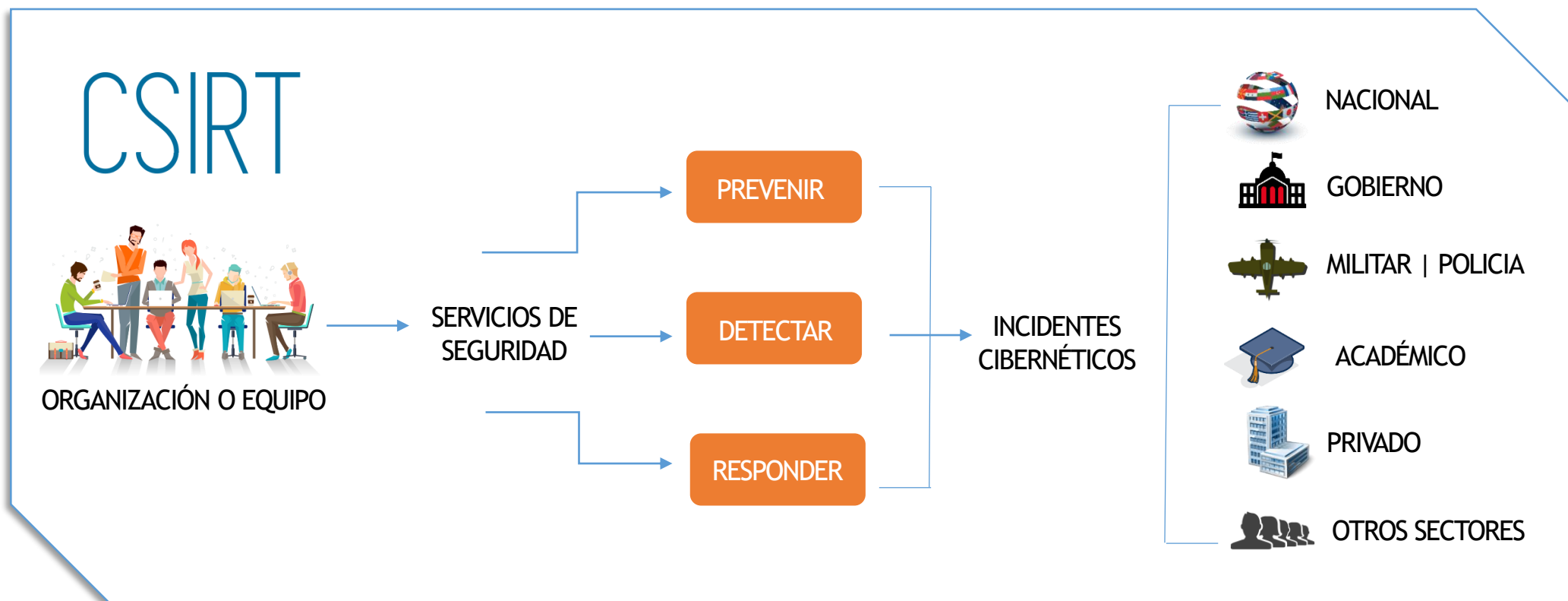
## QUIÉNES SOMOS

El BA-CSIRT es un centro de expertos en ciberseguridad, que se dedica a **ASISTIR** y **CONCIENTIZAR** a los **CIUDADANOS** y al Gobierno de la Ciudad en todo lo relacionado a la seguridad de la información. En tal sentido ofrece a la comunidad un referente al cual acudir ante incidentes de seguridad.



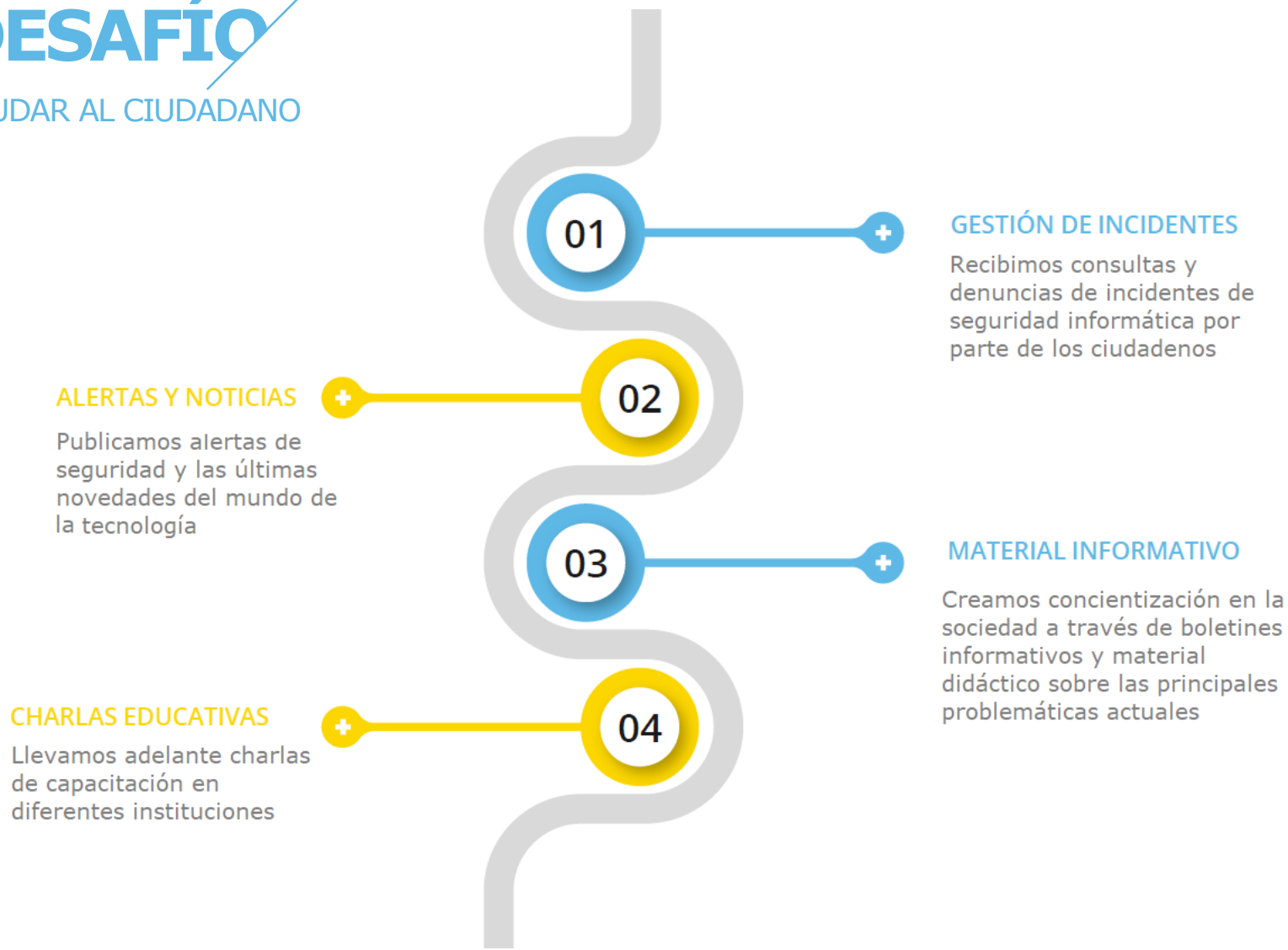
# QUÉ ES UN CSIRT?

