INFORME FINAL

PRESTACIÓN DE SERVICIOS DE APOYO A LA GESTIÓN DE LA SECRETARÍA DEL INTERIOR DEL DEPARTAMENTO DEL ATLÁNTICO MEDIANTE EL FOMENTO DE LA CIBER SEGURIDAD, LA PREVENCIÓN DEL CIBER DELITO Y LA PROMOCIÓN DE LA CIBER CONVIVENCIA EN EL TERRITORIO ATLANTICENSE.

No. DE CONTRATO: 202201713

BARRANQUILLA – 23 DE DICIEMBRE DEL 2022

INTRODUCCIÓN

El uso de las tecnologías, específicamente de las herramientas informáticas, cada vez son más naturalizadas por los individuos en sociedad, es decir, la modernidad (o post modernidad llamada así por algunos autores) casi que obliga a todo ser humano a utilizar estas herramientas, tanto para el uso de bienes y servicios, como para el goce propio. En ese sentido, las transformaciones vertiginosas de la sociedad contemporánea han traído consigo nuevas dinámicas de socialización, de interacción y canales o medios diseñados para dinamizar las relaciones económicas, facilitando los trámites que antes exigían la presencia física de los usuarios. Pero, así mismo, encontramos que los avances tecnológicos en materia informática trajeron consigo nuevas dinámicas criminales. El ciber espacio es sinónimo de nuevas oportunidades para todas las personas y comunidades, pero también un escenario de actividades delictivas de diversa índole. Desde comportamientos de acoso escolar y extorsión, hasta reclutamiento criminal (entre otras muchas).

La ciberdelincuencia, la gran maldición de Internet, se refiere a cualquier actividad ilegal llevada a cabo mediante el uso de tecnología. Los responsables pueden ser personas aisladas, grupos organizados o facciones con patrocinio estatal, y utilizan técnicas como el phishing, la ingeniería social y el malware de todo tipo para cumplir sus siniestros planes. Aprenda aquí cómo funciona la ciberdelincuencia y cómo puede protegerse.*1*

Según la Cámara Colombiana de Informática y Telecomunicaciones (CCTI) en su informe sobre el balance de los delitos cibernético 2019-2020, ha llegado a la conclusión que: El cibercrimen, o ciberdelito, ha experimentado un crecimiento los últimos años casi de forma paralela al uso de las nuevas tecnologías, y las pérdidas generadas por los ciberataques sitúan a esta problemática como una de las principales economías ilegales en el País. Esto representa un reto en materia de seguridad ciudadana, particularmente en cuanto a prevención, capacidades de persecución y articulación institucional.

Es por ello fundamental trabajar en la creación de una cultura digital para la prevención, que logre contrarrestar las diversas amenazas que hoy se presentan en términos de delitos informáticos (ciber acoso, extorción, fraudes electrónicos, estafas masivas y captación ilegal de dinero). Entendiendo por estos, aquellas acciones que se cometen por un medio informático cuyo fin sea el de afectar las libertades, los bienes y los derechos que tienes las personas.

En este sentido, y muy ligado a lo anterior, es importante abrir un espacio al análisis y disertación en torno a esta temática que cada día nos reclama mayor atención y

1 Tomado de https://www.avast.com/es-es/c-cybercrime

responsabilidad desde la institucionalidad, pero con mayor esfuerzo desde la ciudadanía. Este tema del ciberdelito está muy ligado con la ciber convivencia y la ciber seguridad, fenómenos que han llegado con la transformación de las lógicas de socialización de sociedad contemporánea, a los que son casi imposible disociarlos o separarlos. Pues bien, hablar de ciber convivencia, ciber delitos y ciber seguridad, nos debe llevar a comprender que ante la eclosión de las nuevas formas de vida en la sociedad red, o bien sea en la era de la información de la cual habla el Sociólogo Español Manuel Castell (1995), han surgido nuevos retos que hoy nos demandan atenciones oportunas, corresponsabilidad comunitaria y acciones de socialización entorno a la necesidad de crear una sola fuerza, para hacerle frente a este flagelo que cada día está más cercano a nuestros hogares, puesto que trabajar en la prevención y control de todas las formas de ciber delincuencia, nos permitirá gestar un Atlántico para la Gente, un Atlántico donde sus ciudadanos se sientan seguros y confiados de que desde la institucionalidad existe un gran compromiso con la mitigación de todas las acciones que atenten contra su bienestar.

En ese sentido y bajo este marco, la Gobernación del Atlántico viene adelantando un trabajo para la prevención del ciberdelito en cabeza de la Secretaría del Interior y en medio del cual se estructura la ejecución del presente proyecto. En la minuta contractual se han establecido una serie de actividades y entregables, que de a cuerdo al siguiente cuadro se estarán presentando en el presente informe.

Fase	Actividad	Meta	Entregable	Cumplimiento
I	**Diseño de la estrategia de pedagogía social:** Construir una estrategia publicitaria y comunicacional que permita	1	Informe detallado con el diseño publicitaria y comunicacional que servirá para el trabajo de campo en los 6 municipios priorizados.	100%
II	**Identificación de los sectores:** para el cumplimiento de esta actividad será necesario llevar a cabo una reunión con cada una de las alcaldías locales de los municipios priorizados.	6	Evidencia fotográfica y relatoría que contenga la identificación de los lugares seleccionados para la implementación de la estrategia.	100%
	Reunión con el comité de seguridad bancaria del departamento del	1	Evidencia fotográfica y acta de la reunión	100%

	Atlántico: con el fin de articular las acciones de implementación, especialmente la de toma de bancos, se espera tener reuniones previas con delegados de las entidades bancarias que hagan presencia en los 6 municipios priorizados, con el fin de articular dichas acciones.		donde se contemple lugar y hora para la actividad denominada toma de banco.	
III	**Implementación de la estrategia:** Se realizará la implementación de la estrategia publicitaria y comunicacional y por medio de la metodología de pedagogía social se sensibilizará a la comunidad de los sectores anteriormente seleccionados.	4 por municipio es decir un total de 24 sectores.	Evidencia fotográfica por cada una de las intervenciones hechas en cada uno de los 4 sectores seleccionados.	100%
	Toma de bancos: se contemplan unas acciones de prevención en los bancos, que den cuenta de una socialización breve, y por medio de ayudas didácticas, de las recomendaciones que se deben tener los usuarios al momento de realizar transacciones bancarias (en línea o de manera presencial), para no caer como víctimas del ciber delito. Para ello, se espera contar previamente con la aceptación de las entidades bancarías que estarían dispuestas a recibir estos de espacios de socialización dentro de sus instalaciones, el cual contará con un equipo para lograr tal fin.	N/A	Evidencia fotografía de las entidades bancarias que se articulen en los procesos de sensibilización.	100%
IV	**Seminario Taller:** esta fase contempla el desarrollo de un seminario taller dirigido a las personas que componen el Comité de Seguridad Bancaria del Departamento del Atlántico.	1 (4horas)	Evidencia fotográfica, lista de asistencia y acta de realización de la actividad.	100%

Como se evidencia en el cuadro anterior, el presente proyecto ha cumplido con las dos primeras actividades, por lo que se expondrá a continuación.

1. INFORME DETALLADO CON EL DISEÑO PUBLICITARIA Y COMUNICACIONAL QUE SERVIRÁ PARA EL TRABAJO DE CAMPO EN LOS 6 MUNICIPIOS PRIORIZADOS

1.1. Metodología de Pedagogía social

LA PEDAGOGÍA SOCIAL es la metodología más adecuada para la socialización y sensibilización, además, la pedagogía social está relacionada fundamentalmente con la política y se concibe desde una clara estrategia preventiva.

Para Baumer, G. Von 1929: Significa la asistencia educativa otorgada por la sociedad y el estado fuera de la escuela y de la familia. Hehlmann 1957: Es la doctrina de la educación en la comunidad y de la educación por la sociedad y sus órganos.

Paciano Fermoso en 1994 dio su propio concepto sobre pedagogía social y dice que: Es la ciencia práctica social y educativa formal, no formal e informal que fundamenta, justifica y comprende la normatividad más adecuada para la prevención, ayuda y reinserción de quienes pueden padecer o padecen, a lo largo de toda su vida, deficiencias en la socialización o en la satisfacción de necesidades básicas amparadas por los derechos humanos.

Con estos insumos conceptuales para entender la metodología de la pedagogía social, podemos establecer que el presente proyecto implica dicha estrategia como mecanismo de prevención a aplicarse a la sociedad atlanticense objeto de intervención, frente a la ocurrencia o prevención del ciberdelito, pues muchas veces se desconocen o se carece de herramientas conceptuales básicas para poder identificarlos.

La metodología propuesta para el desarrollo del presente proyecto es de carácter pedagógico social, la cual brinda las herramientas necesarias para transmitir un conocimiento experto a otros individuos, con el fin de lograr el objetivo central del proyecto el cual está alineado a fomentar la ciber seguridad, la prevención del ciber delito y la promoción de la ciber convivencia en el territorio atlanticense.

Para el desarrollo del presente proyecto se espera llegar a la población flotante en espacios de interacción comercial, económico y de transacciones monetarias, las cuales pueden verse vulnerables ante el actuar delictivo de los ciberdelincuentes, es por ello que será importante la focalización, en los municipios priorizados para este proyecto, de lugares tales como: centros comerciales, entidades bancarias, cajeros automáticos y/o zonas comerciales.

En ese sentido, se desarrollará el diseño de la estrategia publicitaria y comunicacional. Bajo de la pedagogía social se seleccionarán las temáticas que servirán como contenido para las jornadas de sensibilización, por lo que se establecen las siguientes fases:

Fase I – Diseño de la estrategia de pedagogía social: a través de la cual se busca sensibilizar a la población objetivo con el fin de promocionar un mensaje de prevención y sensibilización sobre el delito cibernético, acompañado de un mensaje de ciberseguridad y ciber convivencia, esta fase estará a cargo del director, Coordinador Operativo y Coordinadores, fotógrafos, que contarán con un vehículo de dedicación exclusiva para el traslado a cada uno de los municipios.

Fase II – Identificación de los sectores: en la cual se busca focalizar los lugares que se recorrerán con el plan de sensibilización en cada uno de los municipios. Este ejercicio de focalización se hará en articulación con los gobiernos municipales, en una reunión en la que esté presente el Alcalde y/o el Secretario de Gobierno y el comandante de policía de los municipios o su delegado y estará cargo de los Coordinadores, con acompañamiento del personal de apoyo diurno, fotógrafos, para ello contarán con un vehículo de dedicación exclusiva para el traslado a cada uno de los municipios y material de trabajo como papelería.

Fase III- Implementación de la Estrategia en campo: Luego de identificar las zonas junto con un trabajo colaborativo con cada alcaldía local, se establecerá un cronograma de intervención en los lugares con las características anteriormente mencionadas.

- Tomas de bancos: una de las actividades con la que se espera impactar por medio del presente proyecto es la de prevenir el delito cibernético y sus diferentes modalidades en las entidades bancarias, para tal fin, se contemplan unas acciones de prevención en los bancos, que den cuenta de una socialización breve, y por medio de ayudas didácticas, de las recomendaciones que se deben tener los ciudadanos al momento de realizar transacción bancarias (en línea o de manera presencial), para no caer como victimas del ciber delito. Para ello, se espera contar previamente con la aceptación de las entidades bancarías que estarían dispuestas a recibir estos de espacios de socialización dentro de sus instalaciones, el cual contará con un equipo para lograr tal fin.

Fase IV- Seminario Taller: esta fase contempla el desarrollo de un seminario taller dirigido a las personas que componen el Comité de Seguridad Bancaria del Departamento del Atlántico. Los objetivos de este taller será dictar una conferencia magistral de un experto en seguridad cibernética y/o delitos informáticos, seguido de un taller en el que los asistentes logren capacitarse en las siguientes temáticas:

- Modalidades del delito cibernético en entidades bancarias
- Retos en ciberseguridad bancaria
- Protección y seguridad a los usuarios por entidades bancarias

1.2. Elementos conceptuales tenidos en cuenta para el diseño de la estrategia

Para hablar de ciberdelito, ciber seguridad y/o ciber convivencia es importante recurrir a los hechos históricos que permitieron elementos para su conceptualización y se establecieran dentro del dialecto común. Luego de la creación del internet en los años sesenta, cuando este pasó de uso exclusivo militar al huso en los hogares (finales de la última década del siglo XX) ocurrió una revolución acelerada de procesos y dinámicas que se gestaron desde la red. Las sociedades cambiaron y con ello el concepto de globalización se materializó en la entrada a un computador, los individuos en sociedad pudieron conectarse de manera muy diferente, a la distancia, realizando actividades que antes requerían movilizarse o su presencialidad. Sin embargo, este avance de la tecnología trajo consigo actividades diferentes al buen uso del internet.

La utilización del manejo de transacciones económicas electrónicas y el uso social de la red permitió que expertos en manejos informáticos afectaran las libertades individuales expuestas en línea, lo que permitió la ilegalidad o delitos cibernéticos, que fueron tipificados en la ley. En el X Congreso de las Naciones Unidas sobre la Prevención del Delito y el Tratamiento del Delincuente, llevado a cabo del 14 al 17 de abril del año 2000 en Viena, se estableció que el concepto de delito cibernético es entendido como “todo delito que puede cometerse por medio de un sistema o una red informática o contra un sistema o una red informática”, estos delitos estarán tipificados de acuerdo con la jurisprudencia establecida por cada Estado. En ese sentido, el ciberdelito “es el conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen un entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual”.

El avance tecnológico en materia informática trajo consigo nuevas dinámicas criminales. El ciber-espacio es sinónimo de nuevas oportunidades para todas las personas y comunidades, pero también un escenario de actividades delictivas de diversa índole. Desde comportamientos de acoso escolar y extorsión, hasta reclutamiento criminal. Esto representa un reto en materia de seguridad ciudadana, particularmente en cuanto a prevención, capacidades de persecución y articulación institucional, es por ello que la ciber-seguridad es un concepto fundamental que debe ser desarrollado, trabajado y liderado

desde la institucionalidad, con el fin de brindar un escenario de protección a los usuarios de las plataformas digitales.

La ciber-seguridad es una herramienta de protección que utilizan los individuos dentro de un escenario informático, que busca salvaguardar las libertades, sean estas personales, comerciales o de asociación. Este concepto engloba un sin número de técnicas o métodos para proteger o asegurar nuestro sistema del ciber-ataque o ciber-delito, sin embargo, también se genera ciber-seguridad cuando se gestan procesos de pedagogía a los ciudadanos en el buen uso del manejo de las tecnologías, por ello, de manera preventiva y por medio de las capacitaciones que se diseñen bajo esta temática, se busca consolidar una ciudadanía ciber segura en el Atlántico. Siguiendo esta lógica, la ciber convivencia son todos aquellos escenarios de uso común (Plataformas educativas, empresariales, redes sociales, etc.) donde confluyen más de un individuo en el que el manejo adecuado de estas garantiza una convivencia sana en estos escenarios virtuales.

¿Qué es el ciberdelito?

Es toda aquella acción antijurídica que se realiza en el entorno digital, espacio digital o de Internet. Ante el extendido uso y utilización de las nuevas tecnologías en todas las esferas de la vida (economía, cultura, industria, ciencia, educación, información, comunicación, etc.) y el creciente número de usuarios, consecuencia de la globalización digital de la sociedad, la delincuencia también se ha expandido a esa dimensión. Gracias al anonimato y a la información personal que se guarda en el entorno digital, los delincuentes han ampliado su campo de acción y los delitos y amenazas a la seguridad se han incrementado exponencialmente.

Tipos de ciberdelitos

La Piratería Informática: consiste en la violación ilegal del derecho de autor. Según la definición que en su artículo 51 brinda el ADPIC (Acuerdo sobre los aspectos de los Derechos de Propiedad Intelectual) son aquellas “mercaderías que lesionan el derecho de autor”. La piratería es una de las modalidades de reproducción técnica (la otra es la -reproducción burda del original cuya apariencia dista mucho de la auténtica), que implica la elaboración de una copia semejante al original, con la intención de hacerla pasar por tal.

La apropiación o hurto de software y datos: Es una modalidad de la piratería informática. En este caso el sujeto accede a un computador ajeno o a la sesión de otro usuario, retirando archivos informáticos, mediante la ejecución de los comandos copiar o cortar, para luego guardar ese contenido en un soporte propio.

Robo de identidad: Luego de obtener los datos personales de un individuo, se procede a realizar todo tipo de operaciones para provecho del victimario, fingiendo ser la persona a la que se extrajo su información sensible. Encuadra como delito de estafa. Si el actuar del sujeto activo comporta dar a conocer datos personales ajenos contenidos en base de datos a las que por su empleo tiene acceso, entonces por expreso mandato legal la figura aplicable es la de revelación de secreto profesional.

Estafa: Este tipo de delito se comete a través del robo de identidad. Los criminales utilizan técnicas como el spam, webs falsas o softwares ilegales para engañar a las víctimas y robarles las contraseñas o claves personales. De esta manera, acceden a información confidencial. Un ejemplo de ello es el acceso a datos bancarios.

Cajeros Automáticos: Conductas mediante las cuales se logra retirar dinero del cajero automático, utilizando una tarjeta magnética robada, o los números de la clave para el acceso a la cuenta con fondos. El ataque de ATM Jackpotting es parte de estas conductas. El ataque aprovecha las vulnerabilidades en las máquinas para instalar firmware malicioso y retirar efectivo de un cajero automático sin usar una cuenta bancaria autenticada.

Suplantación De Identidad: Relacionado con lo anterior, la suplantación de identidad sucede cuando la estafa tiene éxito y el criminal obtiene acceso a la información personal. Una vez obtenida, el criminal puede realizar compras, llegando a arruinar a la víctima, o hacerse pasar por la persona a quien ha robado los datos. Estas son algunas formas de obtener dichos datos:

Phishing: Los ciberdelincuentes utilizan “cebos”, mensajes fraudulentos para atraer a sus víctimas hacia sitios falsificados, de modo que introduzcan en ellos información personal como nombres de usuario, contraseñas y datos bancarios.

PHARMING: El pharming va un paso más allá del phishing y utiliza malware para redirigir a los usuarios desprevenidos hacia versiones falsificadas de sitios web, con el fin de que introduzcan sus datos personales.

Keylogging: Este tipo de malware (o, para ser más específicos, de spyware) registra en secreto todo lo que escribe para obtener información de sus cuentas y otros datos personales.

Sniffing: Si se conecta a una red Wi-Fi pública no protegida y no cifrada, los hackers pueden robarle los datos “olfateando” su tráfico de Internet con herramientas especiales (salvo que utilice una VPN, por supuesto).

Sexting: En su significado más puro y actual, es la producción de imágenes propias (fotografías o vídeos) de alto contenido erótico o pornográfico y su envío a otra persona mediante el teléfono móvil. Realizar sexting, por lo tanto, no supone un daño en sí mismo para quien lo realiza salvo que su producción o envío pudiera tener consecuencias legales directas, como ocurre en alguno de estos casos donde, por ejemplo, la imagen:

- puede ser calificada de pornografía infantil.
- incluye otras personas que no han consentido su producción o difusión.
- es de alto voltaje y enviada a menores o incapaces.

1.3. Actividades diseñadas

Tomas de bancos y lugares comerciales en los municipios

Una de las actividades con la que se espera impactar por medio del presente proyecto es la de prevenir el delito cibernético y sus diferentes modalidades en las entidades bancarias, para tal fin, se contemplan unas acciones de prevención en los bancos, que den cuenta de una socialización breve, y por medio de ayudas didácticas, de las recomendaciones que se deben tener los ciudadanos al momento de realizar transacción bancarias (en línea o de manera presencial), para no caer como víctimas del ciber delito. Para ello, se espera contar previamente con la aceptación de las entidades bancarías que estarían dispuestas a recibir estos de espacios de socialización dentro de sus instalaciones, el cual contará con un equipo para lograr tal fin.

1.4. Cronograma de intervención

CRONOGRAMA PREVENCIÓN CIBERDELITOS				
MUNICIPIO	DURACIÓN	LUGARES	ESTRATEGIA	FOCALIZACIÓN
Soledad	Inicio 9:00 A.M Finalización 3:00 P.M	Carrera 19 con calle 18 hasta calle 26. Zona centro. Colegio John F Kennedy (Barrio San Antonio)	Pedagogía Preventiva	Sector: Educación / Comercio
Baranoa	Inicio 9:00 A.M Finalización 4:00 P.M	Perímetro plaza principal. Corredor gastronómico. Colegio Caldas-Enssa. Banco Agrario.	Pedagogía Preventiva / Toma de Banco	Sector: Educación / Comercio
Sabanalarga	Inicio 9:00 A.M Finalización 4:00 P.M	Perímetro plaza principal. Mercado nuevo y viejo. Colegio NN. Banco Agrario. Bancolombia	Pedagogía Preventiva / Toma de Banco	Sector: Educación / Comercio
Soledad	Inicio 2:00 P.M Finalización 4:00 P.M	Banco BBVA	Toma de Banco	Sector: Comercio
Puerto Colombia	Inicio 9:00 A.M Finalización 12:00 P.M	IED Francisco Javier Sisnero	Pedagogía Preventiva	Sector: Educación
Puerto Colombia	Inicio 9:00 A.M Finalización 3:00 P.M	Plaza Central. Carrera 10 entre calle 7 y 11. Loma Fresca. Villa Campestre. Corredor Universitario. Bancolombia	Pedagogía Preventiva / Toma de Banco	Sector: Educación / Comercio

Galapa	Inicio 9:00 A.M Finalización 4:00 P.M	Colegio Francisco de Paula Santander. Plaza central. Villa Olímpica. Mundo Feliz. Bancolombia (Principal)	Pedagogía Preventiva / Toma de Banco	Sector: Educación / Comercio
Malambo	Inicio 9:00 A.M Finalización 4:00 P.M	Centro Comercial. Pinsa. Perímetro estación de Policía. Colegio Juan 23, Socorro, Quevedo. Bancolombia	Pedagogía Preventiva / Toma de Banco	Sector: Educación / Comercio

1.5. Piezas de diseño para la estrategia

Ilustración 1. Folletos





Ilustración 2. Afiche



Pendodones:

CORPODESC
CORPORACIÓN TÉCNICA PARA EL DESARROLLO HUMANO SOCIAL Y CULTURAL DE COLOMBIA

Atlántico más Seguro para la Gente



CIBERDELITOS

ES UN HONOR SER POLICÍA

Atlántico para la Gente

GOBERNACIÓN DEL ATLÁNTICO

CORPODESC
CORPORACIÓN TÉCNICA PARA EL DESARROLLO HUMANO SOCIAL Y CULTURAL DE COLOMBIA

Atlántico más Seguro para la Gente



CIBERDELITOS

Para prevenir ciberdelitos:

1. Ten cuidado con los mensajes de correo electrónico que contienen enlaces sospechosos o archivos adjuntos que no esperabas.
2. No descargues nada de fuentes desconocidas.
3. Asegúrate de que estás utilizando un sitio web legítimo antes de introducir información personal.
4. Emplea contraseñas seguras y exclusivas: No reutilices la misma contraseña para varias cuentas.
5. Nunca facilites tus datos bancarios, contraseñas o envío de dinero, a solicitudes vía email o telefónica.

ES UN HONOR SER POLICÍA

Atlántico para la Gente

GOBERNACIÓN DEL ATLÁNTICO

CORPODESC
CORPORACIÓN TÉCNICA PARA EL DESARROLLO HUMANO SOCIAL Y CULTURAL DE COLOMBIA

Cuidando de nuestra salud
construimos un

Atlántico más Seguro

La mejor prevención está en tus manos.



Uso permanente de tapabocas.



Lavado de manos constante.



Mantén la distancia.

ES UN HONOR SER POLICÍA

Atlántico para la Gente

GOBERNACIÓN DEL ATLÁNTICO

Ilustración 3. Camisetas







Ilustración 4. Gorras Modelo 1.





Ilustración 5. Gorras modelo 2.



