ERA Digital

Herramientas control parental

Lic. Guido Buhl

- Lic en Sistemas Informacion de las Organizaciones.
- Maestría en Seguridad informática.
- Gestión área de Sistemas.
- Especialidad en diseño de aplicaciones
- Proyecto de digitalización de la Justicia dela Ciudad de Buenos Aires
- Padre de Jerónimo

Temario

- La exposición busca abordar los desafíos de esta “Era Digital” desde la perspectiva de las Herramientas de Control Parental. Para ello se buscará hacer un análisis sobre estas herramientas, entendiendo para qué sirven, cómo funcionan.
- El entendimiento de estas herramientas permiten introducir fenómenos muchos más complejos que si bien están presentes en la cotidianeidad, la mayoría de las veces pasan desapercibidos por gran parte de los usuarios.
- Se verán temas relacionados con el uso de las redes sociales, dentro de los cuales se encuentran los delitos informáticos
- Finalmente en base a lo discutido sobre las herramientas de control parental y los fenómenos asociados a esta era digital se intentará entender cómo estas herramientas pueden llegar a jugar un rol importante durante la investigación de un delito informático aportando evidencia clave para determinar lo ocurrido.

Ser Padres en la era Digital I

- Principios siglo pasado el mundo era un lugar hostil y la mejor manera de prepararse era con una crianza era severa, estricta, en algún sentido desprovista de afecto…
- Los hijos eran una fuerza laboral, tenían un valor económico.
- En la década del 20 surge la Declaración del derecho de los niños
- En 1959, la Asamblea General de las Naciones Unidas aprobó la Declaración de los Derechos del Niño.

Ser Padres en la era Digital I

- Los hijos ya no trabajan para los padres, sino que los adultos trabajan para ellos….
- Prioriza la educación y el desarrollo de los niños
- La educación por miedo o castigo físico evoluciona a la explicación y entendimiento
- Se destina cada vez más recurso (tiempo y dinero) para promover su bienestar
- Aumenta la dificultad para poner y sostener límites
- Nos encontramos con un fenómeno denominado por algunos como el Hijocentrismo

Ser Niños en la era Digital I

- Seguridad Infantil elimina riesgos
- Protegemos Permanentemente de riesgo real o potencial
  - Sillita del auto y como viajamos
  - Jugar en la calle
  - Rejas en las plazas
  - Rejas en las piletas
  - Protectores Muebles para los bordes filosos
  - Traba Cajones
  - Diseño electrodomésticos (pava eléctrica, cafetera)

Cada riesgo que suprimimos protege, pero elimina la necesidad de **usar la palabra para enseñar que se debe hacer y que no.**

Esto Limita la capacidad de lidiar con las dificultades.

Ser Niños en la era Digital II

- Niños repletos de actividades mediadas.
- Sobreestimulación informativa que se recibe de los medios y de las redes.
- La buena noticia no es noticia.
- Consolida una sociedad de consumo
- Productos tecnológicos de Lujo se vuelven accesibles.
- Carácter cada vez más descartable de los bienes de consumo
    - ej. CD vs Spotify

Como nada dura mucho y todo se consigue fácilmente, nada es demasiado apetecible.

La cultura de lo inmediato no ayuda a aprender a lidiar con la frustración

En todo este contexto....

“Todo lo que existía en el mundo cuando tu naciste es normal y una parte natural de la manera en que funciona el mundo.

Todo lo que se inventa entre que tú tienes 15 y 35 es excitante y revolucionario y probablemente puedes hacerte una carrera con ello.

Todo lo que se inventa después de que cumples 35 va en contra del orden natural de las cosas.”

Douglas Adams

Mientras que para nosotros los celulares son un objeto que hemos adoptado, para los chicos es algo que siempre existió con el cual tienen una relación completamente natural.

Tiene características de omnipresencia y omni funcionalidad.

Hasta no hace demasiado tiempo, el marketing de los productos iba dirigido a los adultos que eran quienes tenían el dinero.