COMPUTER SECURITY INCIDENT RESPONSE TEAM



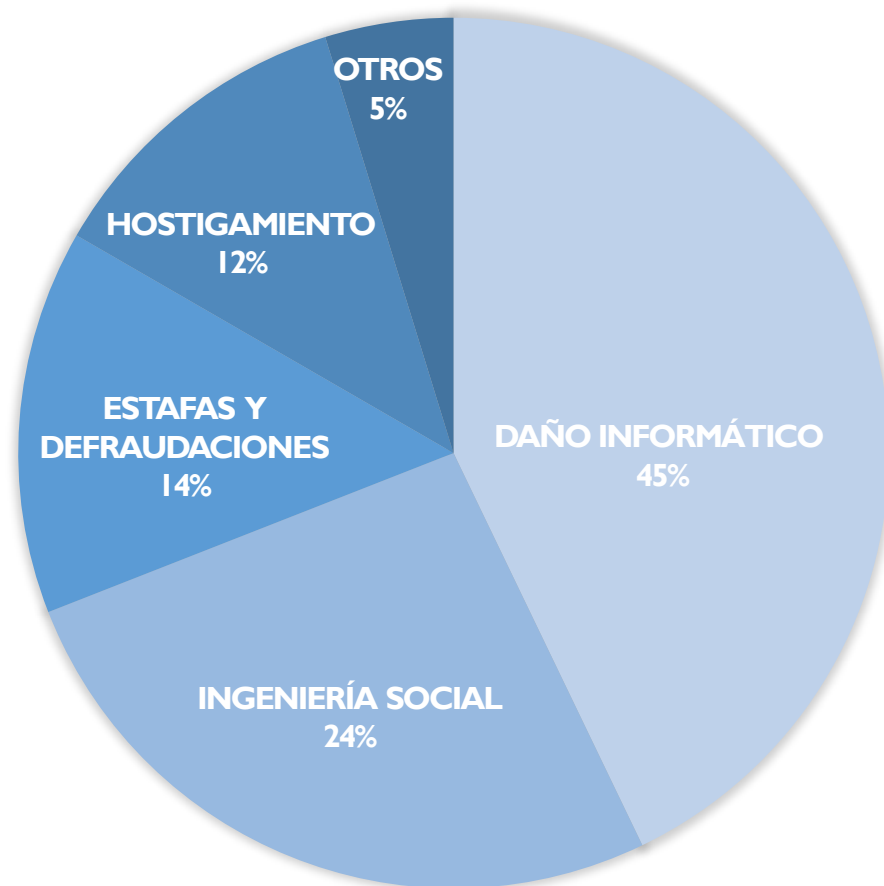
# EL DESAFÍO

CÓMO AYUDAR AL CIUDADANO



# CASOS QUE SE REPORTAN

INCIDENTES DE SEGURIDAD INFORMÁTICA



— **CONCEPTOS DE CIBERSEGURIDAD**

FAA – JORNADA DE CONCIENTIZACION EN CIBERSEGURIDAD

— **BA-CSIRT**

**RIESGOS EN LAS REDES SOCIALES**

# HOSTIGAMIENTO

RIESGOS DE LAS TICS



## NIÑOS

- Acoso digital
- Cyberbullying
- Grooming
- Pornografía infantil



## ADOLESCENTES

- Acoso digital
- Cyberbullying
- Grooming
- Sextorsión / Pornovenganza
- Suplantación de identidad



## ADULTOS

- Acoso digital
- Sextorsión / Pornovenganza
- Suplantación de identidad



# ACOSO DIGITAL

## QUÉ ES



- Uso de las redes sociales, teléfonos celulares u otros dispositivos de comunicación, que suele suceder entre dos personas que poseen una relación, para manipular y controlar con algunas acciones.
- Ejemplos:
  - ✓ Enviar muchos mensajes de texto al día.
  - ✓ Hacer presión para obtener información, como las contraseñas de la otra persona (para poder saber qué hace) y fotos íntimas.
  - ✓ Forzar a la otra persona de ser amigo de algunas otras.
  - ✓ Difamar mentiras, suplantar a alguien e incluso recurrir al chantaje.



## CONCEPTOS DE CIBERSEGURIDAD

FAA – JORNADA DE CONCIENTIZACION EN CIBERSEGURIDAD

CYBERBULLING (INTENCION DE DAÑAR / AGREDIR A UNA PERSONA POR REDES SOCIALES)



Nacional **Colegios: 82% de las denuncias por cyberbullying afecta a mujeres**

MUNDO 26-05-2018 12:59 **Víctima de bullying se suicidó en baño de famosa cafetería**

La joven de apenas 16 años apareció sin vida y con una carta dirigida a sus padres. No tenía signos de violencia, aunque esperan los resultados de la autopsia.

LEY 1.472 - Código Contravencional de la Ciudad Autónoma de Buenos Aires

Art. 52 y Art. 53

DE UNO (1) A CINCO (5) DÍAS DE TRABAJO DE UTILIDAD PÚBLICA, MULTA DE DOSCIENTOS (\$ 200) A UN MIL (\$ 1.000) PESOS O UNO (1) A CINCO (5) DÍAS DE ARRESTO.

# CIBERBULLYING

## HOSTIGAMIENTO



### **CIBERBULLYING:**

Publicación de textos, imágenes, videos y/o audios a través de medios electrónicos, como el correo electrónico, la mensajería instantánea, las redes sociales, los juegos online, utilizada para agredir / humillar a alguien.

### **\*/ FORMAS / \***

- **HOSTIGAMIENTO**  
Envío de imágenes denigrantes, seguimiento a través de las redes sociales, etc.
- **EXCLUSIÓN**  
Denegación a la víctima del acceso a foros, chats o plataformas sociales.
- **MANIPULACIÓN**  
Uso de información de redes sociales para modificarla y difundirla fuera del contexto en el que se la encontró.

### **\*/ CARACTERÍSTICAS / \***

- **VIRALIZACIÓN**
  - No se tiene conciencia sobre el alcance de la publicación.
  - Se pierde control sobre quién comparte o guarda la información.
  - Se expande a un número incierto de personas que tienen acceso.
- **FALSA SENSACIÓN DE ANONIMATO**
  - La falsa sensación de anonimato genera también una falsa sensación de minimización de la agresión, provocando que muchas personas puedan sumarse como agresores.
- **DIVERSOS DISPOSITIVOS PARA EL HOSTIGAMIENTO**
  - Los medios de propagación se combinan, multiplicando los canales de difusión.
- **NO HAY REGISTRO DEL IMPACTO EN EL OTRO**
  - Se desconoce el impacto inmediato del daño que genera en la víctima
  - Las redes sociales, la mensajería, impiden ver las reacciones del otro, lo que hace que la agresión se magnifique.
- **NO HAY DERECHO AL OLVIDO**
  - Por más de que se borre la información difamatoria publicada, si otra persona ya la guardó, comentó o compartió, ésta seguirá difundiéndose.