Atlántico
más Seguro
para la Gente

GOBERNACIÓN DEL
ATLÁNTICO

Ilustración 6. Chaleco







Ilustración 7. Escarapela



Ilustración 8. Tropezón



2. REUNIONES PARA LA IDENTIFICACIÓN DE LOS SECTORES EN LOS MUNICIPIOS

FECHA: junio 29 2022.	**ACTIVIDAD:** Identificación de sectores a intervenir por medio de un análisis cualitativo de los principales riesgos asociados a los ciberdelitos, presentes en los municipios priorizados y a intervenir, en articulación con la Policía Nacional y las Administraciones Municipales.	**MUNICIPIO:** Baranoa.
OBJETIVO DE LA ACTIVIDAD	Identificar los sectores a intervenir en los 6 municipios priorizados, de los cuales Baranoa es uno de ellos. En cada uno de estos municipios se realizarán reuniones y a través de estas, se recolectarán datos, se focalizarán los sectores o lugares a intervenir con la estrategia de pedagogía social en la temática de Delitos Cibernéticos a su vez, que se elegirá el banco a intervenir en la estrategia llamada "Toma de bancos". Este ejercicio de focalización se hará en articulación con los Gobiernos municipales, por medio de los secretarios de Gobierno, y el comandante de la Policía o su delegado.	**DURACIÓN: 1 hora.**
CARACTERÍSTICAS DEL MUNICIPIO.	Baranoa es un municipio del Atlántico, ubicado en el centro y que limita con municipios como Galapa o Sabanalarga. Baranoa es ampliamente conocido por su cultura gastronómica y su zona central, en la cual se encuentra ubicada una gran parte del comercio del municipio. Es uno de los municipios más grandes del departamento y con mayor población de este.	
DESCRIPCIÓN DE LA JORNADA.	La actividad en el municipio de Baranoa inicia las 2:00pm en las instalaciones de la Alcaldía de Baranoa. La actividad contó con la presencia del comandante de la policía y el secretario de Gobierno del municipio de Baranoa. La actividad, se inició mediante de una serie de preguntas orientadas al desarrollo de delitos cibernéticos en el municipio, para poder	

	conocer y priorizar lugares o sectores de alto riesgo, asimismo como población vulnerable a este tipo de delitos. Asimismo, se recalcó la importancia de que la ciudadanía pueda conocer cuáles son estos tipos de delitos, para que pueda identificarlos y evitar que estos sucedan, como a su vez sepa cómo actuar cuando sea víctima de uno de estos delitos cibernéticos. Por parte del equipo de la Gobernación del Atlántico, se dio a conocer el objetivo principal de la actividad a realizar durante la intervención con pedagogía social y su metodología. A su vez, se enseñó la llamada “toma de banco” que consiste en escoger el banco de mayor concurrencia de la ciudad para realizar, al interior de este, la pedagogía específica de delitos cibernéticos que puedan presentarse en estos lugares o con los usuarios de los bancos posterior a la intervención en los sectores priorizados más adelante en la reunión. Durante el ejercicio, se escogieron los lugares o sectores de intervención por medio del equipo interdisciplinario de la Gobernación del Atlántico. Estos lugares fueron propuestos por los representantes del municipio debido a la vulnerabilidad que tienen de sufrir este tipo de delitos cibernéticos. Así, se escogieron los siguientes sectores o lugares a trabajar el día 15 de julio del año 2022: - Institución Educativa Francisco José de Caldas. - Sector comercio en la zona perimetral de la plaza principal del municipio de Baranoa. - Corredor gastronómico. El banco elegido para la actividad de “Toma de Banco” fue propuesto por parte de los representantes del municipio debido a que está en un sector muy concurrido y es el más grande de Baranoa. Se escogió el Banco Agrario, ubicado en el centro del municipio. Posterior a la elección de los lugares o sectores a impactar, se pidió acompañamiento por parte de la Policía Nacional PRECI y Policía

	Nacional de Infancia y Adolescencia. Este último debido a que uno de los lugares priorizados fue una institución educativa. Los representantes del municipio manifestaron a través de la reunión, que actualmente las campañas de prevención al delito cibernético son pocas dentro del municipio y que es de gran ayuda el apoyo de la Gobernación del Atlántico.
RECURSOS	**MATERIALES PEDAGÓGICOS** Computador **MATERIAL HUMANDO** Equipo representante de la Gobernación del Atlántico Secretario de Gobierno Comandante de la Policía del municipio de Baranoa

EVIDENCIA FOTOGRÁFICAS



FECHA: junio 29 2022.	**ACTIVIDAD:** Identificación de sectores a intervenir por medio de un análisis cualitativo de los principales riesgos asociados a los ciberdelitos, presentes en los municipios priorizados y a intervenir, en articulación con la Policía Nacional y las Administraciones Municipales.	**MUNICIPIO:** Baranoa.
OBJETIVO DE LA ACTIVIDAD	Identificar los sectores a intervenir en los 6 municipios priorizados, de los cuales Baranoa es uno de ellos. En cada uno de estos municipios se realizarán reuniones y a través de estas, se recolectarán datos, se focalizarán los sectores o lugares a intervenir con la estrategia de pedagogía social en la temática de Delitos Cibernéticos a su vez, que se elegirá el banco a intervenir en la estrategia llamada “Toma de bancos”.	**DURACIÓN: 1 hora.**

	Este ejercicio de focalización se hará en articulación con los Gobiernos municipales, por medio de los secretarios de Gobierno, y el comandante de la Policía o su delegado.	
CARACTERÍSTICAS DEL MUNICIPIO.	Baranoa es un municipio del Atlántico, ubicado en el centro y que limita con municipios como Galapa o Sabanalarga. Baranoa es ampliamente conocido por su cultura gastronómica y su zona central, en la cual se encuentra ubicada una gran parte del comercio del municipio. Es uno de los municipios más grandes del departamento y con mayor población de este.	
DESCRIPCIÓN DE LA JORNADA.	La actividad en el municipio de Baranoa inicia las 2:00pm en las instalaciones de la Alcaldía de Baranoa. La actividad contó con la presencia del comandante de la policía y el secretario de Gobierno del municipio de Baranoa. La actividad, se inició mediante de una serie de preguntas orientadas al desarrollo de delitos cibernéticos en el municipio, para poder conocer y priorizar lugares o sectores de alto riesgo, asimismo como población vulnerable a este tipo de delitos. Asimismo, se recalcó la importancia de que la ciudadanía pueda conocer cuáles son estos tipos de delitos, para que pueda identificarlos y evitar que estos sucedan, como a su vez sepa cómo actuar cuando sea víctima de uno de estos delitos cibernéticos. Por parte del equipo de la Gobernación del Atlántico, se dio a conocer el objetivo principal de la actividad a realizar durante la intervención con pedagogía social y su metodología. A su vez, se enseñó la llamada “toma de banco” que consiste en escoger el banco de mayor concurrencia de la ciudad para realizar, al interior de este, la pedagogía específica de delitos cibernéticos que puedan presentarse en estos lugares o con los usuarios de los bancos posterior a la intervención en los sectores priorizados más adelante en la reunión. Durante el ejercicio, se escogieron los lugares o sectores de intervención por medio del equipo interdisciplinario de la Gobernación del Atlántico. Estos lugares fueron propuestos por los representantes	

	del municipio debido a la vulnerabilidad que tienen de sufrir este tipo de delitos cibernéticos. Así, se escogieron los siguientes sectores o lugares a trabajar el día 15 de julio del año 2022: - Institución Educativa Francisco José de Caldas. - Sector comercio en la zona perimetral de la plaza principal del municipio de Baranoa. - Corredor gastronómico. El banco elegido para la actividad de “Toma de Banco” fue propuesto por parte de los representantes del municipio debido a que está en un sector muy concurrido y es el más grande de Baranoa. Se escogió el Banco Agrario, ubicado en el centro del municipio. Posterior a la elección de los lugares o sectores a impactar, se pidió acompañamiento por parte de la Policía Nacional PRECI y Policía Nacional de Infancia y Adolescencia. Este último debido a que uno de los lugares priorizados fue una institución educativa. Los representantes del municipio manifestaron a través de la reunión, que actualmente las campañas de prevención al delito cibernético son pocas dentro del municipio y que es de gran ayuda el apoyo de la Gobernación del Atlántico.
RECURSOS	**MATERIALES PEDAGÓGICOS** Computador **MATERIAL HUMANDO** Equipo representante de la Gobernación del Atlántico Secretario de Gobierno Comandante de la Policía del municipio de Baranoa

EVIDENCIA FOTOGRÁFICAS



FECHA: junio 29 2022.	**ACTIVIDAD:** Identificación de sectores a intervenir por medio de un análisis cualitativo de los principales riesgos asociados a los ciberdelitos, presentes en los municipios priorizados y a intervenir, en articulación con la Policía Nacional y las Administraciones Municipales.	**MUNICIPIO:** Sabanalarga.
OBJETIVO DE LA ACTIVIDAD	Identificación de sectores a intervenir en los 6 municipios priorizados, de los cuales Sabanalarga es uno de ellos. En cada uno de estos municipios se realizarán reuniones y a través de estas, se recolectarán datos, se focalizarán los sectores o lugares a intervenir con la estrategia de pedagogía social en la temática de Delitos Cibernéticos	**DURACIÓN: 1 hora.**

	a su vez, que se elegirá el banco a intervenir en la estrategia llamada “Toma de bancos”. Este ejercicio de focalización se hará en articulación con los Gobiernos municipales, por medio de los secretarios de Gobierno/Interior, y el comandante de la Policía o su delegado.	
CARACTERÍSTICAS DEL MUNICIPIO.	Este municipio se encuentra situado en el centro del Departamento del Atlántico. Sabanalarga es uno de los municipios más poblados del departamento y con uno de los sectores comerciales más grandes. Es un municipio que cuenta con calles pavimentadas, parques y fachadas en buen estado, así como una iglesia y plaza llamativa al centro del municipio.	
DESCRIPCIÓN DE LA JORNADA.	La actividad en el municipio de Sabanalarga inicia las10:00am en las instalaciones de la Alcaldía de Sabanalarga, ubicada en el centro de la ciudad. La actividad contó con la presencia del comandante de la policía y el secretario de Interior del municipio de Sabanalarga. La actividad, se abre por medio de una serie de preguntas orientadas al desarrollo de delitos cibernéticos en el municipio, para poder relacionar lugares o sectores de alto riesgo, asimismo como población vulnerable a este tipo de delitos. Asimismo, se recalcó la importancia de que la ciudadanía pueda conocer cuáles son estos tipos de delitos, para que pueda identificarlos y evitar que estos sucedan, como a su vez sepa cómo actuar cuando sea víctima de uno de estos delitos cibernéticos. Posteriormente, por parte del equipo de la Gobernación del Atlántico, se hizo mención del propósito principal de las actividades a realizar durante la intervención con pedagogía social y su metodología. Asimismo, se propuso una llamada “toma de banco” en la cual, se escogería el banco de mayor concurrencia de la ciudad para realizar la pedagogía específica de delitos cibernéticos que puedan presentarse en estos lugares o con los usuarios de los bancos. Durante la reunión, se escogieron los lugares o sectores de intervención por medio del equipo interdisciplinario de la Gobernación del Atlántico. Estos lugares fueron propuestos por los representantes del municipio debido a la vulnerabilidad que tienen de sufrir este tipo de delitos cibernéticos.	

	Así, se escogieron los siguientes sectores o lugares a trabajar el día 18 de julio del año 2022: - Institución Educativa a elección de los representantes del municipio. - Sector comercio en la zona perimetral de la plaza principal del municipio de Sabanalarga. - El Mercado nuevo y el Mercado viejo. - Bancolombia de la plaza principal del municipio de Sabanalarga. El banco elegido para la actividad de “Toma de Banco” fue propuesto por parte de los representantes del municipio debido a que está en un sector muy concurrido y es el más grande de Sabanalarga. Posterior a la elección de los lugares o sectores a impactar, se pidió acompañamiento por parte de la Policía Nacional PRECI y Policía Nacional de Infancia y Adolescencia. Este último debido a que uno de los lugares priorizados fue una institución educativa. Los representantes del municipio manifestaron a través de la reunión, que actualmente las campañas de prevención al delito cibernético son pocas dentro del municipio y que es de gran ayuda el apoyo de la Gobernación del Atlántico.
RECURSOS	**MATERIALES PEDAGÓGICOS** Computador **MATERIAL HUMANDO** Equipo representante de la Gobernación del Atlántico Secretario de Interior Comandante de la Policía del municipio de Sabanalarga

EVIDENCIA FOTOGRÁFICAS





FECHA: junio 30 2022.	**ACTIVIDAD:** Identificación de sectores a intervenir por medio de un análisis cualitativo de los principales riesgos asociados a los ciberdelitos, presentes en los municipios priorizados y a intervenir, en articulación con la Policía Nacional y las Administraciones Municipales.	**MUNICIPIO:** Soledad.

OBJETIVO DE LA ACTIVIDAD	Identificación de sectores a intervenir en los 6 municipios priorizados, de los cuales Soledad es uno de ellos. En cada uno de estos municipios se realizarán reuniones y a través de estas, se recolectarán datos, se focalizarán los sectores o lugares a intervenir con la estrategia de pedagogía social en la temática de Delitos Cibernéticos a su vez, que se elegirá el banco a intervenir en la estrategia llamada "Toma de bancos". Este ejercicio de focalización se hará en articulación con los Gobiernos municipales, por medio de los secretarios de Gobierno, y el comandante de la Policía o su delegado.	**DURACIÓN: 1 hora.**
CARACTERÍSTICAS DEL MUNICIPIO.	El municipio de soledad se encuentra dentro del Área Metropolitana de Barranquilla y su área urbana se encuentra conurbada con la ciudad de Barranquilla. Es uno de los municipios más grandes de la región Caribe a su vez que el tercer más poblado de esta. Soledad se caracteriza por su gran tamaño y sector comercial. Cuenta con centros comerciales y un sector industrial importante del departamento.	
DESCRIPCIÓN DE LA JORNADA.	La reunión en el municipio de Soledad inicia las 2:00pm en las instalaciones de la nueva Alcaldía de Soledad. La actividad contó con la presencia del comandante de la policía y el secretario de Interior del municipio. Se inició la reunión por medio de una serie de preguntas orientadas al desarrollo de delitos cibernéticos en el municipio, para poder relacionar lugares o sectores de alto riesgo, asimismo como población vulnerable a este tipo de delitos. Recalcándose a su vez, la importancia de que la ciudadanía pueda conocer cuáles son estos tipos de delitos, para que pueda identificarlos y evitar que estos sucedan, como a su vez sepa cómo actuar cuando sea víctima de uno de estos delitos cibernéticos. Posteriormente, por parte del equipo de la Gobernación del Atlántico, se hizo mención del propósito principal de las actividades a realizar durante la intervención con pedagogía social y su metodología.	

	Asimismo, se propuso una llamada “toma de banco” por medio de la cual, se escogería el banco de mayor concurrencia de la ciudad para realizar la pedagogía específica de delitos cibernéticos que puedan presentarse en estos lugares o con los usuarios de los bancos. Durante la reunión, se escogieron los lugares o sectores de intervención por medio del equipo interdisciplinario de la Gobernación del Atlántico. Estos lugares fueron propuestos por los representantes del municipio debido a la vulnerabilidad que tienen de sufrir este tipo de delitos cibernéticos. Así, se escogió la siguiente institución y sector a trabajar el día 14 de julio del año 2022: - Institución Educativa John F. Kennedy en el barrio San Antonio. - Sector comercio centro histórico (Carrera 19) Para la actividad de “Toma de Banco”, se escogió el Banco BBVA de la Calle 18 (centro), debido a su alta concurrencia. Se concertó la fecha del 19 de julio del presente año para la realización de esta actividad. Posterior a la elección de los lugares o sectores a impactar, se pidió acompañamiento por parte de la Policía Nacional PRECI y Policía Nacional de Infancia y Adolescencia. Este último debido a que uno de los lugares priorizados fue una institución educativa. Los representantes del municipio manifestaron a través de la reunión, que actualmente las campañas de prevención al delito cibernético son pocas dentro del municipio y que es de gran ayuda el apoyo de la Gobernación del Atlántico.
RECURSOS	**MATERIALES PEDAGÓGICOS** Computador **MATERIAL HUMANDO**

	Equipo representante de la Gobernación del Atlántico Secretario de Gobierno Comandante de la Policía del municipio de Soledad

EVIDENCIA FOTOGRÁFICAS





FECHA: junio 30 2022.	**ACTIVIDAD:** Identificación de sectores a intervenir por medio de un análisis cualitativo de los principales riesgos asociados a los ciberdelitos, presentes en los municipios priorizados y a intervenir, en articulación con la Policía Nacional y las Administraciones Municipales.	**MUNICIPIO:** Puerto Colombia.
OBJETIVO DE LA ACTIVIDAD	Identificación de sectores a intervenir en los 6 municipios priorizados, de los cuales Puerto Colombia es uno de ellos. En cada uno de estos municipios se realizarán reuniones y a través de estas, se recolectarán datos, se focalizarán los sectores o lugares a intervenir con la estrategia de pedagogía social en la temática de Delitos Cibernéticos a su vez, que se elegirá el banco a intervenir en la	**DURACIÓN: 1 hora.**

	estrategia llamada “Toma de bancos”. Este ejercicio de focalización se hará en articulación con los Gobiernos municipales, por medio de los secretarios de Gobierno, y el comandante de la Policía o su delegado.	
CARACTERÍSTICAS DEL MUNICIPIO.	El municipio de Puerto Colombia se encuentra ubicado al noroccidente del departamento del Atlántico y limita al norte y occidente con las costas del Mar Caribe. Cuenta con una gran tradición turística y con recientes arreglos a su zona central, la cual cuenta con una nueva plaza y una zona de malecón muy llamativa. Este municipio pertenece al Área Metropolitana de Barranquilla.	
DESCRIPCIÓN DE LA JORNADA.	La reunión en el municipio de Puerto Colombia inicia las 10:00am en las instalaciones de la Alcaldía de Puerto Colombia, ubicada en el centro de la ciudad. La actividad contó con la presencia del comandante de la policía y el secretario de Interior del municipio. La actividad, se dio inicio por medio de una serie de preguntas orientadas al desarrollo de delitos cibernéticos en el municipio, para poder relacionar lugares o sectores de alto riesgo, asimismo como población vulnerable a este tipo de delitos. Asimismo, se recalcó la importancia de que la ciudadanía pueda conocer cuáles son estos tipos de delitos, para que pueda identificarlos y evitar que estos sucedan, como a su vez sepa cómo actuar cuando sea víctima de uno de estos delitos cibernéticos. Posteriormente, por parte del equipo de la Gobernación del Atlántico, se hizo mención del propósito principal de las actividades a realizar durante la intervención con pedagogía social y su metodología. Asimismo, se propuso una llamada “toma de banco” por medio de la cual, se escogería el banco de mayor concurrencia de la ciudad para realizar la pedagogía específica de delitos cibernéticos que puedan presentarse en estos lugares o con los usuarios de los bancos. Durante la reunión, se escogieron los lugares o sectores de intervención por medio del equipo interdisciplinario de la Gobernación del Atlántico. Estos lugares fueron propuestos por los representantes del municipio	

	debido a la vulnerabilidad que tienen de sufrir este tipo de delitos cibernéticos. Así, se escogió la siguiente institución a trabajar el día 19 de julio del año 2022: - Institución Educativa Francisco Javier Cisneros. A su vez se escogieron otros sectores a trabajar el día 22 de julio del año 2022: - Zona perimetral de la plaza principal. - Sector comercial de Villa Campestre. El banco elegido para la actividad de “Toma de Banco” fue el Banco BBVA del centro, propuesto por parte de los representantes del municipio debido a que está en un sector muy concurrido y es el más grande de Puerto Colombia. Posterior a la elección de los lugares o sectores a impactar, se pidió acompañamiento por parte de la Policía Nacional PRECI y Policía Nacional de Infancia y Adolescencia. Este último debido a que uno de los lugares priorizados fue una institución educativa. Los representantes del municipio manifestaron a través de la reunión, que actualmente las campañas de prevención al delito cibernético son pocas dentro del municipio y que es de gran ayuda el apoyo de la Gobernación del Atlántico.
RECURSOS	**MATERIALES PEDAGÓGICOS** Computador **MATERIAL HUMANDO** Equipo representante de la Gobernación del Atlántico Secretario de Gobierno Comandante de la Policía del municipio de Puerto Colombia

EVIDENCIA FOTOGRÁFICAS





FECHA: junio 28 2022.	**ACTIVIDAD:** Identificación de sectores a intervenir por medio de un análisis cualitativo de los principales riesgos asociados a los ciberdelitos, presentes en los municipios priorizados y a intervenir, en articulación con la Policía Nacional y las Administraciones Municipales.	**MUNICIPIO:** Malambo.
OBJETIVO DE LA ACTIVIDAD	Identificar los sectores a intervenir en los 6 municipios priorizados, de los cuales Malambo es uno de ellos. En cada uno de estos municipios se realizarán reuniones y a través de estas, se recolectarán datos, se focalizarán los sectores o lugares a intervenir con la estrategia de pedagogía social en la temática de Delitos Cibernéticos a su vez, que se elegirá el banco a intervenir en la estrategia llamada "Toma de bancos". Este ejercicio de focalización se hará en articulación con los Gobiernos municipales, por medio de los secretarios de Gobierno, y el Comandante de la Policía o su delegado.	**DURACIÓN: 1 hora.**
CARACTERÍSTICAS DEL MUNICIPIO.	Este municipio se encuentra ubicado a las afueras de Barranquilla y hace parte del Área Metropolitana de Barranquilla. Malambo es un municipio con un gran sector comercial e industrial debido a su ubicación en una de las salidas más importantes de la ciudad de Barranquilla. Cuenta con pavimentación y es uno de los municipios más grandes del departamento del atlántico, así como uno de los más poblados.	
DESCRIPCIÓN DE LA JORNADA.	La actividad en el municipio de Malambo inicia las 3:45pm en las instalaciones de la Alcaldía de Malambo sede Sur. La actividad contó con la presencia del comandante de la policía y el secretario de Gobierno del municipio de Malambo.	

	La actividad, se abre por medio de una serie de preguntas orientadas al desarrollo de delitos cibernéticos en el municipio, para poder relacionar lugares o sectores de alto riesgo, asimismo como población vulnerable a este tipo de delitos. Asimismo, se recalcó la importancia de que la ciudadanía pueda conocer cuales son estos tipos de delitos, para que pueda identificarlos y evitar que estos sucedan, como a su vez sepa cómo actuar cuando sea víctima de uno de estos delitos cibernéticos. Por parte del equipo de la Gobernación del Atlántico, se expuso el objetivo principal de la actividad a realizar durante la intervención con pedagogía social y su metodología. A su vez, se explicó una llamada “toma de banco” por medio de la cual, se escogería el banco de mayor concurrencia de la ciudad para realizar, al interior de este, la pedagogía específica de delitos cibernéticos que puedan presentarse en estos lugares o con los usuarios de los bancos posterior a la intervención en los sectores priorizados más adelante en la reunión. Durante el ejercicio, se escogieron los lugares o sectores de intervención por medio del equipo interdisciplinario de la Gobernación del Atlántico. Estos lugares fueron propuestos por los representantes del municipio debido a la vulnerabilidad que tienen de sufrir este tipo de delitos cibernéticos. Así, se escogieron los siguientes sectores o lugares a trabajar el día 26 de julio del año 2022: - Institución Educativa Francisco Quevedo. - Sector comercio en la zona perimetral de la plaza principal del municipio de Malambo. - Centro Comercial Plaza Malambo. El banco elegido para la actividad de “Toma de Banco” fue propuesto por parte de los representantes del municipio debido a que está en un sector muy concurrido y es el más grande de Malambo. Se escogió el Bancolombia de Malambo, ubicado en la Calle 10.