Desde finales de los 90, los niños son el nuevo target.

Se descubrió que la mente de los bebes/niños puede ser cautivada por cierto tipo de estímulos visuales y sonoros.

La pantalla de la tele se va reemplazando por la de celulares y tablets.

Los contenidos empiezan a estar disponibles en todo hora y lugar. Aumenta la oferta de contenidos.

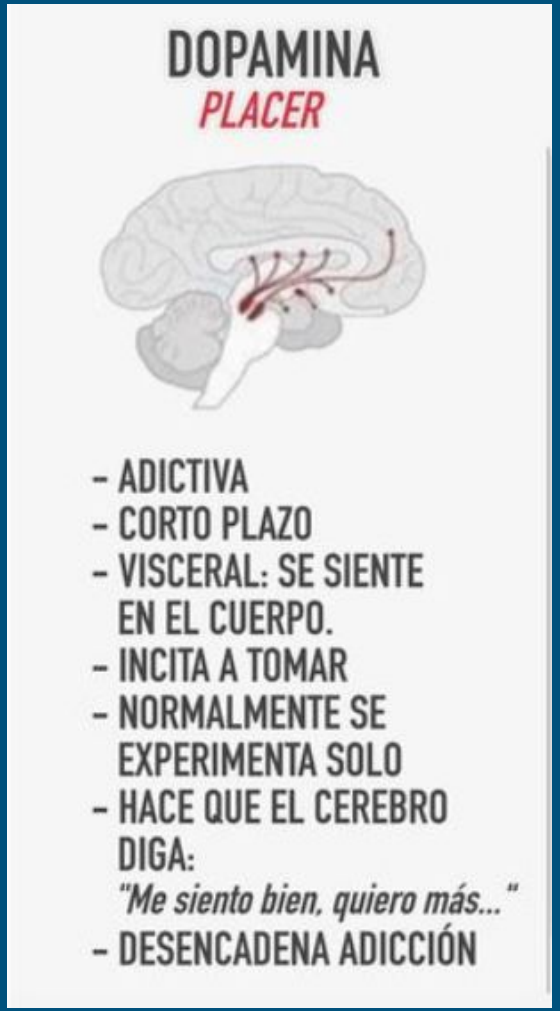
Tendencias que se profundizan.

Mayor número de clics, mayor número de reproducciones significan mayores ganancias para las empresas

EL diseño de videos, juegos y redes sociales busca generar un comportamiento adictivo en los usuarios

La **dopamina** es un neurotransmisor que produce nuestro cerebro y nos genera una **sensación de bienestar**. Se le considera el centro del placer porque regula la motivación y el deseo y hace que sintamos la necesidad de repetir conductas que proporcionan esas “maravillosas” sensaciones.

Ejemplos: like de facebook, videos egg surprise o family hand, endless scroll



Estamos tan **sobreestimulados** que segregamos más dopamina de la recomendable y eso provoca que el cerebro se acostumbre. Así, **lo habitual deja de ser placentero** y cada vez necesita más y más para lograr de nuevo ese placer.

Lanzado en 2012 Candy Crush es uno de los primeros juegos que indaga en estos mecanismos.

Mientras pensamos que depende de nuestra habilidad para reventar, en realidad hay un algoritmo detrás que busca incidir sobre el resultado del juego.

SI ganamos muy fácil se torna aburrido, si perdemos siempre también. Se busca que se gane la cantidad necesaria para mantener el encanto, y si se pierda sea por muy poco y buscar revancha.