# CIBERBULLYING

SÍ ES

- Que suban fotos mías sin mi consentimiento para exponerme al ridículo.
- Que creen perfiles falsos con mi nombre.
- Que me amenacen de manera anónima.
- Que inventen falsos eventos y dejen en claro que a mí no me invitan.
- Que compartan fotos íntimas que hayan sido recibidas durante una relación.
- Que me provoquen en un juego para hacerme reaccionar de manera que el moderador me expulse del juego.



## CONCEPTOS DE CIBERSEGURIDAD

FAA – JORNADA DE CONCIENTIZACION EN CIBERSEGURIDAD

### GROOMING (CONTACTO A MENORES CON FINES SEXUALES)

#### Un maestro pedía por WhatsApp fotos porno a sus alumnas para no dejarles tarea

El padre de una joven de 16 años descubrió el chat entre su hija y el docente, que ya es buscado por las autoridades

#### El árbitro detenido por acosar a una niña tenía más de 2.500 mujeres en Facebook

El acusado utilizaba un perfil de la red social que era de su primo fallecido y con esa identidad, entablaba chats con adolescentes y mayores de edad. Ordenaron su prisión preventiva.

LA NACION | SOCIEDAD | ESCÁNDALO SEXUAL EN EL FÚTBOL

#### Crece el uso de WhatsApp para la captación de chicos sexuales

LEY 26.904

DE 6 MESES A 4 AÑOS AL QUE, POR MEDIO DE COMUNICACIONES ELECTRÓNICAS, CONTACTE A UN MENOR CON EL PROPÓSITO DE COMETER CUALQUIER DELITO CONTRA SU INTEGRIDAD SEXUAL

# GROOMING

HOSTIGAMIENTO



## GROOMING:

Acciones realizadas por un adulto con el fin de establecer una relación y un control emocional sobre una persona menor de edad con el propósito de cometer cualquier delito contra la integridad sexual de la misma



## \*/ FASES DEL ACOSO/ \*



### ▪ CONTACTO Y ACERCAMIENTO - AMISTAD

El acosador se vale de herramientas para mentir sobre su persona al entrar en contacto con el menor, buscando generar confianza y empatía.



### ▪ COMPONENTE SEXUAL - RELACIÓN

El acosador consigue que el menor le envíe alguna fotografía o video con componentes sexuales o eróticos.



### ▪ CIBERACOSO

Si el menor no accede a las demandas (más material, videos eróticos o encuentro personal), el acosador lo amenaza con difundir la imagen con mayor carga sexual que haya capturado y enviarla a los contactos personales del menor.

# REFORMA CÓDIGO PENAL

## La sola tenencia de pornografía infantil es delito

Antes sólo se penaba la producción y distribución.

### \*/ MODIFICACIONES ART.128 DEL CÓDIGO PENAL / \*



- **Reprimir con prisión de 3 a 6 años al que produzca, financie, ofrezca, comercie, publique o divulgue**, por cualquier medio, **toda representación de un menor de 18 años dedicado a actividades sexuales** explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organice espectáculos en vivo de representaciones sexuales explícitas en que participaren menores.
- **Reprimir con prisión de 4 meses a 1 año al que tenga en su poder representaciones** de las descriptas en el párrafo anterior.
- **Reprimir con prisión de 6 meses a 2 años al que tenga en su poder representaciones** de las descriptas en el primer párrafo **con fines de distribución o comercialización.**
- **Reprimir con prisión de un 1 mes a 3 años al que facilite el acceso a espectáculos pornográficos o suministre material pornográfico a menores de 14 años.**
- **Todas las escalas penales** previstas en este artículo **se elevan** en un tercio en su mínimo y en su máximo **cuando la víctima fuere menor de 13 años.**



DELITOS CON IMÁGENES DE PORNOGRAFÍA INFANTIL

Clarín.com · Policiales · 17/02/16

### Caen tres acusados de distribuir pornografía infantil por Internet

**Operativos en Olavarría y Lomas de Zamora** Un caso fue detectado por un organismo estadounidense. Involucra a padre e hijo. En el otro, el imputado es un enfermero.



Clarín.com · Policiales · 31/07/13

### Cayó un profesor que subía pornografía infantil a la Web

**EN RÍO CUARTO, CÓRDOBA** Daba clases de música en una academia a niños y adolescentes. Lo apresaron en un ciber.



ART. 128

DE 3 A 6 AÑOS POR PRODUCIR, OFRECER, PUBLICAR O DISTRIBUIR REPRESENTACIONES DE MENORES DE 4 MESES A 1 AÑO A QUIEN TENGA EN SU PODER ESTAS REPRESENTACIONES DE 6 MESES A 2 AÑOS SI HAY TENENCIA CON FINES DE DISTRIBUCIÓN O COMERCIALIZACIÓN



DELITO DE CORRUPCIÓN DE MENORES

Sábado 01 de Noviembre de 2014

### Dura condena por corrupción de menores a un analista de sistemas de Coronda

La Justicia comprobó que a las niñas las seducía, les pedía fotos de ellas posando desnudas y luego las extorsionaba con divulgarlas. Es un ex empleado del Mercado de Valores.

f FACEBOOK

TWITTER

COMENTAR

### ART. 125. CORRUPCIÓN DE MENORES

3 A 10 AÑOS PARA QUIEN PROMUEVA LA CORRUPCIÓN DE MENORES DE 18 AÑOS  
6 A 15 AÑOS CUANDO LA VÍCTIMA ES MENOR DE 13 AÑOS  
10 A 15 AÑOS, CUALQUIERA SEA LA EDAD DEL MENOR, CUANDO:

- HAYA UN ENGAÑO, VIOLENCIA, AMENAZA, ABUSO DE AUTORIDAD, INTIMIDACIÓN
- SI EL AUTOR ES ASCENDIENTE, HERMANO, TUTOR, PERSONA CONVIVIENTE O ENCARGADA DE SU EDUCACIÓN O GUARDA

Acusado. Nicolás Borra (a la derecha) el día que fue detenido en Santa Fe.

© 06/06/2013 - 18:49 | Clarin.com | Noticias

### DELITOS INFORMÁTICOS

### Condenaron a un pedófilo argentino por corromper a una nena de 9 años

En su perfil, se llamaba Sole, de 10 años. Pero tiene 26 y un tribunal de Necochea le dio diez años de cárcel. En su computadora hallaron vínculos con 70 chicos de todo el país y muchos videos perversos. España pidió que lo investiguen por participar de un foro de pedofilia.