	Posterior a la elección de los lugares o sectores a impactar, se pidió acompañamiento por parte de la Policía Nacional PRECI y Policía Nacional de Infancia y Adolescencia. Este último debido a que uno de los lugares priorizados fue una institución educativa. Los representantes del municipio manifestaron a través de la reunión, que actualmente las campañas de prevención al delito cibernético son pocas dentro del municipio y que es de gran ayuda el apoyo de la Gobernación del Atlántico.
RECURSOS	**MATERIALES PEDAGÓGICOS** Computador **MATERIAL HUMANDO** Equipo representante de la Gobernación del Atlántico Secretario de Gobierno Comandante de la Policía del municipio de Malambo

EVIDENCIA FOTOGRÁFICAS



FECHA: junio 28 2022.	**ACTIVIDAD:** Identificación de sectores a intervenir por medio de un análisis cualitativo de los principales riesgos asociados a los ciberdelitos, presentes en los municipios priorizados y a intervenir, en articulación con la Policía Nacional y las Administraciones Municipales.	**MUNICIPIO:** Galapa.
OBJETIVO DE LA ACTIVIDAD	Identificación de sectores a intervenir en los 6 municipios priorizados, de los cuales Galapa es uno de ellos. En cada uno de estos municipios se realizarán reuniones y a través de estas, se recolectarán datos, se focalizarán los sectores o lugares a intervenir con la estrategia de pedagogía	**DURACIÓN: 1 hora.**

	social en la temática de Delitos Cibernéticos a su vez, que se elegirá el banco a intervenir en la estrategia llamada “Toma de bancos”. Este ejercicio de focalización se hará en articulación con los Gobiernos municipales, por medio de los secretarios de Gobierno, y el Comandante de la Policía o su delegado.	
CARACTERÍSTICAS DEL MUNICIPIO.	El municipio de Galapa se encuentra ubicado dentro del área metropolitana de Barranquilla siendo uno de los municipios más cercados a la ciudad de Barranquilla. Este municipio cuenta con calles pavimentadas en su mayoría y con un alto movimiento de personas que se transportan a la ciudad de Barranquilla todos los días por la vía de la Cordialidad. Cuenta con una plaza e iglesia llamativa y con un centro grande de comercio.	
DESCRIPCIÓN DE LA JORNADA.	La actividad en el municipio de Galapa inicia las 2:00pm en las instalaciones de la Estación de Policía de Galapa, ubicada en la vía de la Cordialidad. La actividad contó con la presencia del comandante de la policía y el secretario de Gobierno del municipio de Galapa. Durante la actividad, se abre por medio de una serie de preguntas orientadas al desarrollo de delitos cibernéticos en el municipio, para poder relacionar lugares o sectores de alto riesgo, asimismo como población vulnerable a este tipo de delitos. Asimismo, se recalcó la importancia de que la ciudadanía pueda conocer cuales son estos tipos de delitos, para que pueda identificarlos y evitar que estos sucedan, como a su vez sepa cómo actuar cuando sea víctima de uno de estos delitos cibernéticos. Posteriormente, por parte del equipo de la Gobernación del Atlántico, se expuso el propósito principal de las actividades a realizar durante la intervención con pedagogía social y su metodología. Asimismo, se propuso una “toma de bancos” en las cuales, posterior a la intervención en los sectores priorizados más adelante en la reunión, se escogería el banco de mayor concurrencia de la ciudad para realizar la pedagogía específica de delitos cibernéticos que puedan presentarse en estos lugares o con los usuarios de los bancos. Durante el ejercicio, se escogieron los lugares o sectores de intervención por medio del equipo interdisciplinario de la Gobernación del Atlántico. Estos lugares fueron propuestos por los representantes	

	del municipio debido a la vulnerabilidad que tienen de sufrir este tipo de delitos cibernéticos. Así, se escogieron los siguientes sectores o lugares a trabajar el día 25 de julio del año 2022: - Institución Educativa Francisco de Paula Santander. - Sector comercio en la zona perimetral de la plaza principal del municipio de Galapa. - El barrio de Villa Olímpica. - Bancolombia de la plaza principal del municipio de Galapa. El banco elegido para la actividad de “Toma de Banco” fue propuesto por parte de los representantes del municipio debido a que está en un sector muy concurrido y es el más grande de Galapa. Posterior a la elección de los lugares o sectores a impactar, se pidió acompañamiento por parte de la Policía Nacional PRECI y Policía Nacional de Infancia y Adolescencia. Este último debido a que uno de los lugares priorizados fue una institución educativa. Los representantes del municipio manifestaron a través de la reunión, que actualmente las campañas de prevención al delito cibernético son pocas dentro del municipio y que es de gran ayuda el apoyo de la Gobernación del Atlántico.
RECURSOS	**MATERIALES PEDAGÓGICOS** Computador **MATERIAL HUMANDO** Equipo representante de la Gobernación del Atlántico Secretario de Gobierno Comandante de la Policía del municipio de Galapa

EVIDENCIA FOTOGRÁFICAS


Secretaría
del Interior
y Gobierno

JORNADAS DE PEDAGOGÍA SOCIAL

Las jornadas de pedagogía social consistió la implementación de la estrategia publicitaria y comunicacional, por medio de la cual se buscó sensibilizar a la comunidad de los sectores anteriormente seleccionados. A continuación, la evidencia correspondiente a este apartado.

FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
01/08/2022	Ciberdelito	Baranoa	Corredor gastronómico
OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.		
DESARROLLO DE LA JORNADA	como punto importante de la jornada de prevención en cuanto a ciberdelito en el municipio de Baranoa se desarrolló dentro del sector comercio, debido a la concentración de habitantes que visitan la zona a diario, esto con la intención de capacitar y prevenir a la comunidad sobre las modalidades más frecuentes de delitos informáticos, la actividad se enfoca en empoderar habitantes de esa zona a que aprendan una conceptualización más precisa de los temas, como punto importante se abordaron las precauciones, recomendaciones y rutas de denuncia en cuanto a esta modalidad delincuencial en crecimiento, además de apoyarnos en la información expuesta en folletos y cartillas y dejando como estrategia de recordación posters y manillas. La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética con la intención de promover un Atlántico ciberseguro.		

EVIDENCIA FOTOGRÁFICA









FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
02/08/2022	Ciberdelito	Baranoa	Educativo. Escuela Normal Superior Santa Ana.

OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.
DESARROLLO DE LA JORNADA	La jornada de concientización y prevención sobre ciberdelito en el colegio Normal Superior Santa Ana del municipio de Baranoa en los grupos de 9,10 y 11 grado, consistió en primera medida en conocer los preconceptos de los estudiantes para luego retroalimentar y brindar una conceptualización más precisa de los temas, a su vez se abordaron los tipos de delitos informáticos, precauciones, recomendaciones y rutas de denuncia en cuanto a esta modalidad delincuencial en crecimiento. Resulta importante tener en cuenta que las herramientas tecnológicas hacen parte de las acciones cotidianas y naturalizadas de la comunidad, por ende se puede inferir que de algún modo todos hemos usado alguna herramienta tecnológica para facilitar tareas por lo cual resulta necesario difundir información de concientización para toda la comunidad de esta forma se apropia a la comunidad de esta problemática basándonos en vivencias cotidianas de las personas para ejemplificar acciones en las que pueden ser víctimas de los ciberdelincuentes además de apoyarnos en la información expuesta en folletos y cartillas y dejando como estrategia de recordación posters y manillas La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética con la intención de promover un Atlántico ciberseguro.
EVIDENCIA FOTOGRÁFICAS	








HORARIO DE CLASE


HORARIO DE CLASE

FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
03/08/2022	Ciberdelito	Baranoa	Centro
OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.		
DESARROLLO DE LA JORNADA	La jornada de concientización y prevención sobre ciberdelito en el sector comercial del municipio de Baranoa, se desarrolló en compañía de la policía nacional y secretaria de gobierno del municipio, la actividad consiste en primera medida brindar una conceptualización en la zonas de mayor afluencia y constante intercambio de información como es el sector comercial, por esto se hace especial ahínco en dar a conocer los tipos de delitos que conforman esta modalidad delincuencial en crecimiento, teniendo en cuenta que las herramientas tecnológicas hacen parte de las acciones cotidianas y naturalizadas de la comunidad, por ende se puede inferir que de algún modo todos hacemos uso de estas herramientas por lo cual resulta necesario difundir información de concientización para toda la comunidad de esta forma se apropia a la comunidad de esta problemática basándonos en vivencias cotidianas de las personas para ejemplificar acciones en las que pueden ser víctimas de los ciberdelincuentes además de apoyarnos en la información expuesta en folletos y cartillas y dejando como estrategia de recordación posters y manillas. La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética con la intención de promover un Atlántico ciberseguro.		

EVIDENCIA FOTOGRÁFICAS











FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
04/08/2022	Ciberdelito	Baranoa	Plaza Principal
OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.		
DESARROLLO DE LA JORNADA	La jornada de concientización y prevención sobre ciberdelito en el municipio de Baranoa se desenvolvió gran parte y principalmente en el sector plaza del municipio, contando con el acompañamiento y el apoyo de la policía nacional, partimos de esta zona teniendo en cuenta la concentración de habitantes que hay constantemente , la actividad como tal consistió en primera medida en conocer los preconceptos de los habitantes para luego retroalimentar y brindar una conceptualización más precisa de los temas, a su vez se abordaron los tipos de delitos informáticos, precauciones, recomendaciones y rutas de denuncia en cuanto a esta modalidad delincuencial en crecimiento, ciberdelincuentes además de apoyarnos en la información expuesta en folletos y cartillas y dejando como estrategia de recordación posters y manillas La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética con la intención de promover un Atlántico ciberseguro.		
EVIDENCIA FOTOGRÁFICA			




Atlántico
más Seguro
para la Gente


CHANCLETAS



FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
05/08/2022	Ciberdelito	Galapa	Plaza
OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.		
DESARROLLO DE LA JORNADA	Parte de la jornada de concientización y prevención sobre ciberdelito en el municipio de Galapa se desarrolló en la plaza con la intención de llevar la información a todos y que su réplica sea mayor, además de resaltar la importante afluencia de ventas, tiendas, almacenes y estudiantes en el sector en mención. La actividad consiste en primera medida brindar una conceptualización de información entorno a la temática y llevarla a viviendas del sector e impactar en tiendas de barrio y negocios internos, convirtiéndolos en foco de información dejando un póster en el establecimiento y así conocer los tipos de delitos que conforman esta modalidad y tips para no caer en las garras de ciberdelincuentes, además de fomentar la curiosidad en cuanto al tema. Se utilizó como material didáctico la información expuesta en folletos y cartillas y dejando como estrategia de recordación posters y manillas La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética con la intención de promover un Atlántico ciberseguro.		

EVIDENCIA FOTOGRÁFICA









FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
08/08/2022	Ciberdelito	Galapa	Institución educativa Francisco de Paula Santander

OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.
DESARROLLO DE LA JORNADA	La jornada de concientización y prevención sobre ciberdelito en la Institución educativa Francisco de Paula Santander del municipio de Galapa en los grupos de 9,10 y 11 grado, se desarrolló de la mano de la policía de infancia y adolescencia del municipio, debido a acciones realizadas y naturalizadas por los chicos en el colegio donde se hizo mal uso de las redes y herramientas tecnológicas para acosar y perjudicar a compañeros y profesores por medio de videos o fotos inadecuadas. La actividad consistió en primera medida en conocer preconceptos de los estudiantes para luego retroalimentar y brindar una conceptualización más precisa de los temas, a su vez se abordaron los tipos de delitos informáticos, precauciones, recomendaciones y rutas de denuncia en cuanto a esta modalidad delincuencial en crecimiento. Resulta importante tener en cuenta que las herramientas tecnológicas hacen parte de las acciones cotidianas y naturalizadas de la comunidad y más de los estudiantes que lo usan como apoyo del aprendizaje por ende se puede inferir que de algún modo todos hemos usado alguna herramienta tecnológica para facilitar tareas por lo cual resulta necesario difundir información de concientización para toda la comunidad de esta forma se apropia a la comunidad de esta problemática basándonos en vivencias cotidianas para ejemplificar acciones en las que pueden ser víctimas de los ciberdelincuentes o volvernos ciberdelincuentes, además de apoyarnos en la información expuesta en folletos y cartillas y dejando como estrategia de recordación posters y manillas. La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética con la intención de promover un Atlántico ciberseguro.

EVIDENCIA FOTOGRÁFICA









FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
09/08/2022	Ciberdelito	Galapa	Centro

OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.
DESARROLLO DE LA JORNADA	La jornada de concientización y prevención sobre ciberdelito en el sector comercial del municipio de Galapa, se desarrolló en compañía de la policía nacional y secretaria de gobierno del municipio, la actividad consiste en primera medida brindar una conceptualización en la zonas de mayor afluencia y constante intercambio de información como es el sector comercial, por esto se hace especial ahínco en dar a conocer los tipos de delitos que conforman esta modalidad delincuencial en crecimiento, teniendo en cuenta que las herramientas tecnológicas hacen parte de las acciones cotidianas y naturalizadas de la comunidad, por ende se puede inferir que de algún modo todos hacemos uso de estas herramientas por lo cual resulta necesario difundir información de concientización para toda la comunidad de esta forma se apropia a la comunidad de esta problemática basándonos en vivencias cotidianas de las personas para ejemplificar acciones en las que pueden ser víctimas de los ciberdelincuentes además de apoyarnos en la información expuesta en folletos y cartillas y dejando como estrategia de recordación posters y manillas. La tecnología e internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética con la intención de promover un Atlántico ciberseguro.

EVIDENCIA FOTOGRÁFICAS











FECHA	ACTIVIDAD	MUNICIPIO	SECTOR

10/08/2022	Ciberdelito	Galapa	Mundo feliz
OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.		
DESARROLLO DE LA JORNADA	La campaña de concientización y prevención sobre ciberdelito en el barrio Mundo feliz del municipio de soledad se desarrolló en compañía de la policía nacional y secretaria de gobierno del municipio, la actividad consistió en pedagogía preventiva mano a mano y puerta a puerta donde se procedió a informar a vecinos y dueños de negocios locales en cuanto a las modalidades de delitos informáticos más frecuentes con la intención de disminuir la creciente actividad e identificar posibles autores de la mano de las denuncias, teniendo en cuenta que las herramientas tecnológicas hacen parte de las acciones cotidianas y naturalizadas de la comunidad es posible inferir que de algún modo todos tenemos acceso a las herramientas tecnológicas por lo cual resulta necesario difundir información de concientización apropiando y empoderando a la comunidad de esta problemática. Basándonos en vivencias cotidianas de las personas para ejemplificar acciones en las que pueden ser víctimas de los ciberdelincuentes además de apoyarnos en la información expuesta en folletos y cartillas y dejando como estrategia de recordación posters y manillas La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética con la intención de promover un Atlántico ciberseguro.		
EVIDENCIA FOTOGRÁFICA			


Barbería







FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
15/08/2022	Ciberdelito	MALAMBO	Barrio abajo
OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.		
DESARROLLO DE LA JORNADA	En el barrio Abajo del municipio de Malambo se desarrolló una de las jornadas de prevención y concientización sobre ciberdelito, la jornada se desempeñó con total satisfacción y recepción pertinente de parte de los habitante en cuanto a la información brindada, la concientización en cuanto a los peligros informáticos fue de total interés para los residentes del sector de igual forma se impartió la información en tiendas y negocios locales. Con la intención de brindar una información pedagógica y dinámica nos apoyamos en la información expuesta en folletos, cartillas y dejando como estrategia de recordación posters y manillas para lograr llevar una información condensada que se grabe en la memoria de todos. La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética con la intención de promover un Atlántico ciberseguro.		

EVIDENCIA FOTOGRÁFICA









FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
16/08/2022	Ciberdelito	Malambo	Institución educativa Juan 23

OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.
DESARROLLO DE LA JORNADA	La jornada de concientización y prevención sobre el ciberdelito en la Institución educativa Juan 23 del municipio de Malambo en los grupos de 9,10 y 11 grado, se desarrolló la actividad de la mano de la policía de infancia y adolescencia del municipio, se focalizó esta institución en específico dentro del municipio debido a acciones realizadas y denuncias internas realizadas por los estudiantes donde afirman que los estudiantes han hecho mal uso de las redes y herramientas tecnológicas para acosar y perjudicar a compañeros y profesores por medio de videos o fotos inadecuadas. La actividad consistió en primera medida en conocer preconceptos de los estudiantes para luego retroalimentar y brindar una conceptualización más precisa de los temas, a su vez se abordaron los tipos de delitos informáticos, precauciones, recomendaciones y rutas de denuncia en cuanto a esta modalidad delincuencial en crecimiento. Se contó con el apoyo de la policía para realizar actividades dinámicas que llamaran la atención de los jóvenes durante la charla. Resulta importante tener en cuenta que las herramientas tecnológicas hacen parte de las acciones cotidianas y naturalizadas de la comunidad y más de los estudiantes que lo usan como apoyo del aprendizaje por ende se puede inferir que de algún modo todos hemos usado alguna herramienta tecnológica para facilitar tareas por lo cual resulta necesario difundir información de concientización para toda la comunidad de esta forma se apropia a la comunidad de esta problemática basándonos en vivencias cotidianas para ejemplificar acciones en las que pueden ser víctimas de los ciberdelincuentes o volvernos ciberdelincuentes,además de apoyarnos en la información expuesta en folletos y cartillas y dejando como estrategia de recordación posters y manillas. La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética Con la intención de promover un Atlántico ciberseguro.

EVIDENCIA FOTOGRAFICA









FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
17/08/2022	Ciberdelito	Malambo	Centro

OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.
DESARROLLO DE LA JORNADA	La jornada de concientización y prevención sobre ciberdelito en el sector comercial del municipio de Malambo, se desarrolló en compañía de la policía nacional y secretaria de gobierno del municipio, la actividad consiste en primera medida brindar una conceptualización en la zonas de mayor afluencia y constante intercambio de información como es el sector comercial, por esto se hace especial ahínco en dar a conocer los tipos de delitos que conforman esta modalidad delincuencial en crecimiento, teniendo en cuenta que las herramientas tecnológicas hacen parte de las acciones cotidianas y naturalizadas de la comunidad, por ende se puede inferir que de algún modo todos hacemos uso de estas herramientas por lo cual resulta necesario difundir información de concientización para toda la comunidad de esta forma se apropia a la comunidad de esta problemática basándonos en vivencias cotidianas de las personas para ejemplificar acciones en las que pueden ser víctimas de los ciberdelincuentes además de apoyarnos en la información expuesta en folletos y cartillas y dejando como estrategia de recordación posters y manillas La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética con la intención de promover un Atlántico ciberseguro.
EVIDENCIA FOTOGRÁFICAS	











FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
18/08/2022	Ciberdelito	Malambo	Perímetro estación de policías

OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.
DESARROLLO DE LA JORNADA	La jornada de concientización y prevención sobre ciberdelito en el perímetro de la estación de policía del municipio de Malambo se desarrolló en compañía de la policía nacional, la actividad consistió en primera medida brindar una conceptualización en la zonas de mayor afluencia y constante intercambio de información como es el sector mencionado que cuenta con negocios locales además de intentar alertar a la comunidad , por esto se hace se hace especial ahínco en dar a conocer los tipos de delitos que conforman esta modalidad delincuencial en crecimiento, por lo cual resulta necesario difundir información de concientización para toda la comunidad de esta forma se apropia a la comunidad de esta problemática basándonos en vivencias cotidianas de las personas para ejemplificar acciones en las que pueden ser víctimas de los ciberdelincuentes además de apoyarnos en la información expuesta en folletos y cartillas y dejando como estrategia de recordación posters y manillas La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética con la intención de promover un Atlántico ciberseguro.

EVIDENCIA FOTOGRÁFICA









FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
20/08/2022	Ciberdelito	Puerto Colombia	Corredor universitario
OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.		
DESARROLLO DE LA JORNADA	Parte de jornada de concientización y prevención sobre ciberdelito en el municipio de Pto Colombia se trasladó al corredor universitario con la intención de llevar la información a todos y que su réplica sea mayor, además de resaltar la importante afluencia de ventas, tiendas, almacenes y estudiantes en el sector en mención. . la actividad consistió en primera medida brindar una conceptualización de información entorno a la temática y llevarla a viviendas del sector e impactar en tiendas de barrio y negocios internos, convirtiéndolos en foco de información dejando un póster en los establecimiento, el cual es un constante recordatorio tipos de delitos que conforman esta modalidad y tips para no caer en las garras de ciberdelincuentes. Promover la ciberseguridad es un compromiso de todos por esto recalcamos la importancia de la información brindada a la comunidad Se utilizó como material didáctico la información expuesta en folletos y cartillas y dejando como estrategia de recordación posters y manillas La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética Con la intención de promover un Atlántico ciberseguro.		

EVIDENCIA FOTOGRÁFICA









FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
21/08/2022	Ciberdelito	Puerto Colombia	Loma fresca

OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.
DESARROLLO DE LA JORNADA	La jornada de concientización y prevención sobre el ciberdelito en el barrio Loma fresca del municipio de Pto Colombia se llevó a cabo con resultados satisfactorios en cuanto a la comunidad que acogió el tema y se atrevió a preguntar para aclarar dudas, la actividad consiste en primera medida brindar una conceptualización en la zonas de mayor afluencia y constante intercambio de información como en tiendas de barrio y negocios internos, por esto se hace especial ahínco en dar a conocer los tipos de delitos que conforman esta modalidad delincuencial en crecimiento, teniendo en cuenta que las herramientas tecnológicas hacen parte de las acciones cotidianas y naturalizadas de la comunidad, apropiando a la comunidad de esta problemática basándonos en vivencias cotidianas de las personas para ejemplificar acciones en las que pueden ser víctimas de los ciberdelincuentes además de apoyarnos en la información expuesta en folletos y cartillas y dejando como estrategia de recordación posters y manillas. La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética Con la intención de promover un Atlántico ciberseguro.
EVIDENCIA FOTOGRAFICA	







FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
22/08/2022	Ciberdelito	Puerto Colombia	Institución educativa técnica comercial Francisco Javier Cisneros

OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.
DESARROLLO DE LA JORNADA	La jornada de concientización y prevención sobre el ciberdelito en la Institución educativa técnica comercial Francisco Javier Cisneros del municipio de Puerto Colombia en los grupos de 9,10 y 11 grado, se desarrolló de la mano de la policía nacional y la alcaldía del municipio dentro de una espacio con todos los estudiantes debido a denuncias internas por ciberacoso y miedo colectivo por medio de las redes a la población estudiantil. Consistió en primera medida en conocer preconceptos de los estudiantes para luego retroalimentar y brindar una conceptualización más precisa de los temas, a su vez se abordaron los tipos de delitos informáticos, precauciones, recomendaciones y rutas de denuncia en cuanto a esta modalidad delincuencial en crecimiento. Resulta importante tener en cuenta que las herramientas tecnológicas hacen parte de las acciones cotidianas y naturalizadas de la comunidad, por ende se puede inferir que de algún modo todos hemos usado alguna herramienta tecnológica para facilitar tareas por lo cual resulta necesario difundir información de concientización para toda la comunidad de esta forma se apropia a la comunidad de esta problemática basándonos en vivencias cotidianas de las personas para ejemplificar acciones en las que pueden ser víctimas de los ciberdelincuentes además de apoyarnos en la información expuesta en folletos y cartillas y dejando como estrategia de recordación posters y manillas de igual forma se usó como apoyo y motivación implementos que iba a donar la alcaldía a los estudiantes como bolsos y Tablet La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética con la intención de promover un Atlántico ciberseguro.

EVIDENCIA FOTOGRÁFICA









FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
23/08/2022	Ciberdelito	Puerto Colombia	Plaza Central

OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.
DESARROLLO DE LA JORNADA	Se realizó una jornada de prevención sobre el ciberdelito en la plaza central de puerto Colombia, debido a que es una zona en la cual podemos advertir e informar a la comunidad en general de esta problemática que cada día avanza un poco más. Esta jornada concluyó exitosamente debido a que el personal que recibió la información se mostró interesado y con ganas de informarse tanto así que realizaban preguntas acerca de la temática. La actividad consiste en primera medida brindar una conceptualización de información entorno a la temática y llevarla a viviendas del sector, a las personas que se encuentran en la plaza, tiendas y almacenes con el fin de que las personas comprendan la información y la puedan replicarla, También se deja un póster en los establecimientos visitados y así conocer los tipos de delitos que conforman esta modalidad y tips para no ser víctima del ciberdelito. Se utilizó como material didáctico la información expuesta en folletos y cartillas y dejando como estrategia de recordación posters y manillas La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar el cuidado y el buen manejo de la tecnología para conservar las consecuencias positivas y no caer en lo negativo que estas traen para todos como lo es el ciberdelito.
EVIDENCIA FOTOGRÁFICAS	








Broaster El Joe
304 2445465
Pollo Breaster
Pollo Asado, Ahumado
PLASTY BARRETO
302 336 2271
JOE

FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
24/08/2022	Ciberdelito	Sabanalarga	El Pradito
OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.		
DESARROLLO DE LA JORNADA	En el barrio el Pradito del municipio de Sabanalarga se desarrolló una de las jornadas de prevención y concientización sobre ciberdelito, la jornada se desempeñó con total satisfacción y recepción pertinente de parte de los habitante en cuanto a la información brindada y el interés de la comunidad de concientización en cuanto a los peligros informáticos, de igual forma se impartió la información en tiendas y negocios locales , esto con la intención de brindar una información pedagógica y dinámica, nos apoyamos en las vivencias diarias y ejemplos cotidianos en los que podemos ser más propensos a convertirnos en víctimas de los ciberdelincuentes y tomamos como base en la información expuesta en folletos, cartillas y dejando como estrategia de recordación posters y manillas para lograr llevar una información condensada que se grabe en la memoria de todos. Dentro de la sociedad actual resulta de gran importancia la educación constante de temas que impactan de manera directa en el desarrollo y crecimiento de la comunidad, la tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética con la intención de promover un Atlántico ciberseguro.		