Control Parental

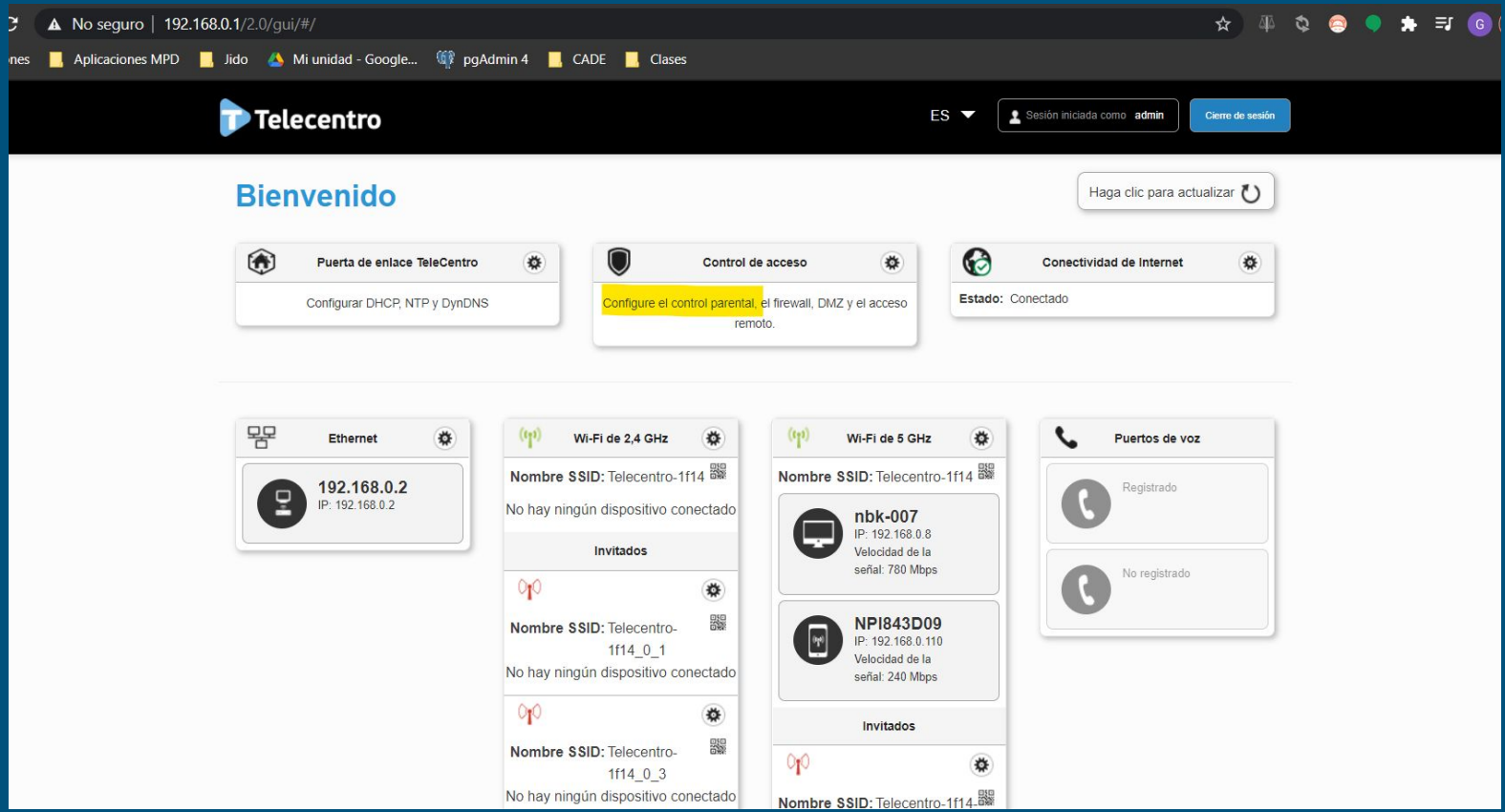
Control parental en sentido estricto o específico hace referencia al conjunto de herramientas informáticas que nos ayudan a controlar el acceso a la red por parte de los menores.

Control Parental

¿Qué dispositivos debemos controlar?