# SEXTING Y PORNOVENGANZA

## HOSTIGAMIENTO



### SEXTING:

Intercambiar mensajes, fotos y videos de contenido sexual **de forma consentida**, a través de medios electrónicos, entre dos personas (ambos mayores o menores, respectivamente).

### PORNOVENGANZA:

Difusión de contenidos sexuales de una persona **con el objetivo de dañarla**.

### SEXTORSIÓN:

**Acto extorsivo** que amenaza con difundir material íntimo de una persona si la misma no accede a acatar las solicitudes del agresor.



- Existe otra persona implicada de la que se depende
- Las personas y las relaciones pueden cambiar
- La protección de la información no se puede garantizar
- La distribución de la información digital es incontrolable

# SHARENTING

CREANDO LA IDENTIDAD DIGITAL



## SHARENTING:

Conducta por parte de los padres o que consiste en la **publicación masiva de información y datos de los menores** en internet **sin el permisos de ellos**.

Esta conducta, pone en peligro diferentes factores de la vida del menor siendo el más importante su **privacidad**.

## \*/ RECOMENDACIONES / \*

### ▪ AJUSTES DE PRIVACIDAD

Controlar quién puede acceder a la información

### ▪ EVITAR CREARLES CUENTAS

Postear las fotos de los niños desde los perfiles de las cuentas de los padres.

### ▪ NO POSTEAR DESNUDOS

Ejemplos como bañándose, en la playa o de un recién nacido.

### ▪ NO FACILITAR DATOS

Evitar información sobre instituciones a las que asisten (colegio, club)

### ▪ PERMITIRLES NEGARSE

Permitir a los niños a negarse a compartir las fotos si puede decidir, consultarle y dejarlo opinar. La privacidad es un derecho personal.

# COMPRAS ONLINE

## ESTAFAS Y DEFRAUDACIONES



- 01 LAS FOTOS NO SON REALES**  
Ninguna de las publicaciones del vendedor tienen fotos reales de los productos
- 02 LA PUBLICACIÓN NO CUMPLE CON LAS NORMAS**  
Indica a los usuarios no realizar la compra mediante el sitio
- 03 EL VENDEDOR NO ES CONFIABLE**  
No posee suficientes ventas para mostrar su reputación en el sitio  
Ofrece el contacto para la transacción en la sección GARANTÍA

mercado libre

Nuevo  
**Apple Iphone X 64gb / 256 Gb Nuevos Caja Sellada Libres**  
\$ 24.000  
Págalo en hasta 12 cuotas  
VISA  
Más información  
Entrega a acordar con el vendedor  
Belgrano, Capital Federal  
Consultar costos  
Cantidad: 1

Más publicaciones del vendedor

\$ 5.500 Samsung Galaxy J7 Prime 16gb 3gb Ram...	\$ 9.000 Nikon D3200 D3400 D5300 D5500 Kit 18...	\$ 9.000 Playstation 4 Pp4 Pro 1 Tb 4k	\$ 40.000 Smart Tv Curvo 4k 65 Samsung Ju6700 Ultr...
---	---	---	--

Ver todas las publicaciones

**\*\*PROMO HASTA AGOTAR STOCK\*\***

**IMPORTANTE: NO OFERTAR EN ESTA PUBLICACIÓN**

TODOS PRODUCTOS SON NUEVOS EN CAJA SELLADA DE FÁBRICA. EMITIMOS FACTURAS A Y B.  
FORMAS DE PAGO ACEPTADAS: RAPIPAGO, PAGO FÁCIL, RED LINK Y PROVINCIA NET –EXCLUSIVAMENTE–  
ENVÍOS A TODO EL PAÍS POR CORREO ARGENTINO. ENVÍOS EN CABA Y GRAN BUENOS AIRES MEDIANTE SERVICIO DE CADETERÍA.  
TAMBIÉN SE PUEDE RETIRAR PERSONALMENTE POR NUESTRAS OFICINAS EN BELGRANO.

**IMPORTANTE: NO OFERTAR EN ESTA PUBLICACIÓN**

Ubicación: Belgrano, Capital Federal

Este vendedor aún no tiene suficientes ventas para calcular su reputación

Garantía  
Compra Protegida con Mercado Pago  
Recibir el producto que esperabas o te devolvemos tu dinero  
Garantía del vendedor  
1 año de Garantía Escrita + Garantía oficial del fabricante - avellanedainsumos4@gmail.com  
Conocer más sobre garantía

Medios de pago  
Tarjetas de crédito  
(Cuotas sin interés con bancos seleccionados)  
VISA, Mastercard, American Express, Diners Club  
Tarjetas de débito  
Visa Debit, Mastercard Debit, American Express Debit  
Efectivo  
rapipago, Provincia Fácil  
Conocé otros medios de pago



# RECOMENDACIONES

## PREVENCIÓN DE LOS PELIGROS DE LAS TICs

### \*/ PREVENCIÓN Y ACCIÓN / \*

- **SÉ VOS MISMO**  
Actúa en la red como actúas en tu vida real.
- **DIALOGÁ**  
Acércate a las personas de confianza si te sentís incómodo/a, amenazada/o y tengas dudas.
- **DESALENTÁ LA VENGANZA**  
No es la solución al conflicto.
- **EVITÁ PUBLICAR INFORMACIÓN PRIVADA**  
Evita publicar tu ubicación, horarios, fotos o algo que puedan utilizar para dañarte. Utiliza contraseñas fuertes.  
Por ejemplo, en el nombre que usas en chats o correo electrónico, evita incluir tu año de nacimiento, ya que esto facilita que personas malintencionadas conozcan tu edad: andreita97@correo.com
- **NO CEDER A PEDIDOS DE EXTRAÑOS**  
No agregues personas que no conoces.  
Abandona conversaciones o sitios web que te incomoden o que tengan contenido inadecuado para tu edad.
- **DENUNCIA Y BLOQUEA**  
La mayoría de chats y redes sociales te permiten bloquear personas y denunciar situaciones incómodas y denuncia ante las autoridades pertinentes.



# CONTROL PARENTAL

## HERRAMIENTAS DE PROTECCIÓN



### **CONTROL PARENTAL:**

Es una herramienta que permite a los padres controlar y/o limitar el contenido a los que sus hijos puedan acceder a internet desde sus dispositivos.

### **\*/ CARACTERÍSTICAS / \***

- **CONTROL WEB**  
Bloqueo de sitios web en función de las diferentes categorías que existen, o especificar páginas concretas a las cuales bloquear.
- **CONTROL DE APLICACIONES**  
Restricción de acceso a ciertas aplicaciones como programas de mensajería instantánea, aplicaciones de redes sociales, acceso a navegadores web, acceso a tiendas como Google Play o Apple Store para realizar compras, etc.
- **BLOQUE DE LLAMADAS**  
Bloqueo a números de teléfono a los que no se permiten emitir o recibir llamadas, además de definir el funcionamiento ante llamadas internacionales o números desconocidos.
- **TIEMPO DE USO**  
Control de tiempo de uso y acceso a juegos o navegadores.
- **GEOLOCALIZACIÓN**  
Obtención de la localización del menor conociendo dónde se encuentra en tiempo real.
- **BOTÓN DE EMERGENCIA**  
Función "Botón del Pánico" con el que se envían alertas de emergencia.