EVIDENCIA FOTOGRÁFICA









FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
28/08/2022	Ciberdelito	Sabanalarga	Centro
OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.		

DESARROLLO DE LA JORNADA	La jornada de concientización y prevención sobre el ciberdelito en el sector comercial del municipio de Sabanalarga, se desarrolló en compañía de la policía nacional y secretaria de gobierno del municipio, la actividad consiste en primera medida brindar una conceptualización en la zonas de mayor afluencia y constante intercambio de información como es el sector comercial, por esto se hace especial ahínco en dar a conocer los tipos de delitos que conforman esta modalidad delincuencial en crecimiento, teniendo en cuenta que las herramientas tecnológicas hacen parte de las acciones cotidianas y naturalizadas de la comunidad, por ende se puede inferir que de algún modo todos hacemos uso de estas herramientas por lo cual resulta necesario difundir información de concientización para toda la comunidad de esta forma se apropia a la comunidad de esta problemática basándonos en vivencias cotidianas de las personas para ejemplificar acciones en las que pueden ser víctimas de los ciberdelincuentes además de apoyarnos en la información expuesta en folletos y cartillas y dejando como estrategia de recordación posters y manillas La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética con la intención de promover un Atlántico ciberseguro.
EVIDENCIA FOTOGRÁFICAS	











FECHA	ACTIVIDAD	MUNICIPIO	SECTOR

30/08/2022	Ciberdelito	Sabanalarga	Diez de Febrero
OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.		
DESARROLLO DE LA JORNADA	Una de las jornada de concientización y prevención sobre ciberdelito en el municipio de Sabanalarga, se desarrolló en el barrio Diez de Febrero con la intención de abordar y llevar el mensaje a la mayor cantidad de habitante que fuera posible, teniendo en cuenta la influencia del desarrollo tecnológico dentro de las comunidades y de nuestra vida cotidiana, por esto, la pertinencia de la jornada de prevención con la intención de poder educar al departamento en cuanto a cómo prevenir ser víctima de ciberdelitos y cómo denunciar para no caer en las redes de los ciberdelincuentes y contribuir a que los demás tampoco sean víctimas. Con la intención de brindar una información pedagógica y dinámica nos apoyamos en la información expuesta en folletos, cartillas y dejando como estrategia de recordación posters y manillas para lograr llevar una información condensada que se grabe en la memoria de todos. La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética con la intención de promover un Atlántico ciberseguro.		

EVIDENCIA FOTOGRÁFICA









FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
31/08/2022	Ciberdelito	Sabanalarga	Mercado

OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.
DESARROLLO DE LA JORNADA	La jornada de concientización y prevención sobre ciberdelito en el municipio de Sabanalarga, se desarrolló de igual forma y con especial importancia en el mercado nuevo y viejo, teniendo como principal motivo la intención de llevar la información a la mayor cantidad posible de habitantes teniendo en cuenta además que la zona del mercado y sus alrededores son de constante intercambio de información y movimiento económico por esto resulta pertinente la pedagogía preventiva en la zona apoyándonos en la información expuesta en folletos , cartillas y dejando como estrategia de recordación posters y manillas. los comerciantes son una parte importante de este proceso de información con carácter preventivo debido a que la sociedad está en un constante desarrollo y crecimiento donde la tecnología es un actor principal, por esto las formas de pago se transforman, cada vez es más usual los pagos por transferencias, link de pagos entre otros medio donde los ciberdelincuentes pueden aprovechar para apropiarse de información, clonar tarjetas,robos de cuentas y ompa.. La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética con la intención de promover un Atlántico ciberseguro.

CORPODESC
CORPORACIÓN TÉCNICA PARA EL DESARROLLO HUMANO SOCIAL Y CULTURAL DE COLOMBIA

EVIDENCIA FOTOGRÁFICA









FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
01/09/2022	Ciberdelito	Soledad	La María
OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.		
DESARROLLO DE LA JORNADA	La jornada de concientización y prevención sobre ciberdelito en el barrio La María del municipio de soledad se desarrolló en compañía de la policía nacional y secretaria de gobierno del municipio donde se buscó llevar la información a la mayor cantidad de habitantes entendiendo la realidad y el crecimiento de los tentáculos de la tecnología en nuestra cotidianidad, por lo tanto, esto crea la necesidad de conciencia en cuanto las formas de ciberdelitos ya que los riesgos de ser robado estafado, suplantando o usado para cometer algún delito en redes o por medio de la tecnología son cada vez más probables por esto en el barrio la María se intentó llegar a la mayor cantidad de habitantes de todas las edades con la campaña de prevención para de esta forma brindar herramientas efectivas para actuar de la mano en cuanto estos temas. La necesidad de esta campaña y proceso de prevención pedagógica radica en la necesidad de enseñar a una sociedad en crecimiento a ser responsables de su realidad tecnológica, donde el crecimiento masivo del uso de la tecnología para realizar compras de todo tipo y vender productos o servicios brindan el medio perfecto para los delincuentes por esto y teniendo en cuenta que la tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento es necesario fomentar una conciencia cibernética Con la intención de promover un Atlántico ciberseguro.		

EVIDENCIA FOTOGRAFICA









FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
02/09/2022	Ciberdelito	Soledad	El cortijo
OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.		
DESARROLLO DE LA JORNADA	La jornada de concientización y prevención sobre el ciberdelito en el barrio El cortijo del municipio de soledad se desarrolló en compañía de la policía nacional y secretaria de gobierno del municipio, la actividad consistió en la realización de pedagogía preventiva mano a mano y puerta a puerta donde se procedió a informar a vecinos y dueños de negocios en cuanto a las modalidades de delitos informáticos mas frecuentes con la intención de disminuir la creciente actividad e identificar posibles autores de la mano de las denuncias, teniendo en cuenta que las herramientas tecnológicas hacen parte de las acciones cotidianas y naturalizadas de la comunidad es posible inferir que de algún modo todos tenemos acceso a las herramientas tecnológicas por lo cual resulta necesario difundir información de concientización apropiando y empoderando a la comunidad de esta problemática. Basándonos en vivencias cotidianas de las personas para ejemplificar acciones en las que pueden ser víctimas de los ciberdelincuentes además de apoyarnos en la información expuesta en folletos y cartillas y dejando como estrategia de recordación posters y manillas La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética Con la intención de promover un Atlántico ciberseguro.		
EVIDENCIA FOTOGRAFICA			


WIN




Atlántico
más Seguro
para la Gente



FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
05/09/2022	Ciberdelito	Soledad	Centro
OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.		
DESARROLLO DE LA JORNADA	La jornada de concientización y prevención sobre el ciberdelito en el sector comercial del municipio de soledad se desarrolló en compañía de la policía nacional y secretaria de gobierno del municipio, la actividad consiste en primera medida brindar una conceptualización en la zonas de mayor afluencia y constante intercambio de información como es el sector comercial, por esto se hace especial ahínco en dar a conocer los tipos de delitos que conforman esta modalidad delincuencial en crecimiento, teniendo en cuenta que las herramientas tecnológicas hacen parte de las acciones cotidianas y naturalizadas de la comunidad, por ende se puede inferir que de algún modo todos hacemos uso de estas herramientas por lo cual resulta necesario difundir información de concientización para toda la comunidad de esta forma se apropia a la comunidad de esta problemática basándonos en vivencias cotidianas de las personas para ejemplificar acciones en las que pueden ser víctimas de los ciberdelincuentes además de apoyarnos en la información expuesta en folletos y cartillas y dejando como estrategia de recordación posters y manillas La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética con la intención de promover un Atlántico ciberseguro.		
EVIDENCIA FOTOGRÁFICAS			








Atlántico
más Seguro
para la Gente



FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
06/09/2022	Ciberdelito	Soledad	San Antonio (Institución Educativa Jhon F Kennedy)
OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.		
DESARROLLO DE LA JORNADA	Esta jornada de concientización y prevención sobre el ciberdelito fue en el barrio San Antonio principalmente se tomó la institución Educativa John F Kennedy debido a que es importante que los jóvenes que son unos de los más expuestos a la tecnología reciban la información. Se abordó a los estudiantes de 10 y 11 grado con la intención de que actúen como voceros de la información para sus compañeros se contó con la participación activa de la policía infancia y adolescencia y el acompañamiento constante de directivos de la institución. La actividad consiste en primera medida brindar una conceptualización en cuanto a términos y tipos de delitos que conforman esta modalidad delincuencial en crecimiento, teniendo en cuenta que las herramientas tecnológicas hacen parte de las acciones cotidianas y naturalizadas de la comunidad, por ende se puede inferir que de algún modo todos hacemos uso de estas herramientas por lo cual resulta necesario difundir información de concientización que llegue a todos. Se apropia a la comunidad de esta problemática basándonos en vivencias cotidianas de las personas para ejemplificar acciones en las que pueden ser víctimas de los ciberdelincuentes además de apoyarnos en la información expuesta en folletos y cartillas y dejando como estrategia de recordación posters y manillas.		

	Resulta pertinente recalcar que como motivación importante para esta visita se tenía conocimiento de denuncias por parte de profesores y estudiantes en cuanto a casos de ciberacoso por parte de los estudiantes a profesores y compañeros. La tecnología y el internet son una herramienta importante del crecimiento y desarrollo del departamento por esto resulta necesario fomentar una conciencia cibernética con la intención de promover un Atlántico ciberseguro.
EVIDENCIA FOTOGRÁFICAS	






DIOS
REDMI NOTE 10 PRO


REDMI NOTE 10 PRO


POLICIA

REUNIÓN CON EL COMITÉ DE SEGURIDAD BANCARIA DEL DEPARTAMENTO DEL ATLÁNTICO

Con el fin de articular las acciones de implementación, especialmente la de toma de bancos, se espera tener reuniones previas con delegados de las entidades bancarias que hagan presencia en los 6 municipios priorizados, con el fin de articular dichas acciones.

<table>
<tr><th>FECHA</th><th>ACTIVIDAD</th><th>SECTOR</th><th>DURACIÓN</th></tr>
<tr><td>05/10/2022</td><td>Reunión con el comité se seguridad Bancaria</td><td>Gobernación del Atlántico, piso 8</td><td>1 hora</td></tr>
<tr><td>OBJETIVO DE LA ACTIVIDAD</td><td colspan="3">Articular acciones con el comité de seguridad bancaria departamental</td></tr>
<tr><td>DESARROLLO DE LA JORNADA</td><td colspan="3">La reunión se desarrolló con el animo de realizar un balance de las actividades denominadas tomas bancarías que se realizaron los municipios priorizados para el presente proyecto, los bancos intervenidos fueron los siguientes:
<table>
<tr><td>Baranoa</td><td>Banco de Bogotá – Bancolombia</td></tr>
<tr><td>Galapa</td><td>Bancolombia</td></tr>
<tr><td>Malambo</td><td>Bancolombia</td></tr>
<tr><td>Puerto Colombia</td><td>Banco Agrario</td></tr>
<tr><td>Sabanalarga</td><td>BBVA – Bancolombia</td></tr>
<tr><td>Soledad</td><td>BBVA (American Bar)</td></tr>
</table>
Estas intervenciones se realizaron en el mes de septiembre, por lo que la presente reunión inició con un balance de las intervenciones, llegando a la conclusión de que fueron un gran éxito, ya que muchos de los delegados de los bancos y que hacen parte del comité bancario mostraron satisfacción por los comentarios recibidos por los gerentes municipales.

Se plateó la importancia de seguir implementado este tipo de estrategias en los municipios, ya que hoy en día es mucho más recurrente las diferentes modalidades de los delitos cibernéticos.</td></tr>
</table>

EVIDENCIA FOTOGRÁFICA







GOBERNACION DEL ATLANTICO	CONTROL DE ASISTENCIA A REUNION	VERSION	003
		ECHA DE APROBACION	2020-01-27

TEMA: Prevencion del ciberdelito

FECHA: 5/octubre/2022

NOMBRE	CARGO	DEPENDENCIA	CORREO ELECTRONICO	Número celular	FIRMA
Miguel De León	Tec. Inv. II		miguel.leon@fiscalia.gov.co	321 [illegible] 3330	
Sergio Lopez	Coordinador Observat.	Alcaldia de Barranquilla OSC.	slopezm@barranquilla.gov.co	3127803 [illegible]	
Carlos Dangond	Fiscal	UNIDAD EDA	carlos.dangond@fiscalia.gov.co	3008148647	
Claudio Lopez	fiscal jefe EDA	EDA-	claudio.lopez@fiscalia	3003197 [illegible]	
Erwin Arroyo	TEC. INV I	SAC	erwin.arroyo@fiscalia.gov.co	3015779475	
Amardo Lozano	AUXILIAR	[illegible]	arlozano@[illegible]	3168503798	
Magaly Zapata	Analista	Banco AV Villas	[illegible]	3[illegible]144112	
Ronald Quintero	Subgerente	Banco W	rquintero@bancow.com.co	3006420374	
FREDY TORRES	GTE RCS	INCOCREDITO	ctorres@incocredito.com.co	3123855879	
Leonell Santiago	Director	Banco Serfinanza	leonell.santiago@bancoserfinanza.com.	3[illegible]	
Felipe Figueroa	Coordinador	Bco Caja Social	ffigueroa@cfs.co	3157185328	
FABIO QUINTERO C.	JEFE REG.	GERENCIA SEGURIDAD	FQUINTERO@BANCOPOPULAR.COM	3153763[illegible]24	

Declaro de manera expresa y libre que autorizo a la Gobernación del Atlántico como responsable de recolectar mis datos personales y registros multimedia (fotos, videos, audios), del uso que se les dé a los mismos y de su protección conforme a la Política de Tratamiento de Datos Personales Ley 1581 de 2012 Régimen General de Protección de Datos Personales. Otorgo mi consentimiento mediante mi firma.

TOMA DE BANCOS

Una de las actividades con la que más se impactó en el desarrollo del presente proyecto fue la de prevenir el delito cibernético y sus diferentes modalidades en las entidades bancarias, para tal fin, se contemplaron unas acciones de prevención en los bancos, que dan cuenta de una socialización breve, y por medio de ayudas didácticas, de las recomendaciones que se deben tener los ciudadanos al momento de realizar transacción bancarias (en línea o de manera presencial), para no caer como víctimas del ciber delito. Para ello, se contactó previamente con la aceptación de las entidades bancarías que estuvieron dispuestas a recibir estos de espacios de socialización dentro de sus instalaciones.

A continuación, la evidencia correspondiente.

FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
12/09/2022	Ciberdelito	Baranoa	BANCOS
OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.		
DESARROLLO DE LA JORNADA	La jornada de concientización y prevención sobre ciberdelito se trasladó como punto central y de gran importancia a los bancos centrales de los municipios, en Baranoa se trabajó con el BANCO DE BOGOTÁ y BANCOLOMBIA. La actividad consistió, primero en una contextualización de conceptos a los clientes presentes y personal de atención con la intención de generar familiaridad y apropiación del tema también se expusieron cifras en aumento de ciberdelitos y suplantación de identidad sobre datos bancario para así alertar a la comunidad de la pertinencia del tema en cuestión. Durante la actividad se usó como material de apoyo y medio de interacción y material didáctico folletos, manillas, cartillas y con la intención de involucrar a la comunidad presente se fomento la lectura de un ítem o concepto y preguntas al público dirigidas por el capacitador a cargo. Finalmente un mensaje por parte de la policía nacional a tener más en cuenta el servicio gratuito de acompañamiento policial en actividades bancarias como retiro y consignación de altas sumas de dinero.		
EVIDENCIA FOTOGRAFICA			


¿Cómo puedo ayudarte?


Banco de Bogotá


Caja 03


Bancolombia
Cajero


Sucursal
Baranoa
POLICIA
Cajero

FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
13/09/2022	Ciberdelito	Galapa	BANCOS
OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.		
DESARROLLO DE LA JORNADA	La jornada de concientización y prevención sobre ciberdelito en el municipio de Galapa se realizó en BANCOLOMBIA, la actividad se desarrolló animando a los presentes a educarse en el manejo responsable y prudente de los medios cibernéticos en especial al momento de suministrar datos bancarios y financieros, especificando conceptos y exponiendo cuales son la modalidades de delitos informáticos y cibernéticos más frecuentes en el Atlántico y a los cuales estamos más expuestos si no tomamos las medidas necesarias en nuestra comunidad, de igual forma se dio conocer cifras expuestas por entidades encargadas y expertas en tema que confirman la necesidad latente de aprendizaje en el tema . Durante la actividad se usó como material de apoyo y medio de interacción y material didáctico folletos, manillas, cartillas y con la intención de involucrar a la comunidad presente se fomento la lectura de un ítem o concepto y preguntas al público dirigidas por el capacitador a cargo.		

EVIDENCIA FOTOGRÁFICA







FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
14/09/2022	Ciberdelito	MALAMBO	BANCOS
OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.		
DESARROLLO DE LA JORNADA	La jornada de concientización y prevención sobre ciberdelito en el banco, BANCOLOMBIA del municipio de Malambo se ejecutó en un primer momento haciendo un mensaje de alerta sobre los aumentos en fraudes y suplantación de identidad en datos bancarios, en especial con personas mayores de igual forma se realizó una contextualización de conceptos a los clientes presentes y personal de atención con la intención de generar familiaridad y apropiación del tema Luego un llamado a educarse y aprender de personas con mejor manejo y uso adecuado, prudente de medios informáticos en especial para trámites financieros y bancarios: compras, transferencias y transacciones en general. Finalmente se les exhortó a profundizar más en el tema de los ciberdelitos utilizando el material impreso que se les proveyó. Y se realizaron recomendaciones preventivas pertinentes en cuanto a uso de cajeros, compras en ompañ, suministro de datos personales y demás.		

EVIDENCIA FOTOGRÁFICA







FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
15/09/2022	Ciberdelito	PUERTO COLOMBIA	BANCOS
OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.		
DESARROLLO DE LA JORNADA	La jornada de concientización y prevención sobre el ciberdelito en el banco AGRARIO del municipio de Puerto Colombia se desarrolló en un primer espacio donde se recordó y recalco a los presentes su obligación de manejar con responsabilidad y cautela sus datos bancarios y financieros (contraseñas, claves); esto, debido al aumento de robos y estafas de las que están siendo víctimas la comunidad en general y en especial personas mayores. Teniendo en cuenta y resaltando el constante crecimiento y desarrollo del municipio en este momento ya que se encuentra en auge y crecimiento turístico , lo cual vuelve masiva las visitas constantes y una afluencia de gente diaria en establecimientos, negocios,cajeros y bancos por lo tanto resulta pertinente dar a conocer conceptos y modalidades de ciberdelitos más frecuentes además de precauciones y medios de denuncia para así disminuir la posibilidad de ser víctima de un ciberdelito Finalmente dimos a conocer el material didáctico impreso que se les entregó exhortándoles a seguir profundizando sobre las modalidades de ciberdelitos que siguen en aumento en nuestra región.		
EVIDENCIA FOTOGRÁFICA			






FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
18/09/2022	Ciberdelito	SABANALARGA	BANCOS
OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.		

DESARROLLO DE LA JORNADA	. La jornada de concientización y prevención sobre ciberdelito se trasladó como punto central y de gran importancia a los bancos centrales de los municipios,en Sabanalarga se trabajó con el BBVA y BANCOLOMBIA. La actividad consistió, primero en una contextualización de conceptos a los clientes presentes y personal de atención con la intención de generar familiaridad y apropiación del tema también se expusieron cifras en aumento de ciberdelitos y suplantación de identidad sobre datos bancario para así alertar a la comunidad de la pertinencia del tema en cuestión.Realizando llamado directo y claro al cuidado de datos bancarios en medios informáticos, cajeros automáticos. Durante la actividad se usó como material de apoyo y medio de interacción y material didáctico folletos, manillas, cartillas y con la intención de involucrar a la comunidad presente se fomento la lectura de un ítem o concepto y preguntas al público dirigidas por el capacitador a cargo. Finalmente un mensaje por parte de la policía nacional a tener más en cuenta el servicio gratuito de acompañamiento policial en actividades bancarias como retiro y consignación de altas sumas de dinero.

EVIDENCIA FOTOGRÁFICA









FECHA	ACTIVIDAD	MUNICIPIO	SECTOR
18/09/2022	Ciberdelito	Soledad	BANCOS

OBJETIVO DE LA ACTIVIDAD	Jornada de concientización y prevención sobre ciberdelito con la intención de impartir conciencia social de la mano de la pedagogía en cuánto a delitos informáticos conceptos modalidades y precauciones.
DESARROLLO DE LA JORNADA	La jornada de concientización y prevención sobre el ciberdelito en el banco BBVA, del municipio de soledad se desarrolló en dos momentos, al inicio mensaje directo a clientes y personal de atención dentro de las instalaciones, haciendo uso de material pedagógico impreso en papel y manillas, permitiendo un espacio de conceptualización básica sobre qué es y cómo operan los ciberdelincuentes, de igual forma se impartió información sobre los tipos de ciberdelitos más comunes y de mayor crecimiento en el departamento. La actividad se desarrolló con la ompañía de la policía nacional los cuales brindaron información pertinentes y ejemplos desde su campo de experiencia en cuanto a delincuentes y modo en el que operan usualmente bajo la modalidad de ciberdelitos. Finalmente, abordaje persona a persona de clientes en cajeros automáticos y en espera a las afueras de las instalaciones realizando llamado directo y claro al cuidado de datos bancarios en medios informáticos, cajeros automáticos.
EVIDENCIA FOTOGRAFICA	


BBVA
POLICIA


Atlántico
más Seguro
para la Gente
POLICIA


BBVA
Atlántico
más Seguro
para la Gente


Atlántico
más Seguro
para la Gente

SEMINARIO TALLER

Esta fase contempló el desarrollo de un seminario taller dirigido a las personas que componen el Comité de Seguridad Bancaria del Departamento del Atlántico, el día 05 de octubre del 2022. El presente taller tuvo como panelista al Doctor Miguel Antonio de León Porras, y dirigió el panel en las siguientes temáticas: • Modalidades del delito cibernético en entidades bancarias • Retos en ciberseguridad bancaria • Protección y seguridad a los usuarios por entidades bancarias.