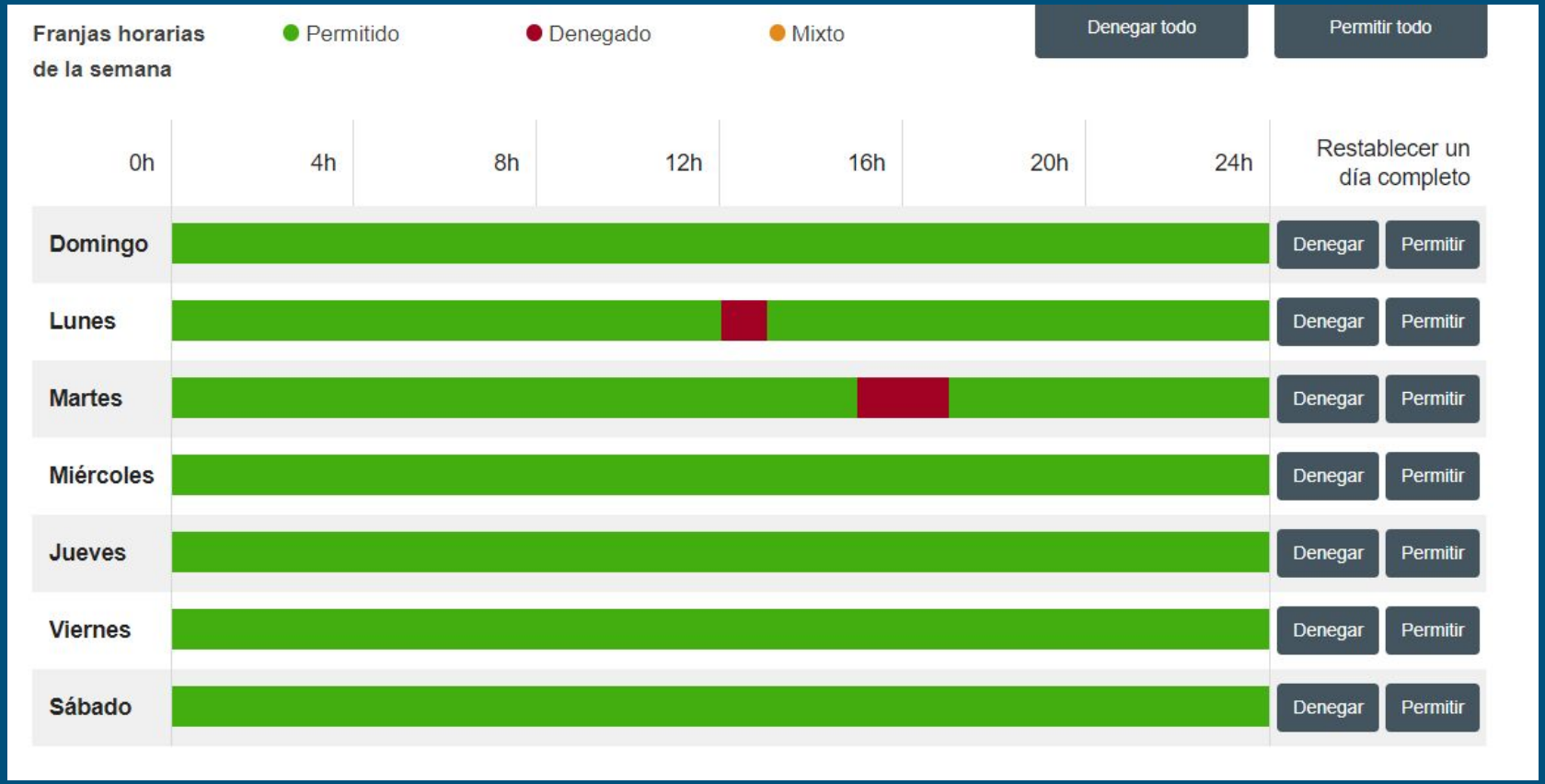
- Consolas de juegos
- Tablets
- Teléfono
- Computadora
- Router/Modem

Control Parental



Control Parental

Control Parental



Control Parental

Control Parental

Establecer límites de tiempo de pantalla

Basta de discusiones. Define un limite equilibrado en los dispositivos, las aplicaciones

Bloquear contenido inapropiado

Asegúrate de que tus hijos vean contenido y usen juegos adecuados para su edad.