# CONTROL PARENTAL

## CARACTERÍSTICAS

- Existen muchos sistemas de control parental. En castellano:
  - ✓ <https://www.qustodio.com/es/> -> bloquea contenido inapropiado, decide cuánto tiempo estarán conectados, controla juegos y aplicaciones, controla el tiempo que pasan en las redes sociales, controla las llamadas y mensajes, sigue la ubicación y permite enviar “alertas de pánico”.
  - ✓ <https://family.norton.com/web/> -> supervisa el uso de la web y bloquea los inadecuados, administra las aplicaciones que pueden descargar los niño/as, permite revisar los términos que buscan para tener más información sobre sus intereses y sigue la ubicación.
  - ✓ <https://securekids.es/> -> permite decidir qué aplicaciones podrán ejecutarse en el dispositivo, programa franjas horarias para que el dispositivo descanse, permite recibir avisos de botón de emergencias, conoce la ubicación, monitorea las llamadas y gestiona las páginas web.



— **CONCEPTOS DE CIBERSEGURIDAD**

FAA – JORNADA DE CONCIENTIZACION EN CIBERSEGURIDAD

— **BA-CSIRT**

**EL LADO DE LAS TICs**

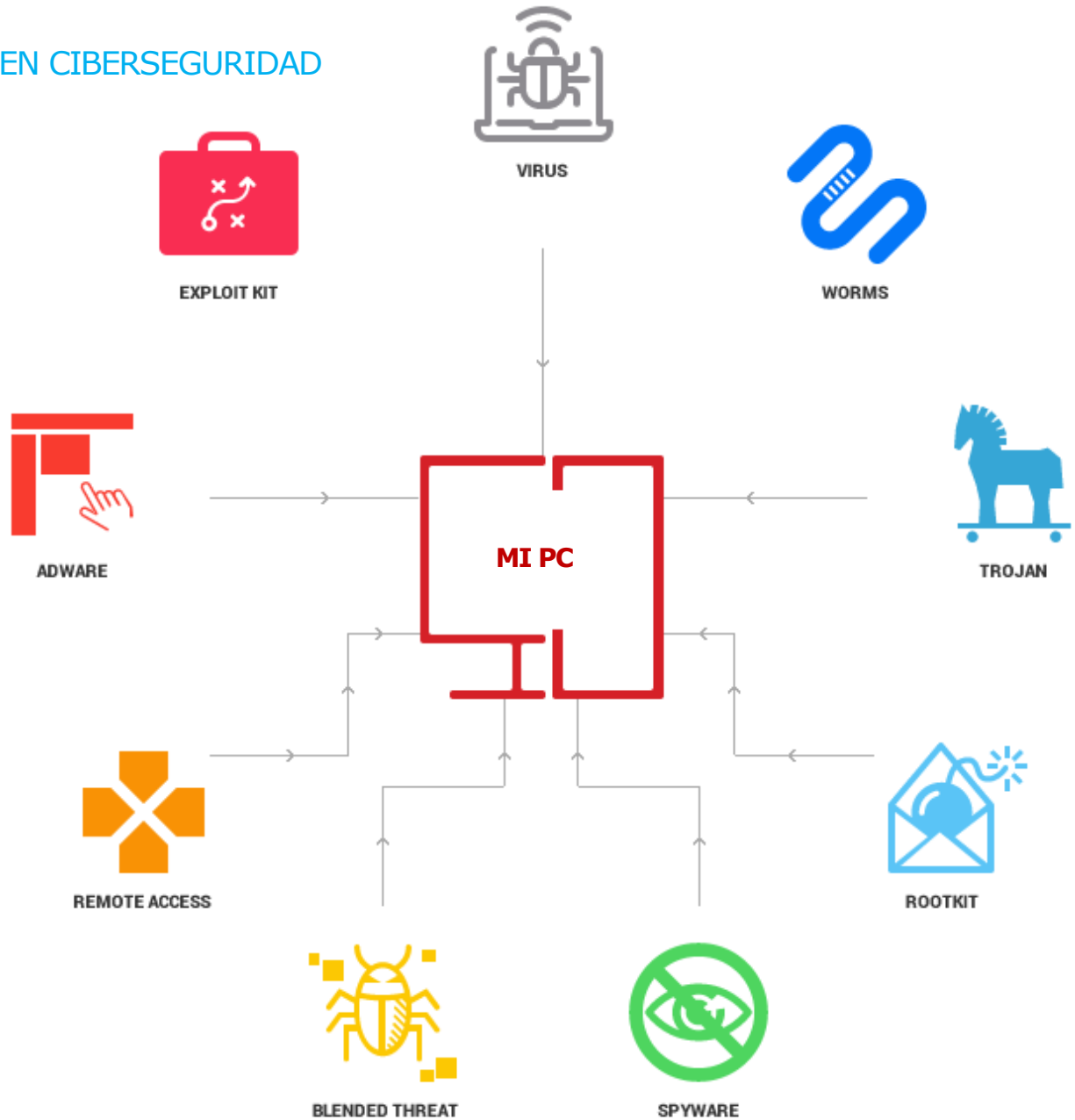
# MALWARE

DAÑO INFORMÁTICO



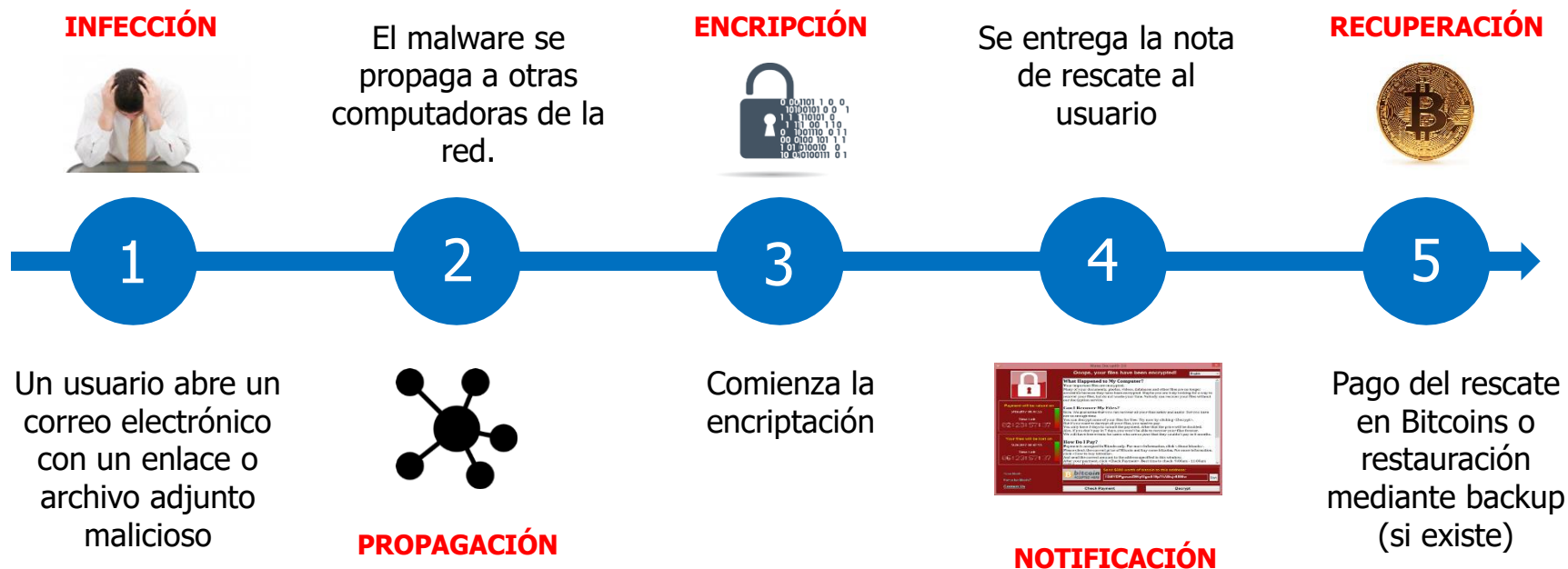
## MALWARE:

Todo tipo de programa o código informático malicioso que tenga como propósito dañar a un sistema o provocar un mal funcionamiento del mismo



# RANSOMWARE

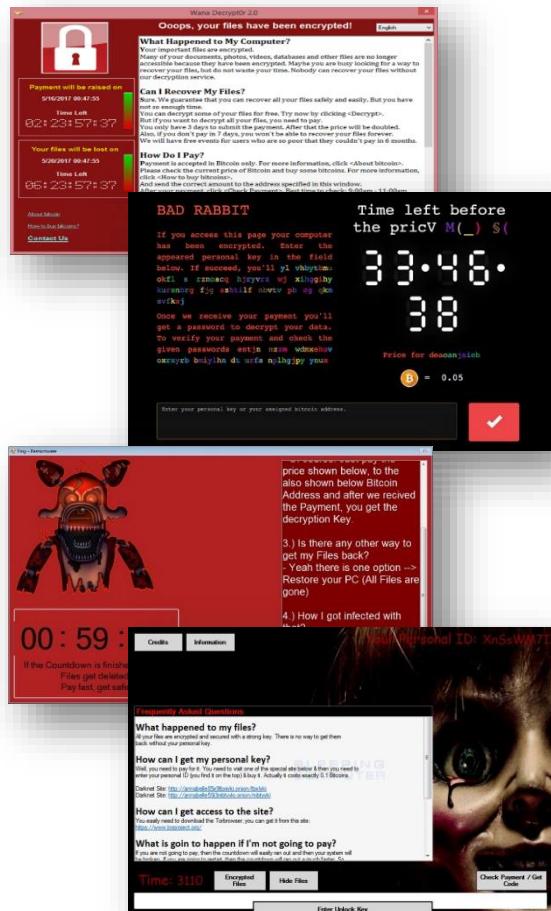
DAÑO INFORMÁTICO



Software malicioso que restringe el acceso a determinadas partes o archivos del sistema infectado y pide un rescate (secuestro de datos) a cambio de desbloquearlo

# RANSOMWARE

DAÑO INFORMÁTICO



## ¿CÓMO PROTEGERSE?

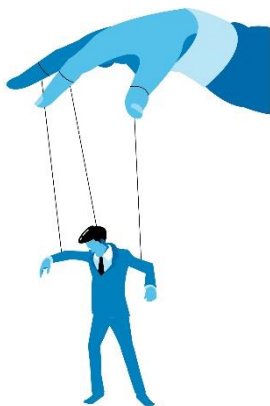
NO SIEMPRE HAY UN ANTÍDOTO CONTRA LA INFECCIÓN POR RANSOMWARE. SIN EMBARGO, SE PUEDE EVITAR SER VÍCTIMA SIGUIENDO ALGUNOS CONSEJOS:

- COPIAS DE SEGURIDAD**  
APLICAR LA REGLA 3-2-1: 3 COPIAS DE SEGURIDAD DE LOS DATOS EN 2 MEDIOS DIFERENTES Y 1 DE ESAS COPIAS EN UN LUGAR DISTINTO