FECHA	ACTIVIDAD	SECTOR	DURACIÓN
10/05/2022	Prevención del ciberdelito	Gobernación del Atlántico, piso 8	3 horas
OBJETIVO DE LA ACTIVIDAD	Fortalecimiento de las estrategias encaminadas en la erradicación del Ciberdelito.		
DESARROLLO DE LA JORNADA	El evento inicio a la hora prevista en la **Gobernación Del Atlántico**, siendo presentado por el Doctor **Noe José Jiménez**, quien le dio la bienvenida a los ponentes y al público presente el cual estaba conformado por personas con diferentes especialidades y funciones como, analistas, técnicos investigativos, fiscales, funcionarios bancarios Etc. Luego de hacer la introducción del evento y explicar la finalidad del mismo, el Doctor Noé recalco la importancia de que todas las entidades trabajen de forma mancomunada para enfrentar de manera eficaz la problemática de los delitos informáticos, lo cual en la actualidad se configura como un grave problema que deja victimas de manera constante. Posteriormente tomo la palabra el primer ponente llamado **Fredy Torres** el cual inicio su intervención haciendo una aclaración sobre lo que se conoce como ciberdelito, recalcando que este se refuerza bajo dos modalidades, la primera tiene que ver con lo operativo, es decir la forma bajo la cual se planean estos delitos y la segunda modalidad, es el proceso posterior al fraude, la forma en		

	que los delincuentes cibernéticos proceden a entrar de forma abusiva a cuentas bancarias sin que las víctimas o los mismos bancos puedan darse cuenta hasta que ya es demasiado tarde y el robo ya se haya concretado. Sobre este aspecto, el ponente aclaro que estos robos cibernéticos se pueden dar con mayor facilidad debido a que no existe una información unificada entre las entidades bancarias y las líneas de telefonía celular, situación que termina favoreciendo a los ciber delincuentes y en ultimas termina perjudicando también el actuar de la justicia pues no existen las herramientas ni la información adecuada para identificar y condenar de manera oportuna a estos delincuentes y por consecuencia el número de víctimas sigue creciendo. Después tomo la palabra el segundo ponente llamado Miguel De León, quien se desempeña como técnico investigativo, a partir de su experiencia narro las distintas modalidades que están implementando los delincuentes informáticos en la actualidad, destaco el uso de falsos paquetes turísticos para estafar a las personas, lo cual funciona bajo la modalidad de suplantación de hoteles particularmente los que se encuentran bajo medida de ocupación por la SAE (sociedad de activos especiales). Es decir hoteles en proceso de liquidación, situación de la cual se aprovechan los delincuentes para publicitar en internet estos hoteles bajo la modalidad de suplantación en la busca de potenciales clientes, y posteriormente venderles planes turísticos totalmente falsos. Otra grave problemática que destaco este ponente es que muchas veces los números telefónicos registrados en las empresas de telefonía celular no son compatibles con la identidad de la persona que aparece como dueña de este mismo número, situación que en la actualidad es un factor facilitador de los delitos informáticos teniendo en cuenta el creciente uso por parte de las personas, de plataformas virtuales móviles para el retiro y transferencia de

	dinero como Nequi y cuentas a la mano. También en esta intervención se destacó que la falta de validación a la hora de abrir los productos financieros virtuales supone un problema del que están sacando provecho los delincuentes informáticos, ya que facilita la suplantación de identidad y pedir o retirar dinero usando el nombre de una persona totalmente diferente. Situación que también se presenta cada vez con mayor frecuencia en herramientas como Marketplace a través de redes sociales de común uso como Instagram y Facebook. Por último se hizo un llamado a mejorar los controles por parte de las entidades bancarias de los productos que se ofrecen de manera virtual, esto articulado también a un mejor manejo de la información por parte de las empresas de telefonía celular para que en este sentido exista una valida información unificada, lo cual en ultimas significaría dificultar el actuar de los delincuentes informáticos los cuales al día de hoy se aprovechan de esta falta de control y siguen dejando víctimas en todo el territorio nacional y en la costa, particularmente en ciudades como Santa marta, Barranquilla, Cartagena y San Andrés. Al final del evento se rescató la importancia de que todas las entidades involucradas en la prevención y sanción de este delito trabajen de forma unificada e involucrar a las diferentes dependencias del gobierno como el Ministerio de las TIC. Y de esta forma seguir tejiendo una estrategia no solo a nivel Regional si no a nivel Nacional que permita ponerle un freno al Ciberdelito y evitar que este siga estando un paso adelante de la justicia.

EVIDENCIA FOTOGRÁFICA











GOBERNACION DEL ATLANTICO	CONTROL DE ASISTENCIA A REUNION	VERSION	003
		ECHA DE APROBACION	2020-01-27

TEMA: Prevencion del ciberdelito

FECHA: 5/octubre/2022

NOMBRE	CARGO	DEPENDENCIA	CORREO ELECTRONICO	Número celular	FIRMA
Miguel De León	Tec. Inv. II		miguel.leon@fiscalia.gov.co	321 [illegible] 3330	
Sergio Lopez	Coordinador Observat.	Alcaldia de Barranquilla OSCI.	slopezm@barranquilla.gov.co	3127803 [illegible]	
Carlos Dangond	Fiscal	UNIDAD EDA	carlos.dangond@fiscalia.gov.co	3008148049	
Claudio Lopez	fiscal jefe EDA	EDA-	claudio.lopez@fiscalia.gov.co	3003197005	
Erwin Arturo P.	Tec. INV I	SAC	erwin.arturo@fiscalia.gov.co	3015799495	
Armando Lozano	AUXILIAR	POLICIA NACIONAL	arturo.lozano@[illegible]	3168503798	
Magaly Zapata	Analista	Banco AV Villas	[illegible]	3117144112	
Ronald Quintero	Subgerente	Banco W	rquintero@bancow.com.co	3006720374	
FREDY TORRES	GTE RCS	INCOCREDITO	ctorres@incocredito.com.co	3123855879	
Leonell Santiago	Director	Banco Serfinanza	leonell.santiago@bancoserfinanza.com	3[illegible]	
Felipe Figueroa	Coordinador	Bancamia Social	ffigueroa@efs.co	3157185328	
FABIO QUINTERO C.	JEFE REG.	GERENCIA SEGURIDAD	FQUINTERO@BANCOPUBLICO.COM.CO	3153763824	

Declaro de manera expresa y libre que autorizo a la Gobernación del Atlántico como responsable de recolectar mis datos personales y registros multimedia (fotos, videos, audios), del uso que se les dé a los mismos y de su protección conforme a la Política de Tratamiento de Datos Personales Ley 1581 de 2012 Régimen General de Protección de Datos Personales. Otorgo mi consentimiento mediante mi firma.

ANEXO

1. PRESENTACIÓN DE LOS EXPOSITORES PARA LA JORNADA DE CAPACITACIÓN



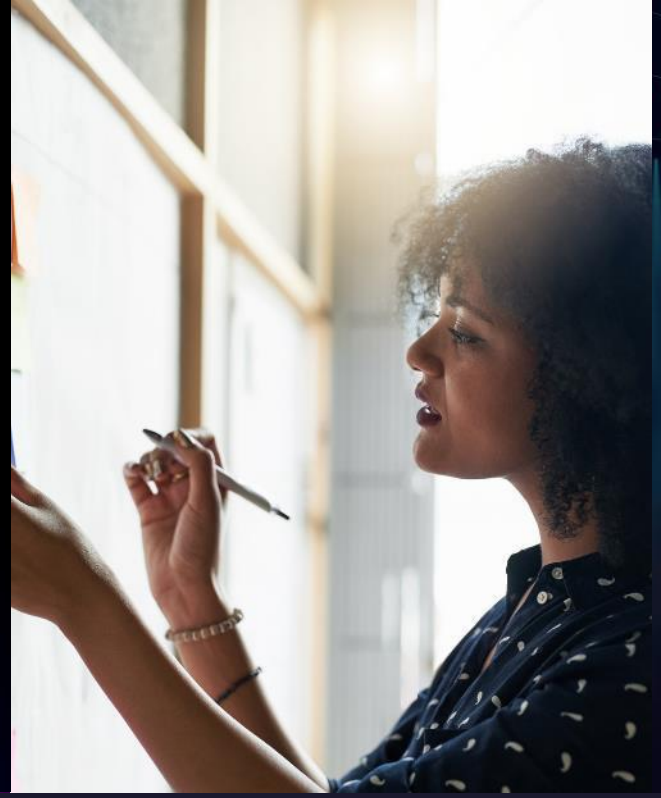
Taller Cibercrimen

Miguel Antonio De león Porras

Abogado Esp. Derecho Penal

Investigador y Analista







Introducción:

Los delitos contra el patrimonio económico que en su medio de ejecución involucran dispositivos electrónicos o sistemas de información, requieren no solo de la planeación, sino que por el simple hecho de que los actos preparativos requieren un elaborado plan, el conocimiento de personas en áreas de ingeniería electrónica y de sistemas; hacen que la premeditación en este tipo de conductas los haga potencialmente más peligrosos para sus víctimas, porque si bien es cierto que ésta última, no resulta lesionada físicamente, ni el acto delincuencial se da por coerción alguna, si se calcula un daño que además de causar el fraude busca quedar oculto, no dejar rastros que los vincule con el hecho.

		
Repochip: Se conoce como el procedimiento mediante el cual el empleado de la compañía sin la autorización del cliente, repone la SIM de la víctima. Por lo general al final de las jornadas de atención al público cuando el usuario no recibe la atención por parte de la entidad.	La SIM repuesta es entregada al miembro de la organización quien previamente obtuvo la información de la entidad financiera, y procede a cambiar las claves del correo electrónico, y así reconfigurar el acceso a las aplicaciones del banco; para posteriormente habilitar los retiros sin tarjeta.	Posteriormente habilitan para realizar operaciones sin tarjeta y con ello realizar los retiros del dinero.

Delitos Informáticos. Según la ley 1273/2009 se incorporaron al código penal colombiano unos tipos penales con la finalidad de proteger un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Que si se quiere se pensar como un nuevo patrimonio inmaterial de las personas, su derecho a la intimidad y la integridad personal.

Un delito informático o ciberdelito es toda aquella acción antijuridica y culpable, que se da por vías informáticas o que tiene como objetivo convertirse en el medio para la comisión de otros tipos penales como el hurto, la estafa y la extorsión entre otros

MODALIDADES DE FRAUDES ASOCIADOS A LOS DELITOS INFORMÁTICOS

Crimen por Computadora (computer crime), más ampliamente conocido como "delito informático", es una violación de la ley que se realiza en forma deliberada utilizando un equipo informático o contra un equipo informático o una aplicación que se ejecute en él. Se refiere a una actividad donde cualquier infraestructura tecnológica actual que emplee equipos informáticos es el origen, la herramienta o el objetivo de un ataque.

Council of Europe Convention on Cybercrime. Año 2001
http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm

Se define como **malware** a cualquier programa informático que pueda representar algún riesgo de daño hacia un equipo o sus sistemas y aplicaciones. Definido de modo amplio, este perjuicio puede ser del tipo físico (muy poco común), relacionado con los tiempos de procesamiento, económico, de fuga o pérdida de información, de interferencia, interrupción o saturación de servicios, daño explícito a la información, a la reputación, etc.

En forma general, se denomina malware a todos los tipos de programas dañinos actuales: virus informático, troyano, gusano, spyware, ransomware, etc.

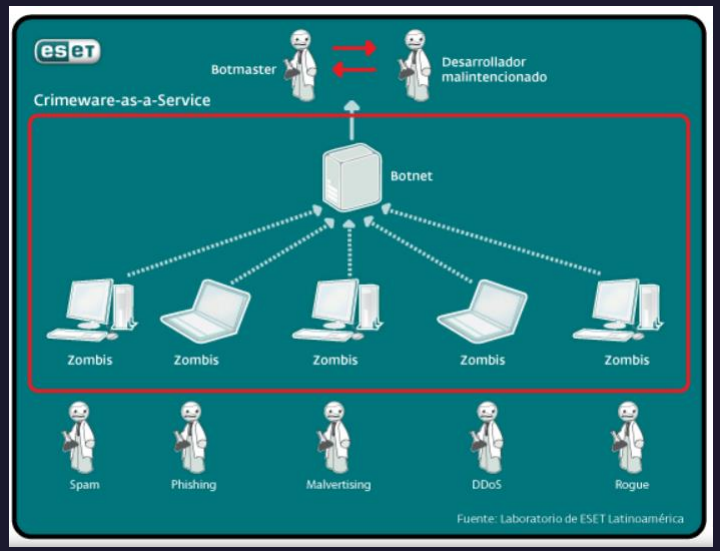
Crimeware: El Crimen del Siglo XXI. ESET Latinoamerica

MODALIDADES DE FRAUDES ASOCIADOS A LOS DELITOS INFORMÁTICOS

Crimeware es cualquier tipo de Malware que ha sido diseñado y desarrollado para perpetrar un crimen del tipo financiero o económico. El término fue definido por el Secretario General del Anti-Phishing Working Group, Peter Cassidy, para diferenciar este tipo de amenaza de otras clases de Software Malicioso.

Actualmente, el **crimeware** envuelve además a todos los procedimientos que sirven de objetivo y plataforma para soportar esas acciones delictivas.

Millones de sistemas infectados son utilizados para enviar malware actualizado, continuando así su ciclo de propagación. En la actualidad, este mecanismo ha permitido reclutar millones de PC que son controladas por un usuario con fines maliciosos, formando lo que se conoce como **botnet**.



Crimeware: El Crimen del Siglo XXI. ESET Latinoamerica

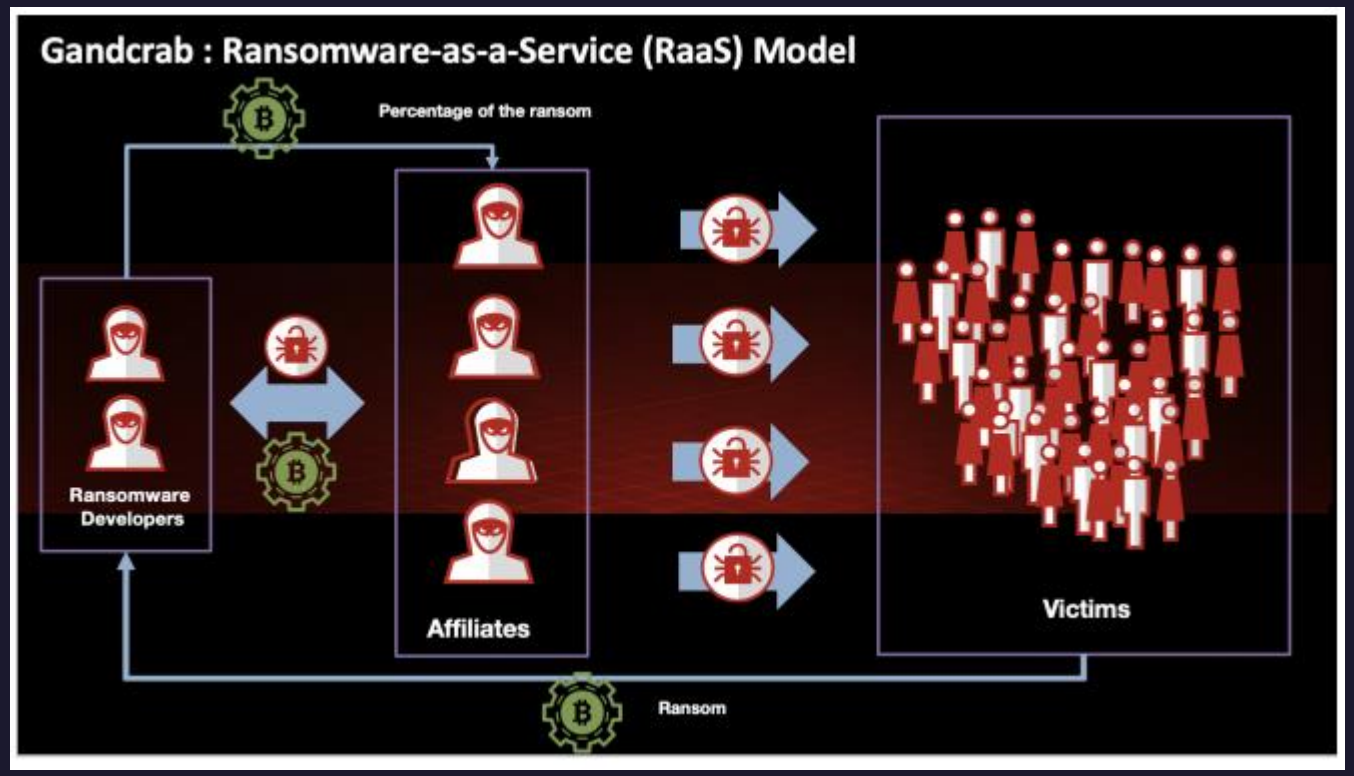
MODALIDADES DE FRAUDES ASOCIADOS A LOS DELITOS INFORMÁTICOS

- El **Crimeware** se propaga haciendo uso de dos canales: la ingeniería social y la explotación de vulnerabilidades.

- **Crimeware** presenta las siguientes características:
  - Actualización constante desde Internet
  - Explotación de diferentes medios para la instalación
  - Empaquetamiento
  - Cifrado y Ofuscamiento
  - Motores polimórficos
  - Técnicas de defensa
  - Instalación silenciosa y ocultamiento
  - Movimiento del código desde el cliente hacia los servidores

Crimeware: El Crimen del Siglo XXI. ESET Latinoamerica

MODALIDADES DE FRAUDES ASOCIADOS A LOS DELITOS INFORMÁTICOS

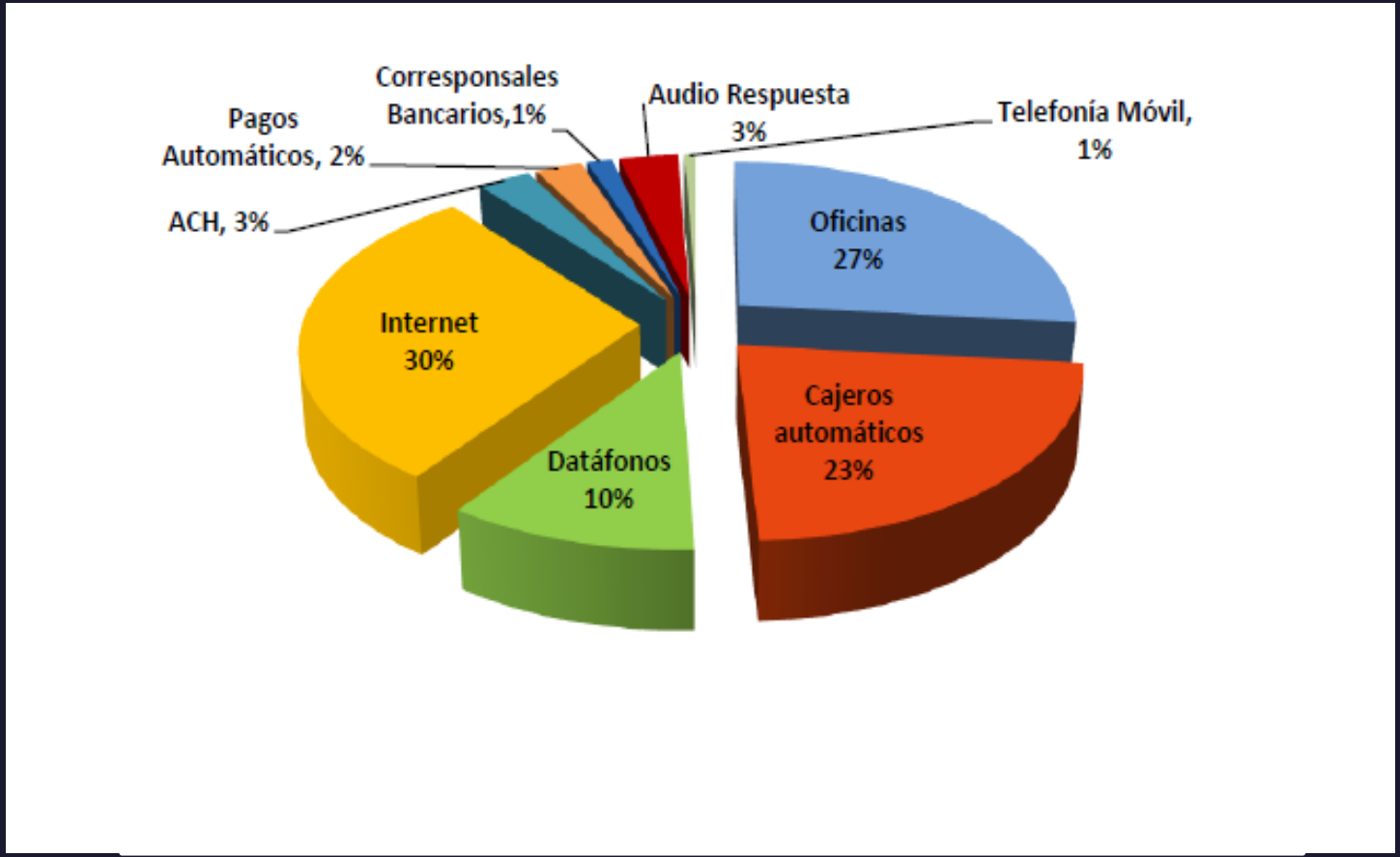


Crimeware as a Service (CaaS), es el ofrecimiento a través de la Web de servicios de creación, actualización, cifrado y polimorfismo del Malware instalado en el cliente.

Criminal to Criminal (C2C). Este concepto se define como el negocio realizado entre criminales a través de diferentes canales. De este modo se conforma el mercado negro virtual, en donde se trafican códigos maliciosos e información obtenida de forma fraudulenta a cambio de dinero

Crimeware: El Crimen del Siglo XXI. ESET Latinoamerica

RIESGO DE FRAUDES ASOCIADOS A LOS DELITOS INFORMÁTICOS



Casos de Fraudes basados en los Delítos Informáticos

Modalidades de Fraudes asociados a los Delitos Informáticos

Rentabilidad obtenida por un spammer

Gastos

- Compra del troyano escrito a medida: U$S 2.000
- Alquiler de la botnet: U$S 5.000
- Costos totales: U$S 7.000 (cabe destacar que se puede alquilar la botnet sin comprar el troyano, y viceversa)

Ganancias

- Un troyano diseñado para enviar spam, infecta 1.000 sistemas
- Cada sistema infectado envía 100.000 correos
- Un anunciante (advertiser), persona que contrata el servicio, paga U$S 0,002 por cada correo
- Ganancia: 1.000 * 100.000 * 0,002 = U$S 200.000

Rentabilidad

- Ganancia Neta (Ganancia - Costos): U$S 200.000 - U$S 7.000 = U$S 193.000
- Índice de rentabilidad (Ganancia / Costos): U$S 193.000 / U$S 7.000 = 25 veces

Crimeware: El Crimen del Siglo XXI. ESET Latinoamerica

5. Casos de Fraudes basados en los Delítos Informáticos

Modalidades de Fraudes asociados a los Delitos Informáticos

Rentabilidad obtenida por un phisher

Gastos

- Un kit de phishing puede adquirirse por U$S 10, asumiendo que el delincuente desee comprarlo y no desarrollarlo por sí mismo
- Costo de una base de datos de correo actualizada: U$S 8
- Alquiler de servidor para enviar correo, por día: U$S 120 (incluso se puede anular este costo)
- Se envían 100.000 correos cada 6 hs. (400.000 en el día). Se asume que no se alquila una botnet y que no se utiliza un troyano como Waledac.
- Sitio vulnerado para alojar la página falsa: U$S 10
- Tarjeta de Crédito válida adquirida a personas que las comercializan ilegalmente: U$S 8
- Registro del dominio (con la Tarjeta de Crédito): U$S 10
- Costos totales: U$S 10 + U$S 8 + U$S 120 + U$S 10 + U$S 8 + U$S 10 = U$S 166

Ganancia

- La tasa de éxito de un correo de phishing es de 0,0001. Una persona es engañada cada 10.000 correos enviados (con 400.000 correos diarios son engañados 40 usuarios)
- Promedio de ganancia (dinero u objetos) obtenido por cuenta robada: U$S 1.000
- Ganancia: 40 * U$S 1.000 = U$S 40.000

Rentabilidad

- **Ganancia Neta (Ganancia - Costos):** U$S 40.000 - U$S 166 = U$S 39.834
- **Índice de rentabilidad (Ganancia / Costos):** 39.834 / 166 = 240 veces