Informes de actividad

Ve la actividad semanal de tus hijos en todas sus aplicaciones, juegos y dispositivos.

Buscar a tu familia

Ten la tranquilidad de saber que tu familia llegó a un lugar sin tener que preguntarles.

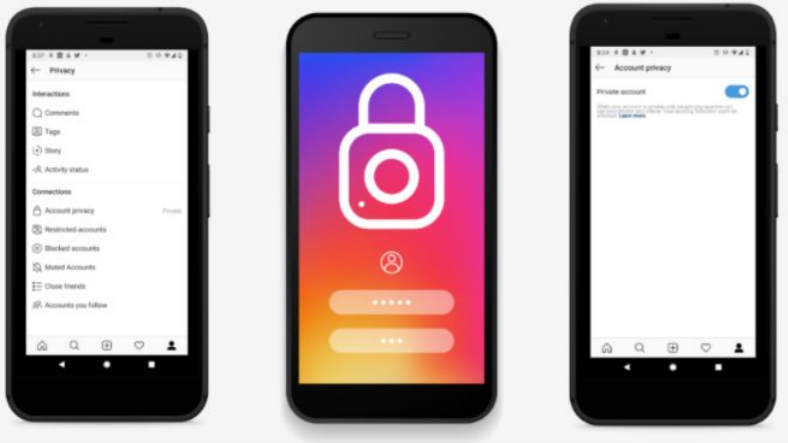
Control Parental

¿Qué necesito?

Una cuenta de Instagram (nombre de usuario y contraseña) y la aplicación

Restricciones que puedes aplicar

- Chateando
- Contenido inapropiado
- Privacidad y robo de identidad
- Redes Sociales



Control Parental

Cuando éramos chicos nos enseñaban a no hablar con extraños, nunca aceptar caramelos de un desconocido.

Nos enseñaban a como cruzar la calle, viajar en transporte público etc.

Gradualmente nos íbamos formando y preparando para lidiar con el mundo y los riesgos que este presentaba.

Control Parental

En contraposición hoy la mayoría de los niños empiezan a usar internet y las redes sin mucha explicación previa, sin demasiada planificación y mucho menos supervisión.

Muchas veces los adultos ni siquiera entendemos lo que están haciendo los niños con los dispositivos o los riesgos que existen en el mundo virtual.

Es muy común que los chicos manejen mejor las herramientas que los propios adultos.

Internet es un espacio público y como tal, hace falta entenderlo y saber cómo moverse, al igual que cuando aprendemos a manejarnos en la calle.

Control Parental

Interacciones con desconocidos

Si de chicos aprendemos a no hablar con extraños, en internet esto resulta clave.

La mayoría de las plataformas y juegos ofrecen distintos medios para hablar y conocer gente.

Esto da lugar a delitos como el grooming, robo de datos personales, robo de identidad etc.

Áreas peligrosas

De la misma forma que en una ciudad hay lugares donde uno se puede mover con bastante tranquilidad y otras donde no, lo mismo pasa en la red. Solo que en la red, las fronteras son mucho más difusas y pasar de un lugar a otro es un click de distancia.

Sin demasiada dificultad se puede caer en lugares de distribución de pornografia, xenofobia, violencia etc

Control Parental

Violencia psicológica

EL supuesto anonimato que provee internet hace que las personas sean mucho más agresivas de lo que pueden llegar a ser cara a cara.

El hecho de no desconectarnos y de no poder ver lo que le pasa al otro, hacen del fenómeno de bullying un tema crítico.

Los niños pueden ser víctimas, pero también ser victimarios o cómplices sin darse cuenta de esto.

Cuentos del tío

En la ciudad existe la posibilidad de un engaño como un supuesto secuestro a un familiar cercano e internet no es la excepción.

Páginas falsas para robar contraseñas o datos bancarios, mails de algún príncipe de arabia

¿Por Qué debemos controlar los Dispositivos?