- MARCAR FAVORITOS**  
MARCAR LAS PÁGINAS WEB DE CONFIANZA Y VISITADAS CON FRECUENCIA EVITARÁ INTRODUCIR DIRECCIONES EQUIVOCADAS
- VERIFICAR EMAIL**  
COMPROBAR LA DIRECCIÓN DE CORREO DEL REMITENTE ANTES DE ABRIR UN ENLACE O DESCARGAR ADJUNTOS
- ACTUALIZAR EL SOFTWARE**  
MANTENER EL SOFTWARE ACTUALIZADO AÑADE UNA CAPA ADICIONAL DE SEGURIDAD EN LA PROTECCIÓN ANTI-MALWARE

Si esto te llega a pasar, toma el control de la situación, no te dejes intimidar y no efectúes ningún pago, lo único que debes hacer es denunciarlo.

# INGENIERÍA SOCIAL

## DEFINICIÓN



### INGENIERÍA SOCIAL

Conjunto de técnicas psicológicas y habilidades sociales utilizadas de forma consciente y premeditada para la **obtención de información de otras personas.**

### PHISHING

Engaño mediante correo electrónico, páginas web, perfiles sociales o mensajes falsos de aplicaciones, con el fin de robar información confidencial.



### EL FACTOR HUMANO

El factor humano es el eslabón más débil de la seguridad informática. No hay un sólo equipo que no dependa de un ser humano, por lo que es una vulnerabilidad universal e independiente de la plataforma tecnológica.

# SEGURIDAD EN LAS REDES WIFI

## RECOMENDACIONES



**Desactivar la sincronización:** Son tareas que se desarrollan en segundo plano, sin la intervención del usuario. Es recomendable deshabilitar estos servicios cuando nos encontramos conectados a una red no segura.

**Limpiar la lista de puntos de acceso guardados:** Es conveniente revisar la lista de puntos de acceso memorizados para dejar únicamente aquellos que son confiables.

**Navegar en páginas HTTPS:** Siempre que estén disponibles, conectarse a páginas con certificado de seguridad.

**Proteger la privacidad:** Evitar realizar transacciones bancarias ni exponer datos de usuario y contraseña.

**Desactivar la conexión WIFI:** Una vez fuera del alcance de nuestras redes WIFI de confianza, se debe deshabilitar la opción de conexión automática.