Crimeware: El Crimen del Siglo XXI. ESET Latinoamerica

Casos de Fraudes basados en los Delítos Informáticos

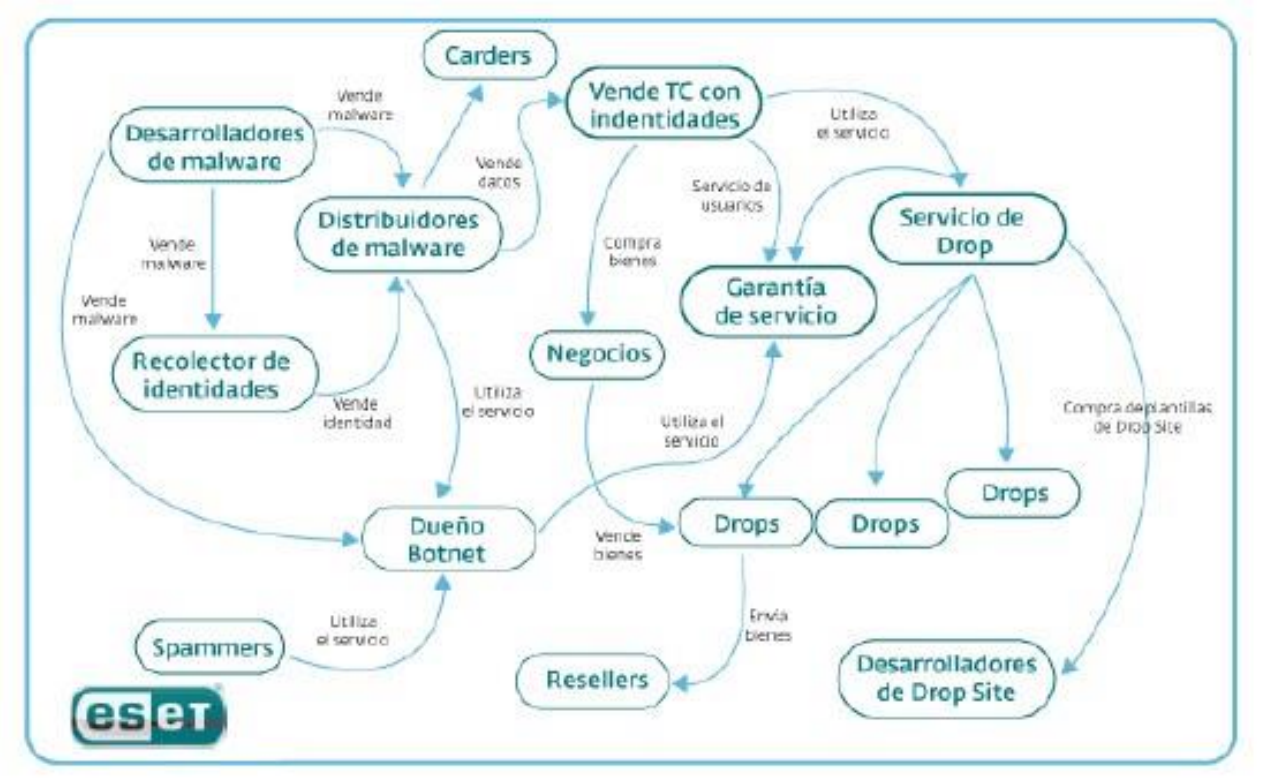
Modalidades de Fraudes asociados a los Delitos Informáticos

Rentabilidad por tipo de acción fraudulenta

Acción	Rentabilidad
Phishing	400 (en el ejemplo del presente trabajo, 240)
Remates falsos desde cuentas robadas	317
Spam	187 (en el ejemplo del presente trabajo, 25)
Simulación de tareas con Bots	166
Instalación de Adware/Spyware	102
Extorsión online	32
Tráfico de credenciales	31
Inyecciones de código	27
Compra/venta de números de tarjetas de crédito robadas (carding)	9

Casos de Fraudes basados en los Delítos Informáticos

Actores

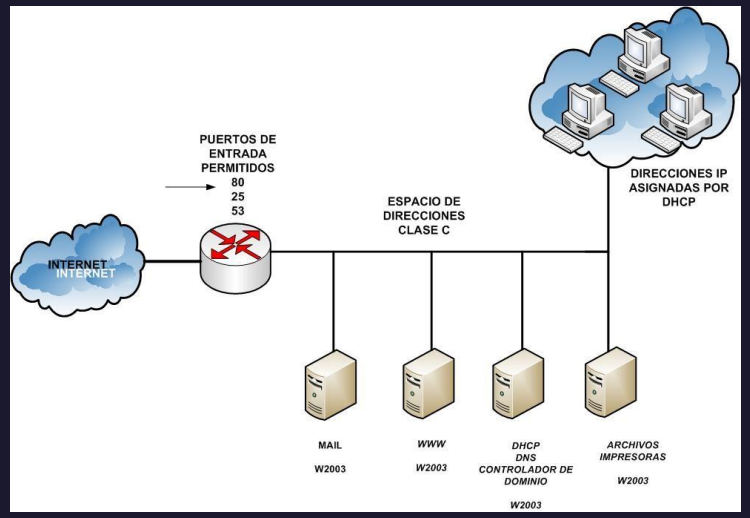


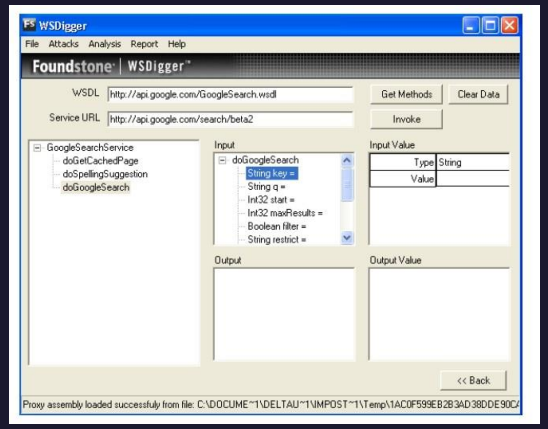
Crimeware: El Crimen del Siglo XXI. ESET Latinoamerica

Casos de Fraudes basados en los Delítos Informáticos

Modalidades de Fraudes asociados a los Delitos Informáticos – Ley 1273 de 2009

Artículo 269 A. *Acceso abusivo a un sistema informático.* El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.



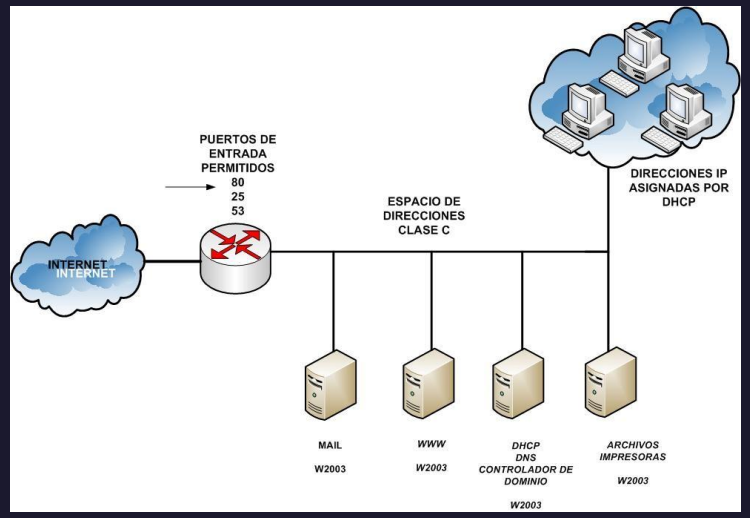


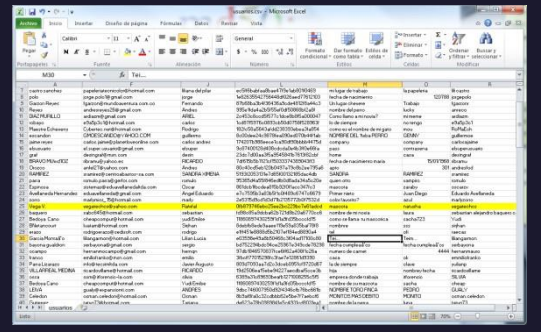
Prueba WSDigger

5. Casos de Fraudes basados en los Delítos Informáticos

Modalidades de Fraudes asociados a los Delitos Informáticos – Ley 1273 de 2009

Artículo 269 A. *Acceso abusivo a un sistema informático.* El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.



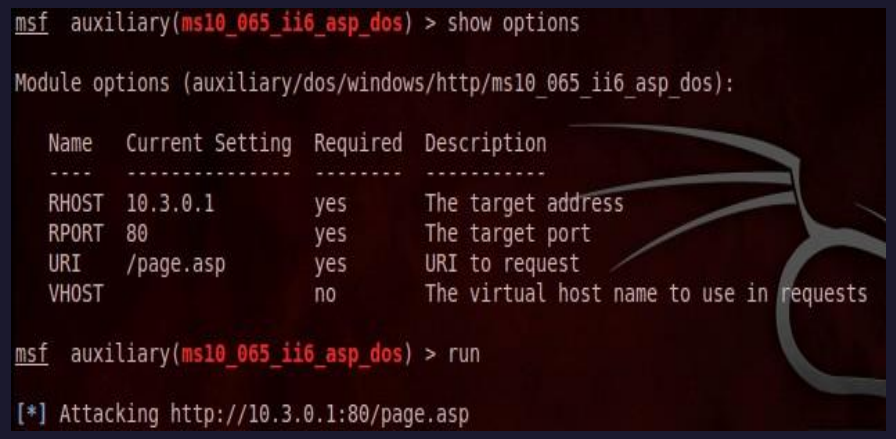


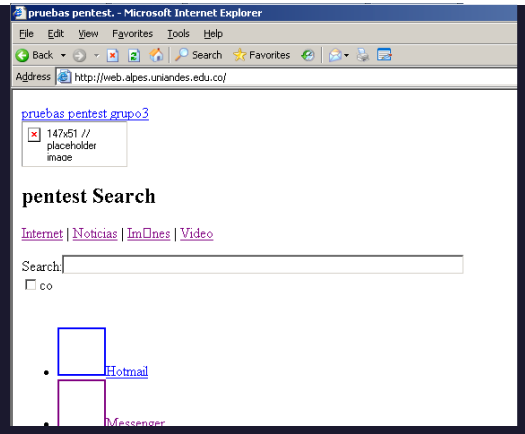
SQL Injection

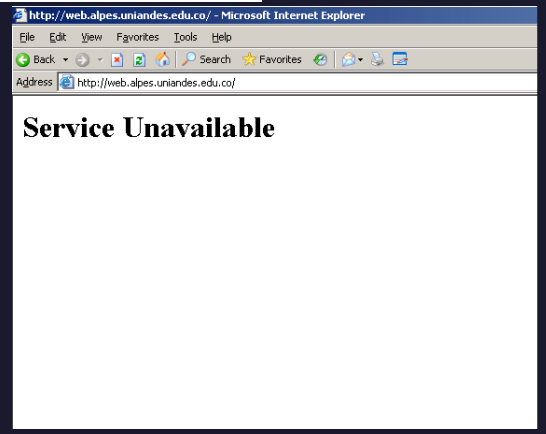
Casos de Fraudes basados en los Delítos Informáticos

Modalidades de Fraudes asociados a los Delitos Informáticos – Ley 1273 de 2009

Artículo 269 B. *Obstaculización ilegítima de sistema informático o red de telecomunicación.* El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.







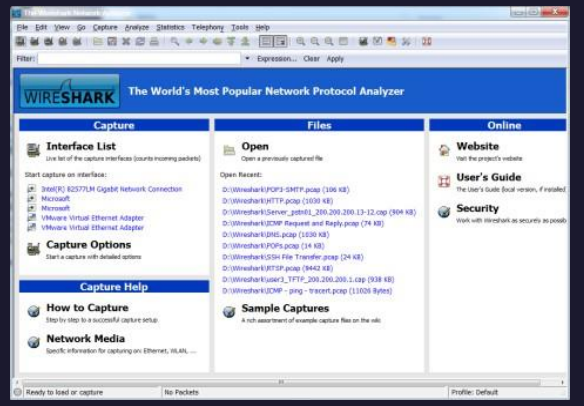
Casos de Fraudes basados en los Delítos Informáticos

Modalidades de Fraudes asociados a los Delitos Informáticos – Ley 1273 de 2009

Artículo 269 C. *Interceptación de datos informáticos*. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.



email



VoIP

Casos de Fraudes basados en los Delítos Informáticos

Modalidades de Fraudes asociados a los Delitos Informáticos – Ley 1273 de 2009

Artículo 269 E: *Uso de software malicioso*. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.



Spamming

Casos de Fraudes basados en los Delítos Informáticos

Modalidades de Fraudes asociados a los Delitos Informáticos – Ley 1273 de 2009

Artículo 269 F. *Violación de datos personales*. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.



Phishing

Casos de Fraudes basados en los Delítos Informáticos

Modalidades de Fraudes asociados a los Delitos Informáticos – Ley 1273 de 2009

Artículo 269 G: *Suplantación de sitios web para capturar datos personales*. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

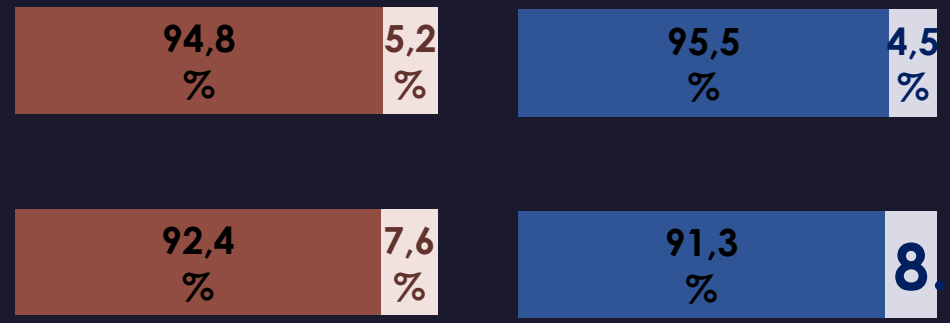
COMPARATIVO DELITOS INFORMATICOS

Año corrido 1 de enero al 29 de septiembre

Entradas Efectivas (Año hecho = Año Entrada)

	2021	2022	Var. %
Delitos Informáticos	15.022	20.937	+39%
Medios informáticos	15.566	22.055	+42%

Entradas Efectivas* por año de hechos



Avance de esclarecimiento delitos informáticos año corrido 2022 vs 2021

Seccional	Avance de esclarecimiento año corrido 2022	Avance de esclarecimiento año corrido 2021	Variación %	Variación absoluta	Casos año corrido 2022	Casos año corrido 2021	Tasa de avance de esclarecimiento 2022	Tasa de avance de esclarecimiento 2021
Caquetá	3	3	0,00 %	0	27	122	11,11 %	2,46 %
La Guajira	5	0	-	5	46	37	10,87 %	0,00 %
Guainía - Vaupés	1	0	-	1	11	9	9,09 %	0,00 %
Arauca	1	1	0,00 %	0	19	21	5,26 %	4,76 %
Putumayo	3	1	200,00 %	2	60	40	5,00 %	2,50 %
Boyacá	10	0	-	10	210	190	4,76 %	0,00 %
Cauca	16	0	-	16	338	199	4,73 %	0,00 %
Quindío	4	2	100,00 %	2	159	205	2,52 %	0,98 %
Tolima	10	6	66,67 %	4	652	474	1,53 %	1,27 %
Risaralda	7	3	133,33 %	4	566	313	1,24 %	0,96 %
Meta	5	1	400,00 %	4	445	332	1,12 %	0,30 %
Norte De Santander	4	1	300,00 %	3	406	438	0,99 %	0,23 %
Bolívar	3	3	0,00 %	0	356	354	0,84 %	0,85 %
Magdalena Medio	1	0	-	1	124	90	0,81 %	0,00 %
Córdoba	2	1	100,00 %	1	295	267	0,68 %	0,37 %
Sucre	1	0	-	1	170	139	0,59 %	0,00 %
Santander	3	2	50,00 %	1	575	478	0,52 %	0,42 %
Total Nacional	102	51	100,00 %	51	20.937	15.022	0,49 %	0,34 %
Caldas	1	1	0,00 %	0	218	138	0,46 %	0,72 %
Cesar	1	2	-50,00 %	-1	253	72	0,40 %	2,78 %
Cali	5	6	-16,67 %	-1	1.561	1.147	0,32 %	0,52 %
Huila	1	0	-	1	380	215	0,26 %	0,00 %
Magdalena	1	1	0,00 %	0	382	266	0,26 %	0,38 %
Medellín	5	2	150,00 %	3	3.661	1.588	0,14 %	0,13 %
Atlántico	1	2	-50,00 %	-1	758	685	0,13 %	0,29 %
Bogotá	7	8	-12,50 %	-1	5.871	5.206	0,12 %	0,15 %
Cundinamarca	1	2	-50,00 %	-1	1.896	960	0,05 %	0,21 %
Nariño	0	0	-	0	383	337	0,00 %	0,00 %
Guaviare	0	0	-	0	15	5	0,00 %	0,00 %
Chocó	0	0	-	0	167	90	0,00 %	0,00 %
San Andrés	0	0	-	0	20	5	0,00 %	0,00 %
Casanare	0	0	-	0	153	106	0,00 %	0,00 %
Valle Del Cauca	0	1	-100,00 %	-1	150	164	0,00 %	0,61 %
Vichada	0	0	-	0	2	2	0,00 %	0,00 %
Antioquia	0	2	-100,00 %	-2	608	325	0,00 %	0,62 %
Amazonas	0	0	-	0	0	3	-	0,00 %

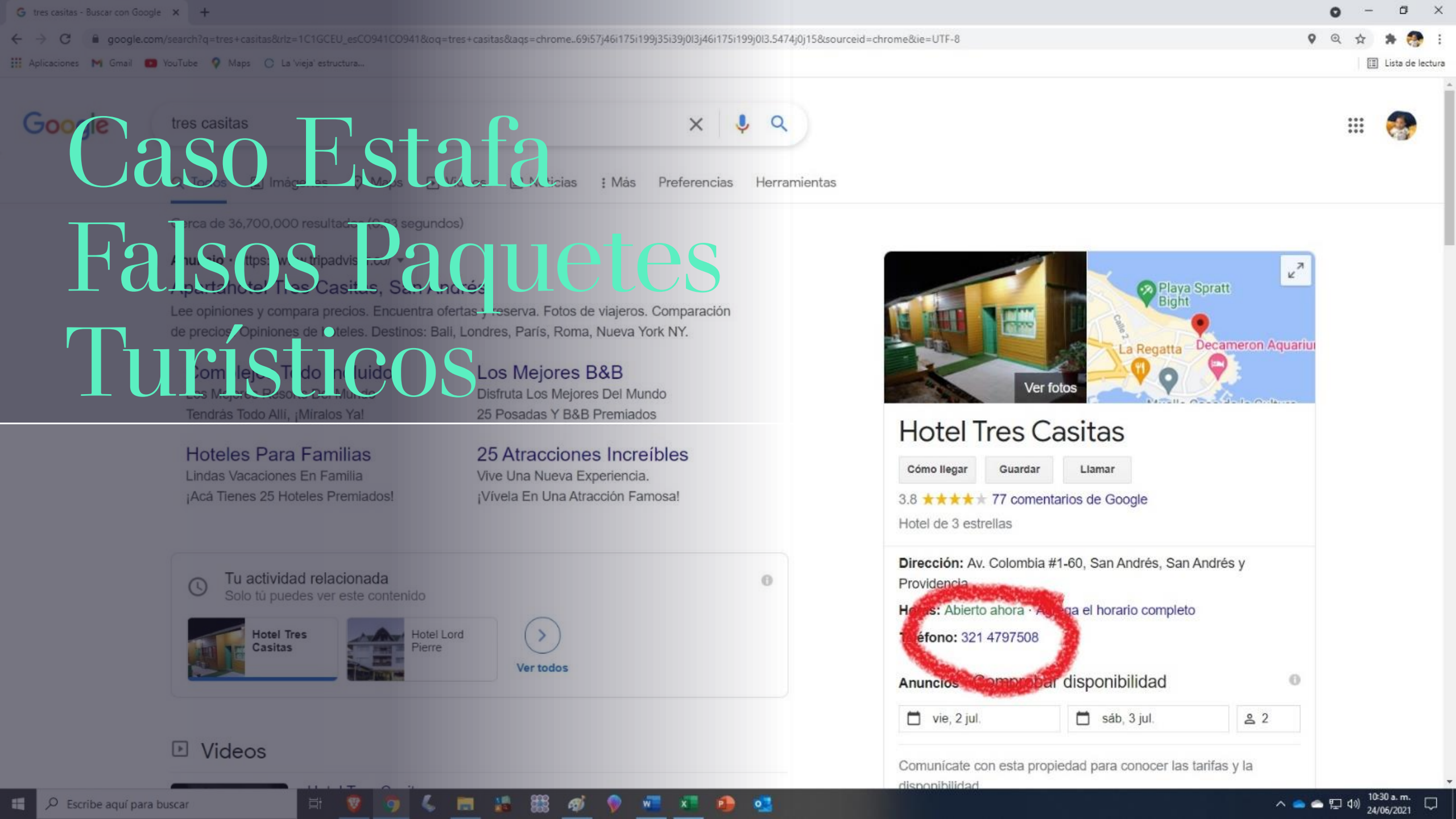
Avance de esclarecimiento medio informático año corrido 2022 vs 2021

Seccional	Avance de esclarecimiento año corrido 2022	Avance de esclarecimiento año corrido 2021	Variación %	Variación absoluta	Casos año corrido 2022	Casos año corrido 2021	Tasa de avance de esclarecimiento 2022	Tasa de avance de esclarecimiento 2021
Quindío	38	0	-	38	276	197	13,77 %	0,00 %
Magdalena Medio	11	3	266,67 %	8	135	133	8,15 %	2,26 %
Cauca	10	1	900,00 %	9	349	292	2,87 %	0,34 %
Casanare	3	1	200,00 %	2	118	94	2,54 %	1,06 %
Bolívar	11	2	450,00 %	9	497	391	2,21 %	0,51 %
Norte De Santander	6	16	-62,50 %	-10	331	362	1,81 %	4,42 %
Tolima	7	3	133,33 %	4	529	447	1,32 %	0,67 %
Santander	10	8	25,00 %	2	928	624	1,08 %	1,28 %
La Guajira	1	0	-	1	109	60	0,92 %	0,00 %
Antioquia	3	2	50,00 %	1	356	316	0,84 %	0,63 %
Caldas	3	1	200,00 %	2	403	280	0,74 %	0,36 %
Córdoba	2	0	-	2	274	272	0,73 %	0,00 %
Risaralda	4	3	33,33 %	1	559	408	0,72 %	0,74 %
Boyacá	4	3	33,33 %	1	571	365	0,70 %	0,82 %
Meta	4	0	-	4	634	385	0,63 %	0,00 %
Total Nacional	138	68	102,94 %	70	22.055	15.566	0,63 %	0,44 %
Medellín	11	1	1.000,00 %	10	2.516	1.509	0,44 %	0,07 %
Atlántico	1	3	-66,67 %	-2	436	793	0,23 %	0,38 %
Cali	3	12	-75,00 %	-9	2.252	1.741	0,13 %	0,69 %
Bogotá	6	1	500,00 %	5	6.696	4.709	0,09 %	0,02 %
San Andrés	0	0	-	0	31	13	0,00 %	0,00 %
Sucre	0	0	-	0	188	172	0,00 %	0,00 %
Valle Del Cauca	0	0	-	0	670	278	0,00 %	0,00 %
Vichada	0	0	-	0	1	2	0,00 %	0,00 %
Putumayo	0	0	-	0	74	53	0,00 %	0,00 %
Amazonas	0	0	-	0	2	6	0,00 %	0,00 %
Nariño	0	0	-	0	288	183	0,00 %	0,00 %
Magdalena	0	3	-100,00 %	-3	381	189	0,00 %	1,59 %
Guaviare	0	0	-	0	25	15	0,00 %	0,00 %
Guainía - Vaupés	0	0	-	0	12	7	0,00 %	0,00 %
Cundinamarca	0	0	-	0	1.287	689	0,00 %	0,00 %
Chocó	0	0	-	0	67	41	0,00 %	0,00 %
Cesar	0	4	-100,00 %	-4	287	166	0,00 %	2,41 %
Caquetá	0	0	-	0	159	118	0,00 %	0,00 %
Arauca	0	1	-100,00 %	-1	42	17	0,00 %	5,88 %
Huila	0	0	-	0	572	239	0,00 %	0,00 %

Dificultades en la actividad investigativa y la evidencia digital:

- La imposibilidad de la comprobación de datos al momento de adquirir el producto financiero virtual
- Dificultades de identificar el lugar en donde se adquirió el producto para establecer jurisdicción.
- Se le está atribuyendo responsabilidad penal a víctimas de falsedad personal.
- La lesión patrimonial a las entidades financieras.
- La falta de unificación en los datos presentados por las entidades financieras y las empresas de telefonía móvil. Entonces no sabemos qué pedirle a quien
- Colapso de audiencias para búsquedas selectivas y los respectivos controles posteriores.