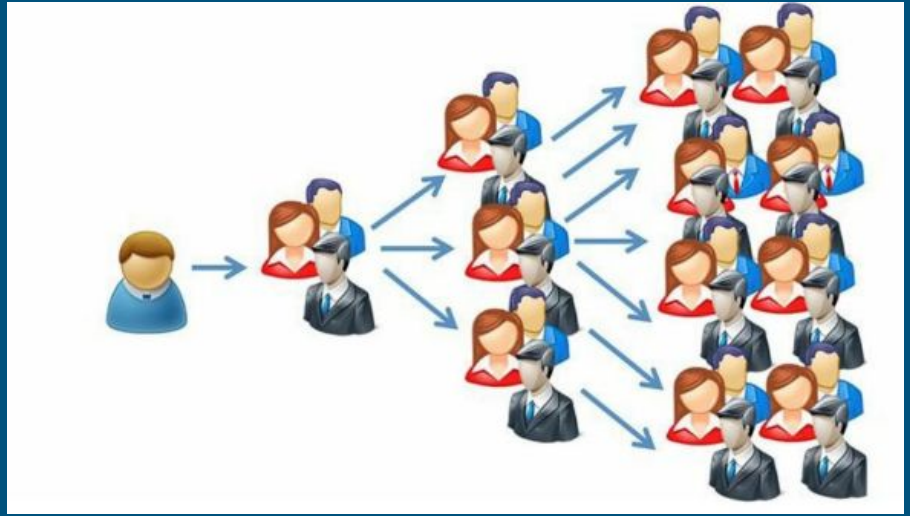
Control Parental

Exposición y viralización

La velocidad y la potencia con que se transmite la información genera una exposición impensado o difícil de calcular.

La facilidad con el cual un mensaje privado se hace público, o que dicho en un ámbito se transmite a otro son partes de los nuevos desafíos de las redes.

Decimos o publicamos algo que no sabemos quien lo recibe.



Control Parental

Indelebilidad

Lo que sucede en la red, queda prácticamente de forma indefinida. Algo que hacemos hoy, será visible en 50 años.

Es muy difícil, casi imposible, eliminar.

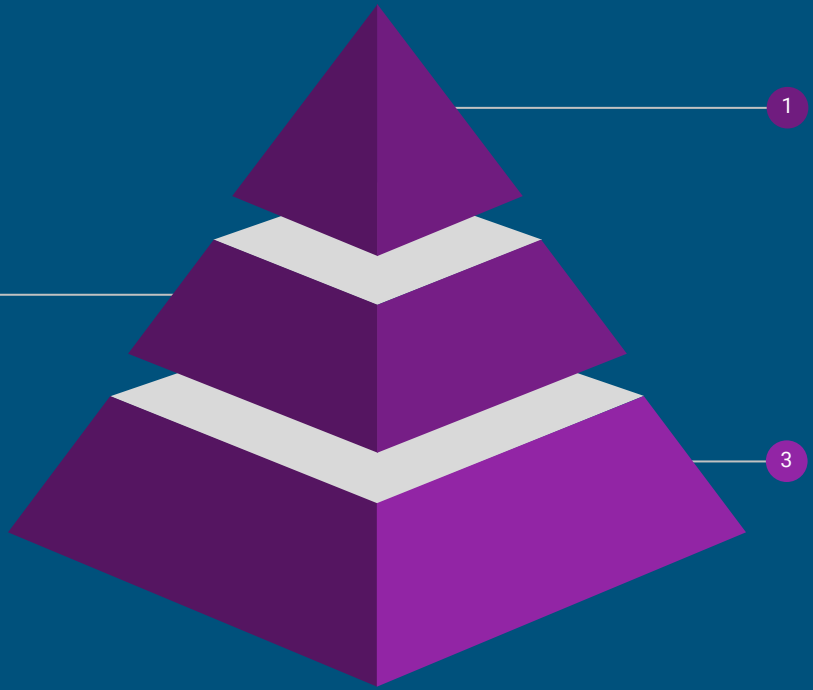
El derecho al olvido existe, pero probablemente el daño ya está hecho para cuando se consiga el “olvido”.