**Antivirus:** Instalar un software antimalware que pueda detectar y bloquear intentos de ataques.

**Parches de seguridad:** Las aplicaciones y los servicios pueden contener fallos de seguridad que un atacante utilizará para ganar acceso a nuestro equipo. Los fabricantes de software están constantemente lanzando actualizaciones que deben ser instaladas lo antes posible.



# PRIVACIDAD: CONTRASEÑAS

RECOMENDACIONES



SECRETAS



ROBUSTAS



NO REPETIDAS



CAMBIADAS  
REGULARMENTE

Emplear Parafrases: NxMmC@+t421



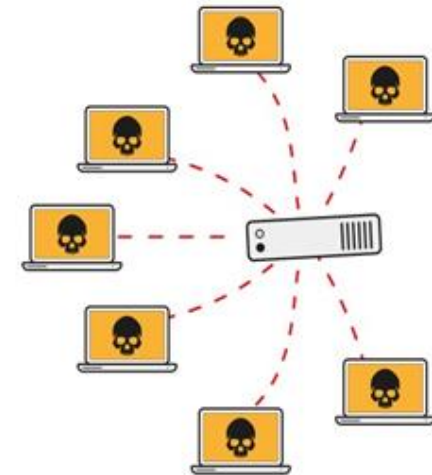
# MALWARE EN DISPOSITIVOS MÓVILES

QUÉ BUSCA UN ATACANTE



¿Para QUÉ NOS INFECTAN?

Para crear una  
**Red Zombie (Botnet)**  
SIN QUE LO SEPAMOS



¿QUÉ DATOS LES INTERESAN?

- **VIGILANCIA** (Audio, cámara, registros de llamadas, ubicación, etc.)
- **IDENTIDAD** (Redireccionamiento de SMS, posteos en redes sociales, envío de emails, etc.)
- **DATOS** (Detalles de cuentas, robo de IMEI, etc.)
- **FINANZAS** (Robo de OTP, extorsión vía ransomware, llamadas internacionales, envío de SMS premium)

# SEGURIDAD EN DISPOSITIVOS MÓVILES

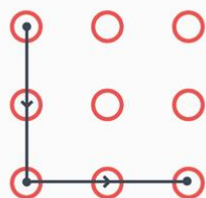
TIPOS DE BLOQUEO



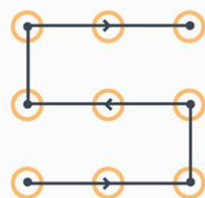
# SEGURIDAD EN DISPOSITIVOS MÓVILES

## PATRÓN DE DESBLOQUEO

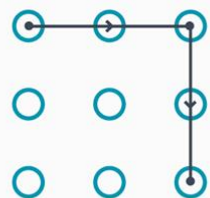
Los Passwords más comunes en Android.



44% inicia arriba a la izquierda.



77% inicia de alguna esquina.



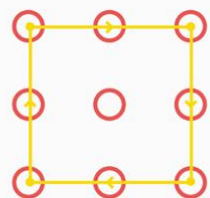
Más del 50% utiliza una secuencia de 5 puntos.



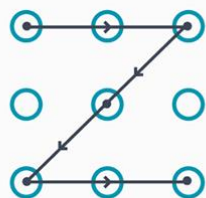
La mayoría utiliza forma de letras...



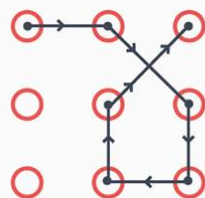
...o números.



La "0" es el unlock más común...



...seguido por la "Z".



Usar 8 puntos y ser random es lo más seguro

Los patrones de desbloqueo en Android pueden contener un mínimo de cuatro puntos y un máximo de nueve, haciendo posible hasta 389.112 posibles combinaciones.

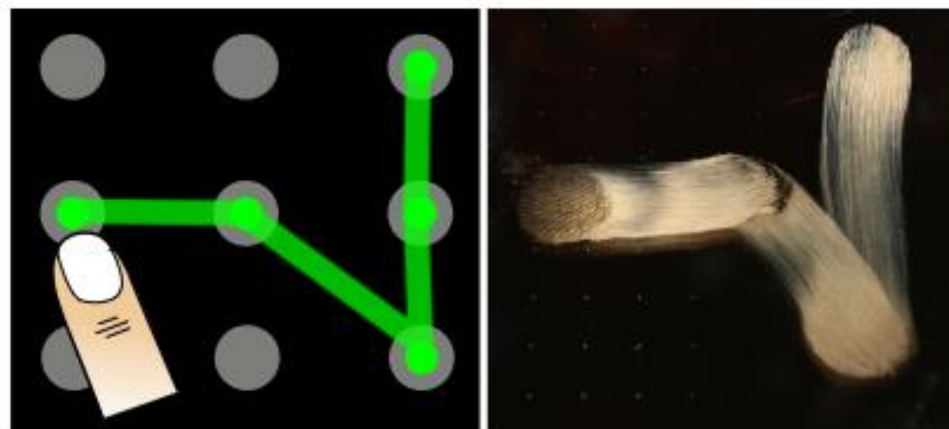
Nº MERO DE PUNTOS	POSIBLES COMBINACIONES
4	1.624
5	7.152
6	26.016
7	72.192
8	140.704
9	140.704