Caso Estafa Falsos Paquetes Turísticos



Caso Estafa Falsos Paquetes Turísticos

Total Productos Financieros 37

Bancolombia:

91215476141
91215590734
91216981044
91222303872
91200385107
91200343901
91202343908

Banco de Bogotá

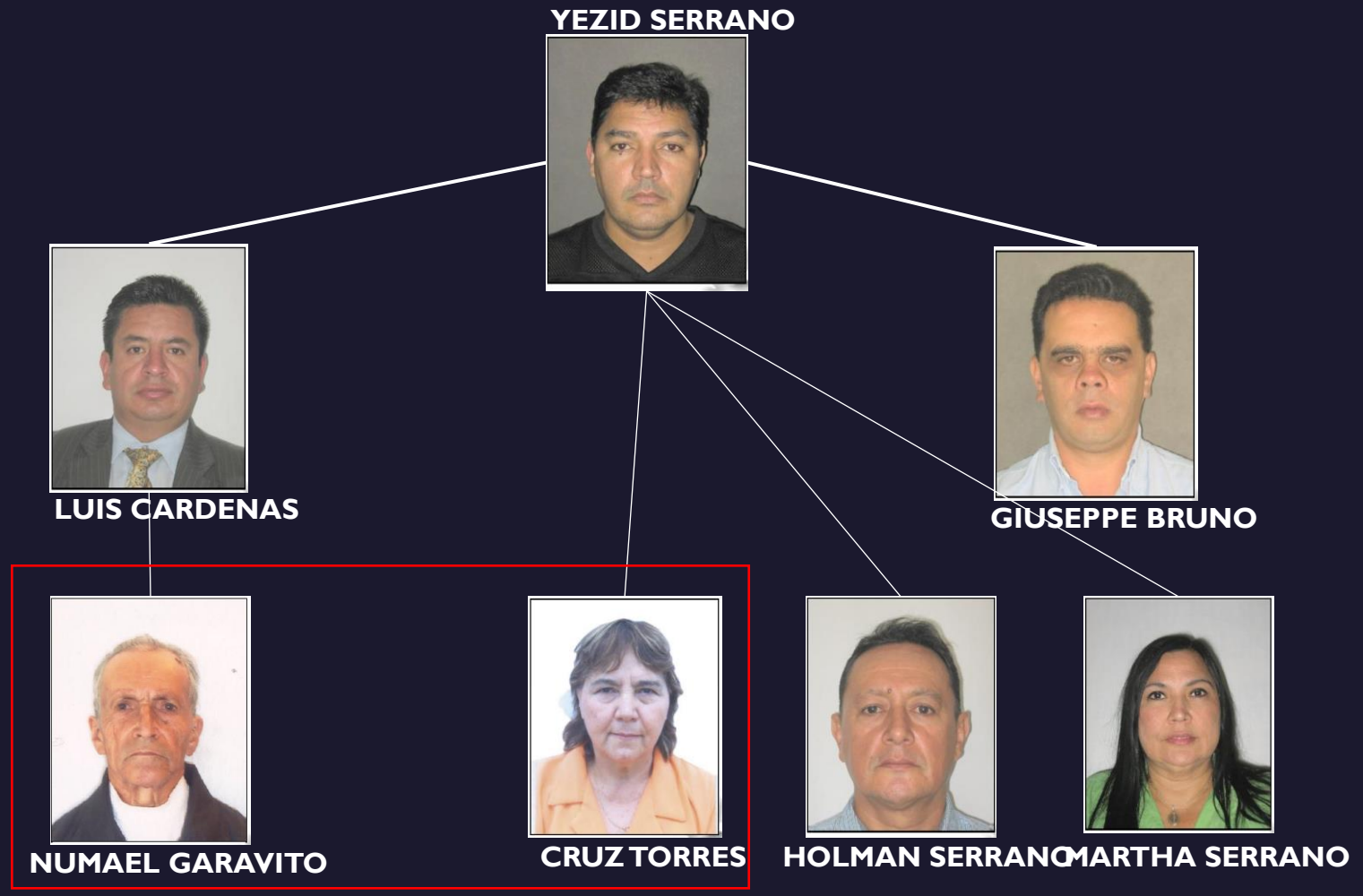
469507958

Banco Colpatria

5732007104

DIRECCIÓN SECCIONAL ATLÁNTICO
Cuerpo Técnico de Investigación – Sección de Análisis Criminal

ESTRUCTURA CRIMINAL ESTAFADORES TURISTICOS



Retos:

- La Hiperautomatización: La automatización de muchos procesos con base en el uso de la inteligencia artificial (Watson).
- La Multiexperiencia: Las nuevas plataformas de conversación mejorarán la experiencia de los usuarios gracias a tecnologías como la realidad virtual, la realidad aumentada o la realidad mixta que nos conducirán a una futura experiencia multisensorial.
- La Democratización de la experticia: Las personas tendrán acceso a la experiencia técnica o empresarial sin necesidad de conocimientos complejos.
- Maquinas capaces de aprender: Reconocimiento de patrones, Interacción con las personas o otras maquinas, Algoritmos que gestionan la gran cantidad de datos existentes.
- Transparencia y trazabilidad.

La mejor manera de empezar es dejar de hablar y comenzar a actuar.

Walt Disney



Gracias





Tendencias de los Delitos Informáticos.

Programa Profesionales® en CIBERCRIMINALIDAD

Juan Diego Jiménez León.
Profesor Maestría en seguridad de la Información
Coordinador Infraestructura Tecnológica y Laboratorio Forense
jujimene@uniandes.edu.co
2020



Temas

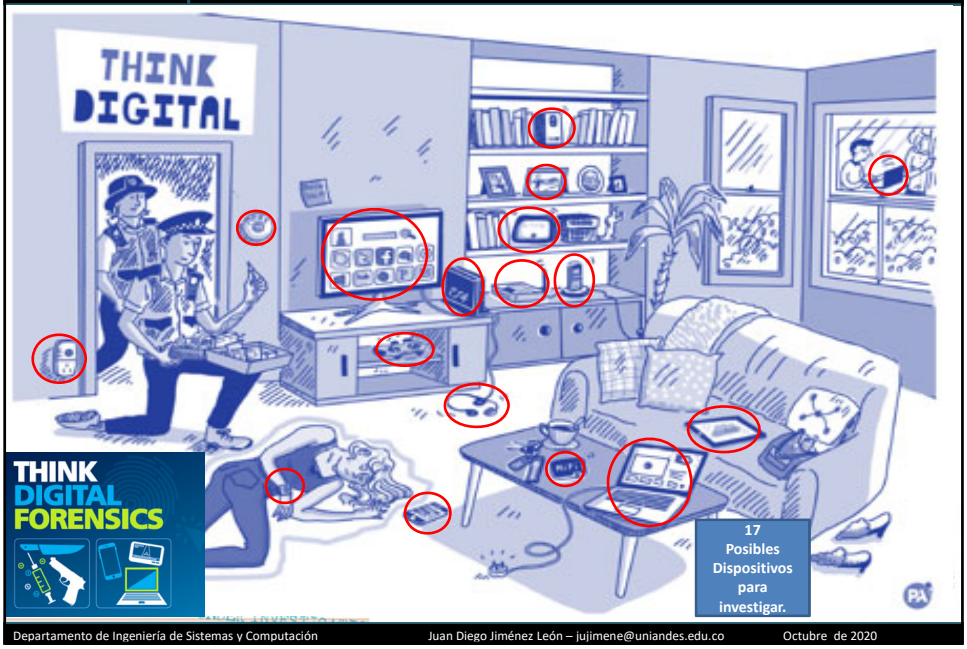
- Tendencias Tecnológicas
- Retos
- Balance del Cibercrimen 2019
- Ciberdelitos
- Paradigmas Futuros



Temas

- **Tendencias Tecnológicas**
  - Retos
  - Balance del Cibercrimen 2019
  - Ciberdelitos
  - Paradigmas Futuros





Fuente: Gartner



1



Hyperautomation

Hiperautomatización

La hiperautomatización, aparte de utilizar inteligencia artificial y machine learning, va más allá de las herramientas que se puede automatizar, para automatizar procesosy potencializar a los humanos. Desde Gartner señalan también la importancia de los pasos de la propia automatización: descubrir, analizar, diseñar, automatizar, medir, monitorear y reevaluar.





2



Multiexperience

Multiexperiencia

La nuevas plataformas de conversación mejorarán la experiencia de usuario gracias a tecnologías como la realidad virtual, la realidad aumentada o la realidad mixta que nos conducirán a una futura experiencia multisensorial y multimodal.





3

Democratization

Democratización del 'expertise'
Gracias a la democratización del expertise, las personas tendrán acceso a la experiencia técnica o empresarial sin necesitar de formación compleja. Gartner señala cuatro aspectos clave que serán democratizados; datos y análisis, desarrollo, diseño y conocimiento.



4

Human Augmentation

Human augmentation
¿Cómo podrá la tecnología proporcionar mejoras cognitivas y física en los humanos? Nuestros expertos del Future Trends Forum analizan los avances científicos y tecnológicos que aumentan y mejoran las capacidades humanas en el informe "Superhumanos". Ver https://www.fundacionbankinter.org/ftf/tendencias/superhumanos



5

Transparency and Traceability

Transparencia y trazabilidad

En un mundo con consumidores cada vez más concientes con la privacidad y la protección de datos, la transparencia y la trazabilidad se presentan como elementos fundamentales a tener en cuenta por parte de las empresas.





6

Empowered Edge

The Empowered Edge

Gartner posiciona el Edge computing como un “factor dominante en prácticamente todas las industrias y casos de uso”.

La informática perimetral o cercana al límite, edge computing, es la computación que se realiza en la fuente de datos o cerca de ella, en lugar de confiar en la nube para hacer todo el trabajo





7

Distributed Cloud

Examina una evolución importante en la computación en la nube donde las aplicaciones, plataformas, herramientas, seguridad, administración y otros servicios están cambiando físicamente de un modelo de centro de datos centralizado a uno en el que los servicios se distribuyen y se entregan en el punto de necesidad. El punto de necesidad puede extenderse a los centros de datos del cliente o hasta los dispositivos de borde.





8

Autonomous Things

Objetos Autónomos

Los objetos autónomos utilizan la inteligencia artificial para ofrecer comportamientos avanzados y así interactuar de forma más natural con el entorno y con las personas.

Explora cómo se mejoran las cosas físicas en los espacios que rodean a las personas con mayores capacidades para percibir, interactuar, moverse y manipular estos espacios con varios niveles de orientación humana, autonomía y colaboración.





9

Practical Blockchain

Blockchain práctico
Gartner destaca algunas de las posibles aplicaciones de blockchain como el seguimiento de activos, la gestión de identidad o los contratos inteligentes. Se centra en cómo se puede aprovechar esta tecnología en casos prácticos de uso empresarial que se están expandiendo en los próximos tres a cinco años.





10

AI Security

Seguridad IA
La aplicación de la inteligencia artificial y machine learning supondrán grandes ventajas para tendencias como la hiperautomatización o los objetos autónomos, pero genera nuevos desafíos en materia de seguridad.





Tendencia #11

- Computación Cuántica

EL ESPECTADOR

Google anuncia que logró la "supremacía cuántica" con un computador

Ciencia 21 Sep 2019 - 1:21 PM
Por: Redacción Vivir

Según la información filtrada al Financial Times, la empresa habría logrado que un computador cuántico realizara en tan sólo tres minutos y 20 segundos un cálculo le tomaría a la supercomputadora más avanzada del mundo alrededor de 10,000 años.

CASE Np.21567
LEVEL ONE SECURITY CLEARANCE
HACKING CASE 21567 UNDER INVESTIGATION

EL TIEMPO

Drones, la nueva arma letal de la mafia en Colombia

En Tumaco, disidencias de ex-Farc los cargan de explosivos para atacar al Ejército. ¿Qué riesgo hay?

Por: Unidad Investigativa | 22 de septiembre 2019 , 10:05 p.m.

Martes 17 de septiembre. Zona rural de Tumaco, Nariño, región entapetada de narcocultivos.

Inteligencia del Ejército reportó el hallazgo de dos drones –aviones no tripulados– con 600 gramos de explosivos adheridos a su estructura.



Algún delito informático se puede tipificar?

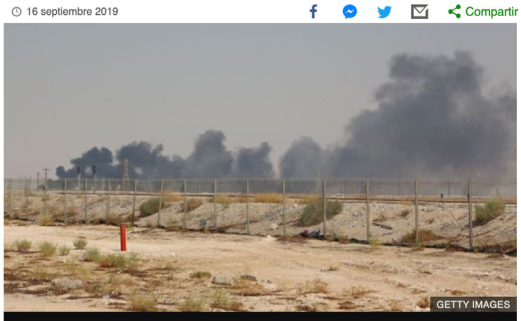
Que elementos tecnológicos se pueden adquirir, como evidencia?

HACKING CASE 21567 UNDER INVESTIGATION

Saudi Aramco, la empresa petrolera más rentable del mundo que fue blanco de ataques "con drones" (y que puede hacer que se disparen los precios del crudo)

Redacción
BBC News Mundo

16 septiembre 2019 Compartir



La planta de la estatal Aramco en Abqaiq fue una de las principales afectadas por los ataques.

Los ataques de un escuadrón de drones a dos instalaciones petroleras en Arabia Saudita, ocurridos el sábado, pusieron en alerta los mercados de la energía.

EL TIEMPO

Curioso 'wearable' que cambia la cara y evita el reconocimiento facial

Creadores del dispositivo de proyección evitan su relación con las protestas en Hong Kong.

Un video sobre una banda en la cabeza que proyecta sobre su rostro la cara de Leonardo DiCaprio o el personaje famoso que usted elija se ha hecho viral en el marco de las multitudinarias manifestaciones en Hong Kong, **que han sido escenario de despliegue de numerosas estrategias para evadir el reconocimiento facial por parte de las autoridades.**

El proyector de cara portátil, como ilustra el video, permite al usuario proyectar sobre su rostro una apariencia diferente. Aunque al ojo humano es evidente este truco, para las cámaras, que cada vez son más inteligentes, podría pasar desapercibido. **Sin embargo, la tecnología aún no se comercializa ni tampoco apoya el movimiento político en el territorio asiático.**



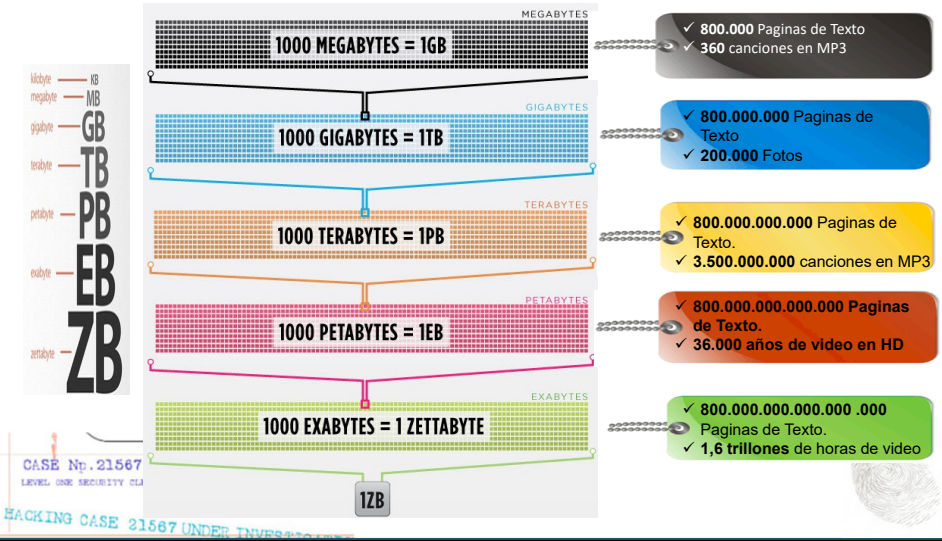


Temas

- ~~Tendencias Tecnológicas~~
- **Retos**
- Balance del Cibercrimen 2019
- Ciberdelitos
- Paradigmas Futuros



Tamaños de la Evidencia



Explosión de complejidad

Específicamente, la evidencia ya no se limita a un solo host sino que se disemina entre diferentes ubicaciones físicas o virtuales, como redes sociales en línea, carteras de criptomonedas, maquinaria CaaS y unidades de almacenamiento personal conectadas a la red.









Privacidad y Legitimidad

Desafortunadamente, la recopilación de información para reconstruir y localizar un ataque puede violar gravemente la privacidad de los usuarios y está vinculada a otros obstáculos cuando la computación en la nube está involucrada.

Un desafío importante para la ciencia forense digital moderna será ejecutar investigaciones legalmente, por ejemplo, sin violar las leyes en escenarios sin fronteras.



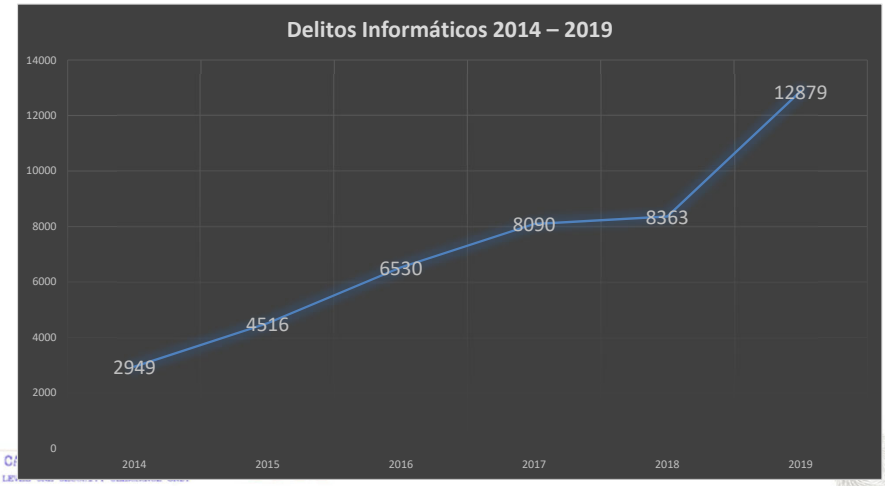




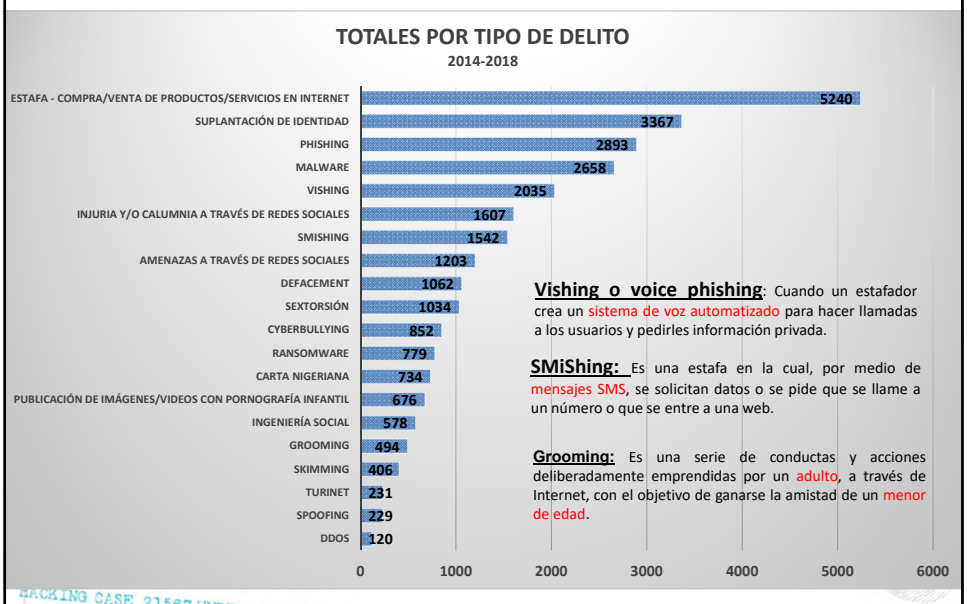
Temas

- ~~Tendencias Tecnológicas~~
- ~~Retos~~
- **Balance del Cibercrimen 2019**
- Ciberdelitos
- Paradigmas Futuros

CASE NO. 21567
LEVEL ONE SECURITY CLEARANCE ONLY
HACKING CASE 21567 UNDER INVESTIGATION



HACKING CASE 21567 UNDER INVESTIGATION


TOTALES POR TIPO DE DELITO
2014-2018
ESTAFA - COMPRA/VENTA DE PRODUCTOS/SERVICIOS EN INTERNET 5240
SUPLANTACIÓN DE IDENTIDAD 3367
PHISHING 2893
MALWARE 2658
VISHING 2035
INJURIA Y/O CALUMNIA A TRAVÉS DE REDES SOCIALES 1607
SMISHING 1542
AMENAZAS A TRAVÉS DE REDES SOCIALES 1203
DEFACEMENT 1062
SEXTORSIÓN 1034
CYBERBULLYING 852
RANSOMWARE 779
CARTA NIGERIANA 734
PUBLICACIÓN DE IMÁGENES/VIDEOS CON PORNOGRAFÍA INFANTIL 676
INGENIERÍA SOCIAL 578
GROOMING 494
SKIMMING 406
TURINET 231
SPOOFING 229
DDOS 120
0 1000 2000 3000 4000 5000 6000
Vishing o voice phishing: Cuando un estafador crea un sistema de voz automatizado para hacer llamadas a los usuarios y pedirles información privada.
SMiShing: Es una estafa en la cual, por medio de mensajes SMS, se solicitan datos o se pide que se llame a un número o que se entre a una web.
Grooming: Es una serie de conductas y acciones deliberadamente emprendidas por un adulto, a través de Internet, con el objetivo de ganarse la amistad de un menor de edad.


PERIODO 2020
Corte del 01 de enero al 21 de septiembre de cada año
5 Delitos de mayor afectación
PERIODO COVID-19
Corte del 25 de marzo al 21 de septiembre de cada año
Variación 2019 2020
2019 2020 Variación
124% 2.375 5.314 Violación de datos personales 1.564 4.115 163%
386% 712 3.461 Suplantación de sitios web 488 2.612 435%
84% 1.176 2.166 Transferencia no consentida de activos 774 1.601 107%
215% 309 972 Interceptación de datos informáticos 193 716 271%
68% 2.673 4.490 Acceso abusivo a un sistema informático 1.798 3.382 88%
76% 16.043 28.207 TOTAL 9 delitos ley 1273 10.853 20.990 93%

Temas

- ~~Tendencias Tecnológicas~~
- ~~Retos~~
- ~~Balance del Cibercrimen 2018~~
- **Ciberdelitos**
- Paradigmas Futuros

ESTAFAS (5.240)

BEC (Bussiness Email Compromise)

Que es el BEC?

El *Business E-mail Compromise* o *BEC*, es definido por el FBI como una **estafa sofisticada** dirigida a las empresas que trabajan con **proveedores extranjeros** y que por lo tanto, realizan de manera regular pagos a través de **transferencias bancarias** internacionales.

La estafa se ejecuta comprometiendo las cuentas de correos electrónicos de los directivos de la empresa, de manera concreta, los ciberdelincuentes ubican y atacan las cuentas de los responsables de autorizar y realizar los pagos a los proveedores.

Las principales técnicas utilizadas para estos ataques de intrusión son la **ingeniería social, el mail spoofing (suplantación de identidad), el phishing, los keylogger y el malware.**

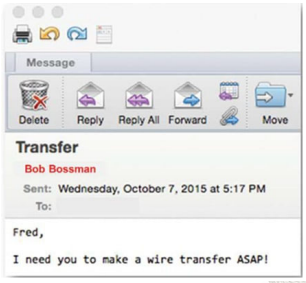
ESTAFAS (5.240)

BEC (Bussiness Email Compromise)

Esas amenazas son sumamente dirigidas y comienzan con una buena cantidad de investigación a fin de encontrar a la persona adecuada dentro de una organización, averiguar su cadena de mando y determinar la mejor hora para enviarle el mensaje; de preferencia cuando el "remitente" se encuentre de viaje para aumentar la posibilidades de éxito. .