Control Parental

Control Parental

Control Parental

Control Parental o Mediación Parental



La educación que los adultos les den a los menores para conseguir un uso seguro de Internet y de los dispositivos para acceder a ella.

Los programas de prevención y actuación ante casos que puedan ponerse en funcionamiento en los centros educativos e incluso a nivel familiar.

El establecimiento de normas de uso, recomendaciones y pautas de actuación a la hora de conectarse a la Red, tanto en el centro educativo, domicilio, como en cualquier otro lugar.

Las herramientas de control parental en el proceso penal

Poniendo a la persona detrás de la computadora

- Probar quien cometió el delito
  - Uno de los más grandes desafíos de la mayoría casos de delitos informáticos está en probar quién estaba en el ordenador, es decir la autoría.
  - La posibilidad que se ofrece de localizar el ordenador u ordenadores desde donde se ha cometido el delito perseguido no es prueba plena de la participación en los hechos de una persona concreta, que permita inculpar.
  - No es lo mismo localizar el ordenador, que al usuario
  - En los delitos cometidos a través de internet, la prueba indiciaria, rara vez permitirá identificar al autor o autores.
  - Esta prueba casi siempre depende de algún tipo de evidencia circunstancial.

Poniendo a la persona detrás de la computadora

Para investigar quién ha podido realizar una acción concreta a través de Internet, se debe:

- IP como medio de prueba:
- Proveedor de acceso:
    - Dirección electrónica
    - Momento de la conexión
- Proveedor de servicios
    - Identidad del abonado
- Interceptación de comunicaciones
- Entrada y registro

Poniendo a la persona detrás de la computadora

Para la defensa penal informática, la identificación de una dirección IP no supone que sea un usuario concreto el que ha cometido la infracción. Esto se evidencia porque: la relación de ser propietario de un ordenador y línea telefónica no lleva necesariamente a la conclusión de que sea esa persona el autor del hecho investigado. Sobre todo, cuando existen dudas y/o alternativas razonables.

Poniendo a la persona detrás de la computadora

Escenarios

- Habiendo determinado desde donde se realizó el delito, hay varias personas con distintos dispositivos que usan esa conexión.
- Habiéndose determinado el dispositivo, hay varios usuarios que lo utilizan.

Poniendo a la persona detrás de la computadora

Zombi es la denominación asignada a computadores personales que, tras haber sido infectados por algún tipo de malware, pueden ser usados por una tercera persona para ejecutar actividades hostiles. Este uso se produce sin la autorización o el conocimiento del usuario del equipo

Bajo mandato judicial las autoridades policiales podrán instalar software que permita de forma remota y telemática examinar a distancia el contenido de un ordenador. Si lo puede hacer la policía también lo puede hacer un atacante.

Poniendo a la persona detrás de la computadora

Si las conexiones a Internet se realizan a través de artilugios electrónicos de los denominados “router inalámbrico”. Esto significa que para conectarse a Internet no se precisa de un cable que conecte el ordenador con el “router inalámbrico”. La conexión se realiza por ondas de radio y no por cables. Por lo que cualquier persona que estuviese en el alcance de esas ondas puede conectarse a Internet a través del “router inalámbrico” del domicilio del acusado.

Poniendo a la persona detrás de la computadora

Hackear wi-fi

Un método para hackear las contraseñas cifradas de Wi-Fi es mediante la fuerza bruta, por lo que cada combinación de caracteres se intenta hasta que llegue a la correcta. Es teóricamente posible, pero esto puede tomar años en la práctica, especialmente si se utiliza una contraseña larga.

Diferentes software buscan como acelerar este proceso considerablemente. Esto se hace generalmente intentando con una listas de palabras pre-compiladas que contienen contraseñas predeterminadas y comunes, así como forzando a los dispositivos a volver a autenticarse para que pueda capturar el procedimiento crucial: handshake, donde la clave del WiFi se intercambia con el router.