# SEGURIDAD EN DISPOSITIVOS MÓVILES

ATAQUES AL DESBLOQUEO

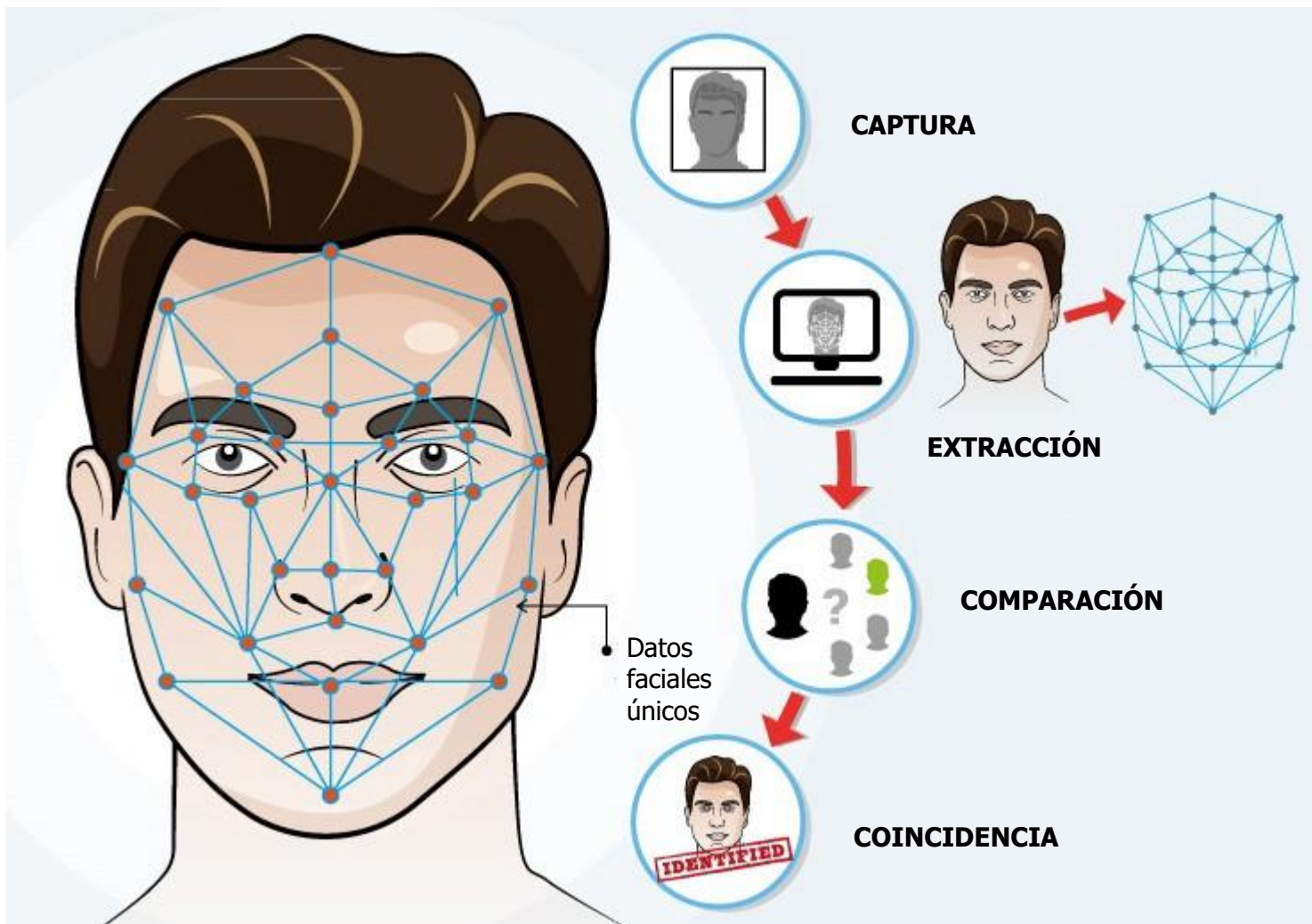


## SMUDGE ATTACK



# RECONOCIMIENTO FACIAL

DATOS BIOMÉTRICOS





---

## CONCEPTOS DE CIBERSEGURIDAD

FAA – JORNADA DE CONCIENTIZACION EN  
CIBERSEGURIDAD

---

# BA-CSIRT

## SEGURIDAD DE DATOS PERSONALES

# LA IMPORTANCIA DE LA PRIVACIDAD

**“ NO DEFENDER LA PRIVACIDAD  
PORQUE NO TIENEN NADA QUE  
OCULTAR, ES COMO NO  
DEFENDER LA LIBERTAD DE  
EXPRESIÓN PORQUE NO TIENEN  
NADA QUE DECIR ”**



## **EDWARD SNOWDEN**

Es un analista de inteligencia que denunció los abusos del espionaje masivo que realizan los servicios secretos de Estados Unidos.

Expuso la fragilidad de la privacidad de las comunicaciones en la era digital, dejando al descubierto a gigantes de Internet como Google, Facebook, Microsoft, entre otros.

# SEGURIDAD DE LOS DATOS PERSONALES

LEY 25.326

TIPO DE DATOS	DESCRIPCIÓN	
DATOS DE IDENTIFICACIÓN	DNI, CUIT/L, fecha de nacimiento, edad, nacionalidad, estado civil, sexo, imagen, dirección de IP, etc.	BAJO
DATOS LABORALES	social, aportes, historial en la empresa	
DATOS ACADÉMICOS	curriculum vitae, trayectoria educativa, títulos, matrículas habilitantes, certificados, condición de alumno, calificaciones, etc.	MEDIO
DATOS PATRIMONIALES	información fiscal, historial crediticio, cuentas bancarias, ingresos y	
DATOS IDEOLÓGICOS	organizaciones de la sociedad civil, asociaciones religiosas, etc.	
DATOS DE SALUD	relacionada con cuestiones de carácter psicológico, psiquiátrico, é gimen de licencias, etc.	CRÍTICO
CARACTERÍSTICAS PERSONALES Y FÍSICAS	tipo de sangre, ADN, huella digital, altura, peso, discapacidades, color de piel, iris y cabellos, señales particulares, etc.	
VIDA Y HABITOS SEXUALES		

**OBJETIVOS**  
 Protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios de tratamiento de datos, sean éstos públicos o privados destinados a dar informes.  
  
 Garantizar el derecho al honor y a la intimidad de las personas.

# DATOS SENSIBLES

DATOS PRIVADOS



# DERECHO AL OLVIDO

DATOS PRIVADOS



## DERECHO AL OLVIDO

- Es un concepto donde los buscadores deben atender a las solicitudes de borrar contenidos que puedan considerarse irrelevantes o perjudiciales para el usuario.
- La idea es encontrar un equilibrio entre el derecho a la privacidad del usuario y el derecho del público a conocer información.
- En Argentina no existe, aunque sí se reconoce legalmente al usuario que pueda pedir corrección o eliminación de datos (**Ley 25.326** de Protección de Datos Personales)





— **CONCEPTOS DE CIBERSEGURIDAD**

FAA – JORNADA DE CONCIENTIZACION EN CIBERSEGURIDAD

— **BA-CSIRT**

**DELITOS INFORMÁTICOS**

# QUÉ HACER

PASOS

## \*/ PRIMERAS MEDIDAS/ \*

- **EVIDENCIA**

No borres ningún contenido del dispositivo. Todo debe ser resguardado como prueba del hostigamiento, tanto en formato digital o impreso.

- **DENUNCIÁ**

Antes de llevar adelante cualquier acción, llamanos para orientarte.

- **PREVENCIÓN**

No continúes el contacto con el abusador ni lo bloques antes de llamarnos. Podemos usar las pruebas para una posible investigación.

- **ALGUNAS HERRAMIENTAS DE SEGURIDAD**

<https://dominemoslatecnologia.org/es/recursos>

# CONTACTO BA-CSIRT



**WWW.BA-CSIRT.GOB.AR**



**CIBERSEGURIDAD@BA-CSIRT.GOB.AR**



**+54 11 4323-9362**



**FACEBOOK: /BACSIRT**  
**TWITTER: @BACSIRT**  
**INSTAGRAM: @BACSIRT**



CONCEPTOS DE CIBERSEGURIDAD  
MUCHAS GRACIAS



**¡MUCHAS  
GRACIAS!**



[www.ba-csirt.gob.ar](http://www.ba-csirt.gob.ar)



**Carina Birarda**  
ISO27032LM<sup>®</sup>, C|CISO<sup>®</sup>,  
ISO27001LA<sup>®</sup>, ISO22301LA<sup>®</sup>,  
CCSK<sup>®</sup>.-