Gran parte de la seguridad está en la robustez de la clave

Poniendo a la persona detrás de la computadora

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Poniendo a la persona detrás de la computadora

El rol de la evidencia circunstancial

- Ante todo cabe recordar que en el derecho penal y particularmente en el derecho procesal penal rige el principio de libertad probatoria en virtud del cual, como es bien sabido, los hechos investigados pueden acreditarse recurriendo a todo tipo de elementos de convicción, siempre y cuando no se vulneren garantías constitucionales de los involucrados.

- Si bien la IP no resulta suficiente, sirve como un indicio que enmarcado y respaldado por todo un plexo probatorio puede permitir inferir y determinar autoría

Poniendo a la persona detrás de la computadora

Ante la ausencia de evidencia directa que una a una persona con el delito, puede aportar a la investigación

- Capacidad de acceso
- Nivel de Conocimiento
- Oportunidad
- Motivación
- actitud de culpabilidad

Poniendo a la persona detrás de la computadora

Ante la ausencia de evidencia directa que una a una persona con el delito, puede aportar a la investigacion

Capacidad de acceso

- Computadora (hardware, software, archivos)
- Teléfono o cable usado para llevar adelante el delito
- Cuentas online involucradas (Email, online banking, social networking)
- ¡Quién más tiene acceso?

Poniendo a la persona detrás de la computadora

Ante la ausencia de evidencia directa que una a una persona con el delito, puede aportar a la investigacion

Nivel de Conocimiento del acusado

- Experiencia con el programa, sistema o red que se utilizó o fue comprometida
- Entrenamiento en el uso de computadoras, nivel educativo y experiencia o habilidades
- Conocimiento con hechos específicos relacionados al delito
- Posesión de password

Poniendo a la persona detrás de la computadora

Ante la ausencia de evidencia directa que una a una persona con el delito, puede aportar a la investigacion

Oportunidad del acusado de haber cometido el crimen

- Haber usado la computadora en el momento del hecho
- Sin coartada creíble

Poniendo a la persona detrás de la computadora

Ante la ausencia de evidencia directa que una a una persona con el delito, puede aportar a la investigacion

Motivación del acusado para haber cometido el delito

- Revancha
- Dinero (incluyendo chantaje o extorsión)
- Políticas
- Desafío personal

Poniendo a la persona detrás de la computadora

Ante la ausencia de evidencia directa que una a una persona con el delito, puede aportar a la investigacion

Actitud de culpabilidad

- Engaño
- Ocultación
- Destrucción de pruebas

Poniendo a la persona detrás de la computadora

La mejor evidencia circunstancial puede venir del trabajo de metodos tradicionales de recolección de evidencia, como:

- Entrevistas con sospechosos y testigos
- Evidencia física
- Vigilancia

La evidencia tradicional puede corroborar la electrónica evidencia

Poniendo a la persona detrás de la computadora

La evidencia circunstancial puede proporciona el vínculo clave entre el sospechoso y la computadora o demostrar su inocencia

Prueba circunstancial tradicional complementa la evidencia electrónica al hacer un caso más fuerte de que el sospechoso fue responsable

Control Parental puede aportar evidencia clave

Poniendo a la persona detrás de la computadora

Estrategia genéricas de la Defensa

1º.- Comprobar la autenticidad e integridad de la prueba de cargo que pretenda sustentar la acusación.

Normalmente las pruebas informáticas presentadas en la denuncia se pueden manipular. Es por ello que en la acusación debe existir una actuación que garantice la autenticidad e integridad de la prueba informática presentada.

2º.- Analizar la investigación que determinó la dirección IP desde la que se realizó la acción por la que se es acusado.

3º.- Comprobar si los hechos han sido realizados por el acusado. Porque otra persona ha podido cometer el delito usando su conexión a Internet.

4º.- Comprobar si los hechos han sido realizados por el investigado. Porque otra persona ha podido cometer el delito informático usando su ordenador de forma remota.

Complejidad en el abordaje