2. Business Email Hack – CEO Masquerading



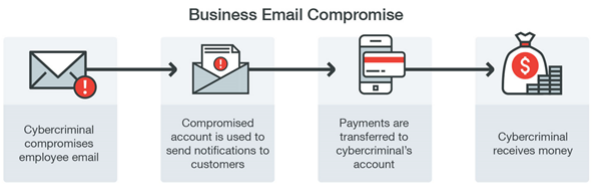


ESTAFAS (5.240)

BEC (Bussiness Email Compromise)

A quienes buscan:

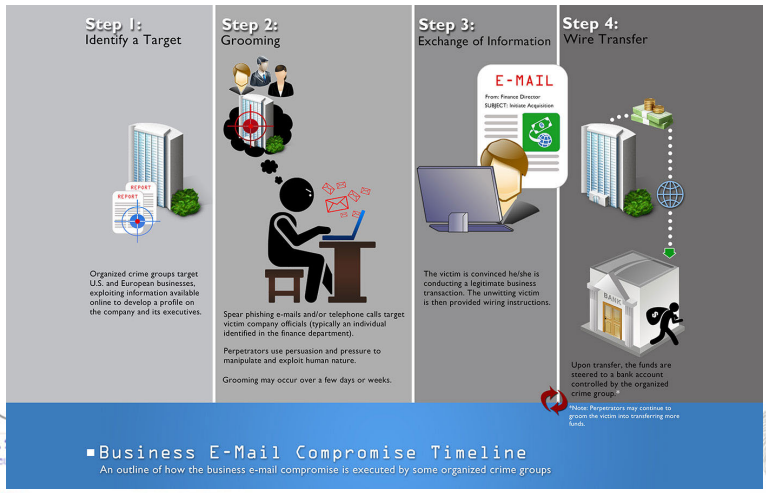
1. TESORERIA
2. GERENCIA
3. PROVEEDORES





ESTAFAS (5.240)

BEC (Bussiness Email Compromise)





ESTAFAS (5.240)

BEC (Bussiness Email Compromise)

Dominio de remitente falso o suplantado

De: juan.ochoa@cultivosfl.com 1
Enviado: Thursday, February 23, 2017 3:18 PM
Para: ana.arias@cultivosfl.com
Asunto: Proceso de pago INMEDIATO 2

Un asunto urgente solicitando un tramite urgente

Buenas tardes,

Ana, le pido que se comunique con el Dr. [redacted].com a la brevedad, y le pida instrucciones acerca de una transferencias que debemos realizar.

Es un asunto reservado, y así debe mantenerse hasta su conclusión. 3

Me mantiene informado luego de cada transferencia, a este correo.
juan.ochoa.duarte@directors.com.co

Cordialmente,
JUAN OCHOA DUARTE
Director Operativo 4

Cuerpo del correo, necesidad urgente de una transferencia

Posición del remitente del correo

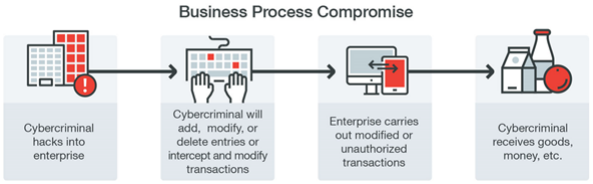




ESTAFAS (5.240)

BPC (Bussiness Process Compromise)

Business Process Compromise (BPC) se basan en alterar procesos y sistemas críticos, que continúan funcionando pero de manera no autorizada. BPC es un ataque más complejo que implica modificar procesos para generar un resultado diferente.







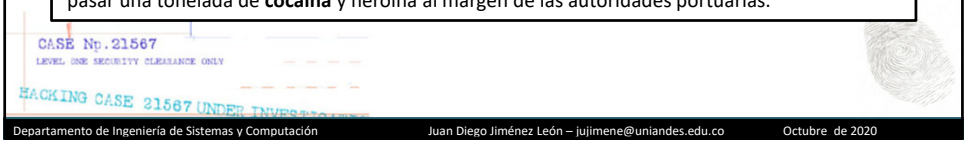
ESTAFAS (5.240)

BPC (Bussiness Process Compromise)

BPC requiere un conocimiento en profundidad de los sistemas de procesamiento de transacciones financieras.

El robo al Banco Central de Bangladesh es un ejemplo reciente de **BPC**. En este ataque, que provocó pérdidas de hasta **81 millones de dólares**, los ciberdelincuentes demostraron que tenían una idea clara de cómo funciona la plataforma financiera **SWIFT** y que conocían las debilidades de los bancos asociados que la utilizan. Al comprometer la red informática del Banco Central de Bangladesh, los cibercriminales fueron capaces de rastrear cómo se realizaron las transferencias y aprovechar las credenciales del banco para llevar a cabo **transacciones no autorizadas**.

BPC también se extiende más allá de las transacciones financieras. En 2016, un sistema de seguimiento de contenedores en el **puerto marítimo** de Amberes en Bélgica fue hackeado para pasar una tonelada de **cocaína** y heroína al margen de las autoridades portuarias.



ESTAFAS (5.240)

BEC (Bussiness Email Compromise)

- **Caso ejemplo (trabajo en grupos de 2 o 3 personas)**
  - **Andrés Pérez** el Gerente de una compañía de manufactura realiza negocios con una **empresa en China**, para la compra de materia prima "Telas". El valor de la compra es de **U$400.000**, los cuales se vienen negociando tiempo atrás entre el Gerente de la compañía y la persona de la compañía China encargada del área internacional de negocios.
  - El medio de comunicación principal es el **correo electrónico**. Pactan el negocio para ser pagado **50% con el pedido y el otro 50% contra entrega**. Cabe mencionar que ambos llevan relaciones comerciales de años.
  - El Sr. **Andrés Pérez** deja encargada al área contable para realizar los pagos, adicionando a los correos la persona encargada **Antonio Rodríguez**. Posterior a esto, les llega un correo de la empresa China confirmándoles que ya tienen todo listo, y les envían los datos para realizar la **transferencia electrónica** en un **banco** en **Italia**. La persona de Colombia (Antonio Rodríguez) les dice, que esas **no son las cuentas habituales**, que si confirman la información, a lo que contestaron que **Si**. Pasado unos días el Sr. **Antonio Ramírez** envía un correo preguntando que si recibieron la transferencia para seguir con el tramite, a lo que le contestaron que **si**. Que ya enviaron el pedido, que por favor les **transfieran el resto del dinero**. Lo cual le pareció raro, ya que nunca había sido así el tramite. Por tal razón **llamaron a la empresa en China** y les contestaron que **nunca habían enviado un correo** y que nadie en la empresa China les envió correo alguno.

(1. Cuales dispositivos?, 2. Que se debe pedir?, 3. A quien se debe pedir?, 4. Que autoridades?

ESTAFAS (5.240)

BEC (Bussiness Email Compromise)

- Identifique que Dispositivos están involucrados.
- Que se debe pedir para tener como evidencia e investigar.
- A quien se debe pedir?
- Que autoridades estarían involucradas?





ESTAFAS (5.240)

PSE (Pagos Seguros En línea)







ESTAFAS (5.240)

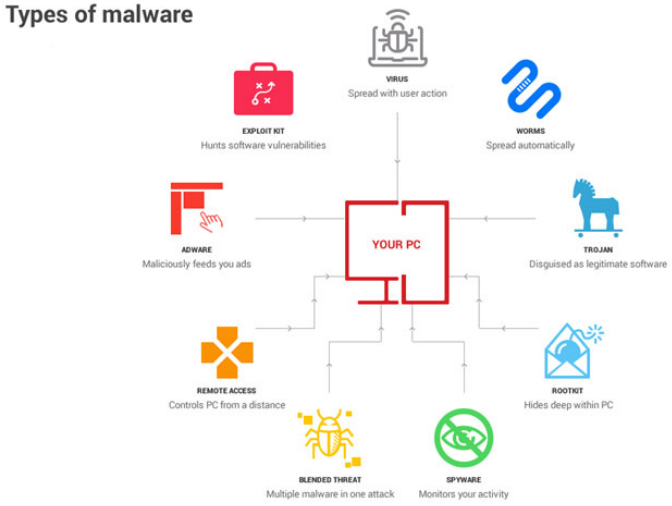
PSE (Pagos Seguros En línea)





ESTAFAS (5.240)

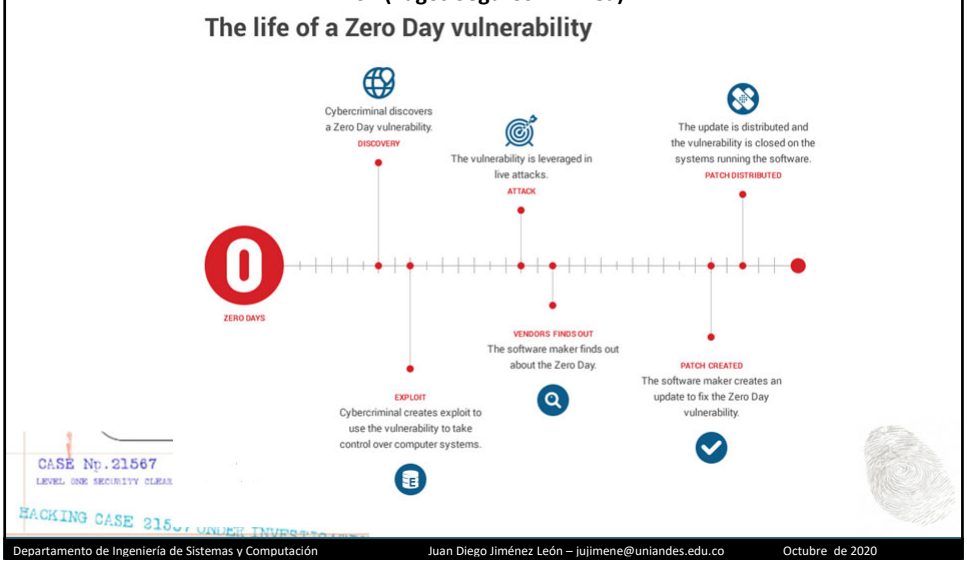
PSE (Pagos Seguros En línea)





ESTAFAS (5.240)

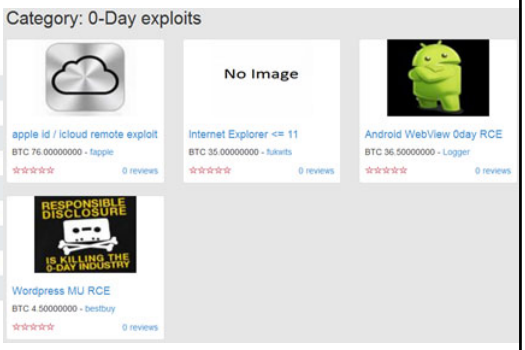
PSE (Pagos Seguros En línea)



ESTAFAS (5.240)

PSE (Pagos Seguros En línea)

ADOBE READER	$5,000-$30,000
MAC OSX	$20,000-$50,000
ANDROID	$30,000-$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000-$100,000
MICROSOFT WORD	$50,000-$100,000
WINDOWS	$60,000-$120,000
FIREFOX OR SAFARI	$60,000-$150,000
CHROME OR INTERNET EXPLORER	$80,000-$200,000
IOS	$100,000-$250,000







ESTAFAS (5.240)

PSE (Pagos Seguros En línea)

- **Caso ejemplo (trabajo en grupos de 2 o 3 personas)**

Jorge Andrade, llama asustado al banco Amazonas para preguntar que pasó con su cuenta, por que le llegaron varios mensaje con la confirmación de varios pagos a través de PSE. El total de los pagos es por valor de $18.000.0000.

El no entiende que ocurrió, dado que el solo utiliza como medio de pago su portátil personal, y no utiliza ningún otro medio. Y dice que el banco tiene la culpa.

1. **En este tipo de casos que evidencia se debe pedir?**
2. **Donde esta la evidencia?**
3. **A quien se le debe pedir la evidencia?**

SUPLANTACION DE IDENTIDAD (3.367)



- https://youtu.be/pMKJ471a3d8

SUPLANTACION DE IDENTIDAD (3.367)

- Actividad maliciosa en la que un atacante se hace pasar por otra persona por motivos como:
  - Cometer fraudes, contratar servicios, pedir prestamos, atacar a terceros (ciberacoso, sextorsion …).
  - La apropiación de derechos y facultades propias de la persona suplantada (por ejemplo acceder a cuentas y/o perfiles en Internet).



SUPLANTACION DE IDENTIDAD (3.367)

- **Caso ejemplo (trabajo en grupos de 2 o 3 personas)**

1. **En este tipo de delitos, que elementos tecnológicos pueden estar involucrados?**
2. **Que tipos de evidencia se pueden adquirir?**

PHISHING (2.893)

Phishing, conocido como **suplantación de identidad**, es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña, información detallada sobre tarjetas de crédito u otra información bancaria).

El cibercriminal, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas



PHISHING (2.893)



Estimado Cliente:

Le saludamos cordialmente y le agradecemos su confianza . En breve debera responder la siguiente solicitud y recibira un email de confirmacion.

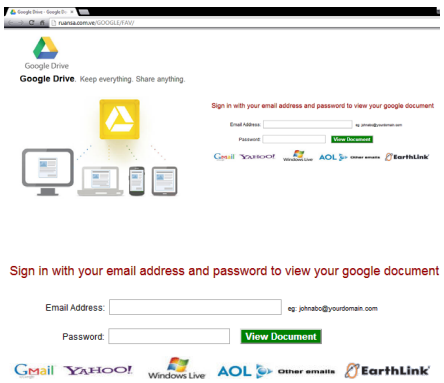
Como parte de nuestra seguridad en linea con regularidad son realizados Monitereos a la Actividad de nuestras Cuentas recientemente, nos hemos puesto en contacto con usted despues de notar accesos a su cuenta desde diferentes direcciones IP.

- Tenemos la incertidumbre de que su cuenta haya podido ser tomado por un tercero. debido a que la proteccion y seguridad de su cuenta correo por nuestra parte, hemos limitado el acceso en linea de modo temporal , esta medida es tomada con eventualidad en caso de proteccion y les levantado un Reporte del mismo. ID-223.038.076
- Para restablecer el monitereo de su cuenta y poder volver a accesar a ella con la continuidad de siempre solo sera necearío establecer conexion mediante este correo electronido que cuente con los Estandares de Seguridad marcados por nuestro banco estableciendo una Conexion Segura.

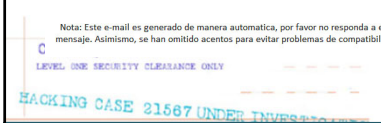
Los procedimientos de seguridad requieren que usted verifique la actividad en su cuenta antes del **30 de marzo del 2014.**

Atentamente
Éxito S.A.

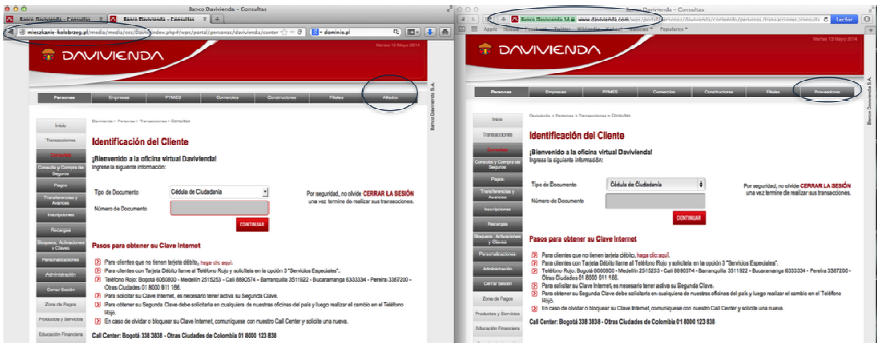
Nota: Este e-mail es generado de manera automatica, por favor no responda a este mensaje. Asimismo, se han omitido acentos para evitar problemas de compatibilidad.



Sign in with your email address and password to view your google document
Email Address:
Password:
View Document
Gmail YAHOO! Windows Live AOL Other emails EarthLink

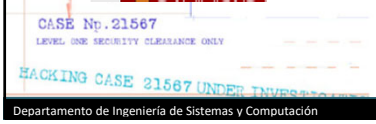


PHISHING (2.893)











PHISHING (2.893)

Campaña de phishing activa suplanta identidad de conocida marca de tarjetas de crédito

¡Alerta! En las últimas horas se detectó una campaña de phishing activa en Argentina que suplanta la identidad de una conocida marca de tarjetas de crédito y débito para robar las credenciales de acceso de las cuentas de los usuarios.

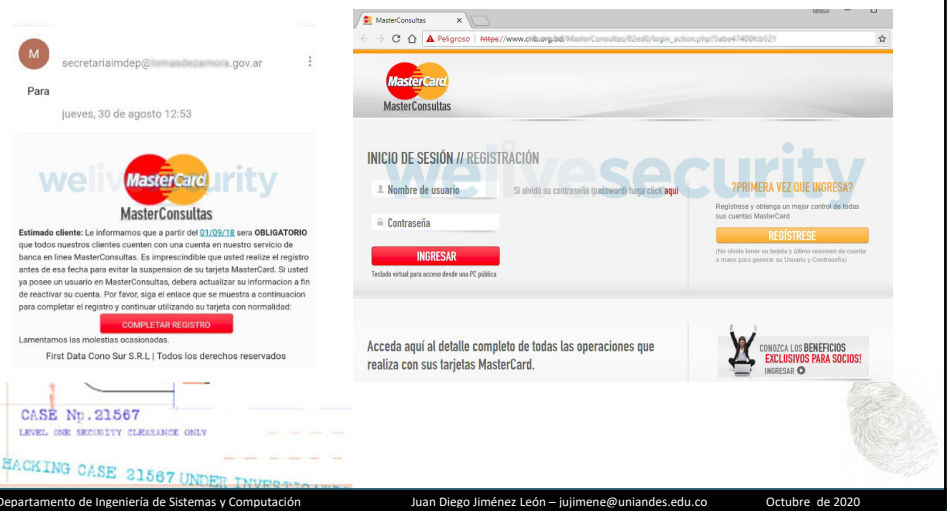


Lucas Paus 31 Aug 2018 - 02:12PM

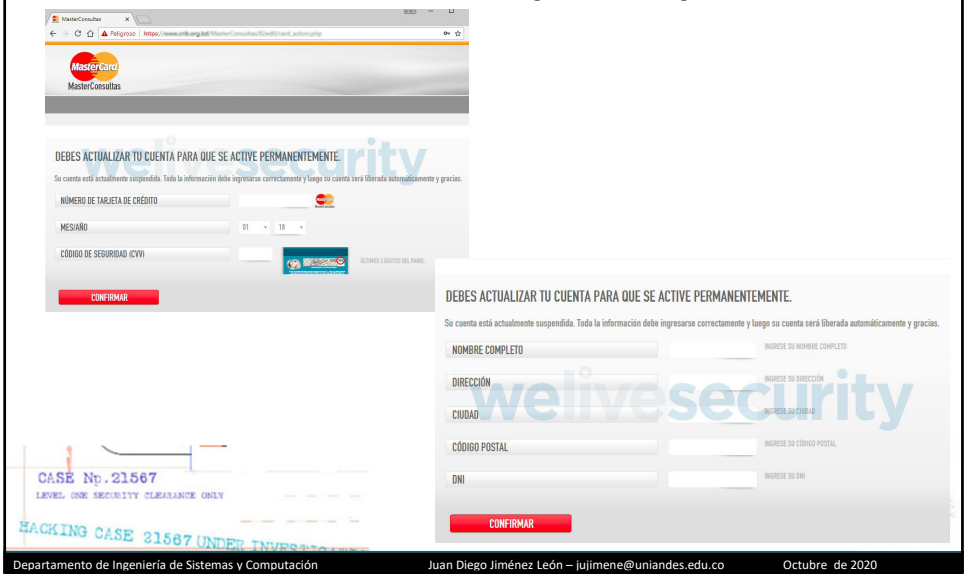




PHISHING (2.893)



PHISHING (2.893)



PHISHING (2.893)

Tipos de Phishing

- **Phishing engañoso**. Esta forma de phishing a menudo carece de personalización y se difunde sin centrarse en un objetivo concreto. El atacante espera que, si el volumen de mensajes es muy alto, acabará abriéndolos el número de usuarios suficiente para lograr su objetivo.

- **Spear-phishing.** A diferencia de los correos electrónicos de phishing normales, los de spear-phishing están muy personalizados. El objetivo final es el mismo, engañar al destinatario para que haga clic en un enlace URL o un archivo adjunto maliciosos; pero, en este caso, el mensaje contiene el nombre, la empresa o el cargo de la víctima, o se mencionan a sus compañeros de trabajo y contactos.





PHISHING (2.893)

Whale-phishing, fraude dirigido a directores ejecutivos o ataques de correos electrónicos de empresa (BEC). Este tipo de phishing se dirige al equipo ejecutivo de una empresa con el fin de recopilar las credenciales de inicio de sesión de una "ballena" ("whale"), es decir, un alto ejecutivo. Una vez robados estos datos, los ciberdelincuentes pueden suplantar su identidad, llevando a cabo lo que se conoce como fraude dirigido a directores ejecutivos a través de correos electrónicos de empresa (BEC), y autorizar transferencias bancarias u otras acciones de gran impacto.





PHISHING (2.893)

Está en: UN Periódico Digital /
Phishing: ¡me sacaron la plata del banco!

ECONOMÍA

AGOSTO 14 DE 2018 | BOGOTÁ D.C.

Phishing: ¡me sacaron la plata del banco!

LINA MARIA PATRICIA MANRIQUE VILLANUEVA | PERIODISTA UNIMEDIOS
lpmanriquev@unal.edu.co





PHISHING (2.893)

Un ejemplo de este tipo de estafa sería un correo electrónico de phishing de un "banco" que se envía a un gran número de personas, esperando que algunos de los destinatarios resulten ser clientes del banco suplantado.

El asunto del correo electrónico suele escribirse de manera que genere una sensación de urgencia; por ejemplo, "**Han robado su cuenta bancaria, actualice su contraseña inmediatamente**" o "**Factura vencida adjunta, páguela ahora para evitar acciones legales**". Como se ha descrito anteriormente, una vez que se hace clic en el enlace y se envía la información, o se abre el archivo adjunto, el daño ya está hecho.





PHISHING (2.893)

- **Caso ejemplo (trabajo en grupos de 2 o 3 personas)**

Un fraude comenzó con un correo electrónico proveniente de la cuenta informacion@bancolombia.com.co que eran enviados a las cuentas de correo de los usuarios de este banco en el que se le informaba a los clientes que por motivos de seguridad los servicios contratados por este habían sido suspendidos temporalmente y que para volver a hacer uso de estos canales virtuales debían hacer clic en un enlace proporcionado en el cuerpo del correo.

Una vez el cliente ingresaba a la página fraudulenta, se le solicitaba que ingresara los datos correspondientes al usuario, contraseña y preguntas de seguridad con el fin de obtener en una base de datos toda la información necesaria a la hora de realizar una transferencia de dinero. Para darles sensación de seguridad a los usuarios, los delincuentes diseñaron el teclado virtual que usa realmente el banco y hacían que, para ingresar la contraseña solo se pudiera por medio de este teclado virtual. Así, el cliente no sospechaba que estaba entregándoles información valiosa a personas sin escrúpulos.

Que se puede investigar en este tipo de casos? Que se necesita?

VISHING (2.035)

Es una práctica criminal fraudulenta en donde se hace uso del Protocolo Voz sobre IP (VoIP) y la ingeniería social para engañar a personas y obtener información delicada como puede ser información financiera o información útil para el robo de identidad.



VISHING (2.035)

- **¿Cómo se lleva a cabo el Vishing?**

A través de una voz computarizada, Luis recibió una llamada de su banco avisándole que "habían detectado" un cargo no reconocido a su tarjeta; que en ese momento efectuarían la cancelación de la compra y una bonificación por "x" cantidad. Para continuar con el proceso le pedían comunicarse a cierto número.

Al escuchar la grabación, que incluía avisos de privacidad, no sospechó. Lo atendió un supuesto ejecutivo diciendo que, "por políticas de seguridad", le mencionaría los primeros seis dígitos de su plástico y si eran correctos, él debía proporcionar los demás. **Luis fue víctima de Vishing**.





VISHING (2.035)

- Se efectuó con éxito el fraude siguiendo estos pasos:
  1. Generaron un mensaje pre-grabado a nombre del banco, el cual contenía un número que llevó a Luis a ponerse en contacto con el criminal.
  2. Esperaron a que Luis cayera en la trampa y compartiera los datos de sus plásticos.
  3. Ya con la información, usar la tarjeta de manera ilegal fue lo más sencillo.





VISHING (2.035)

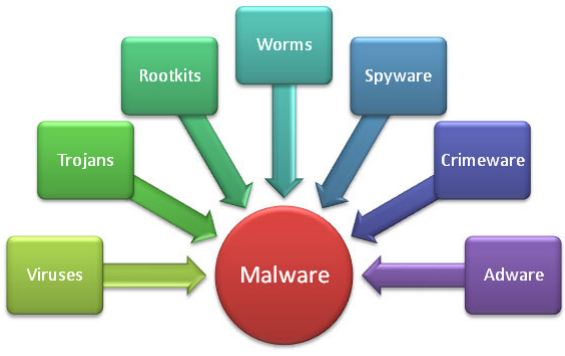
- **Caso ejemplo (trabajo en grupos de 2 o 3 personas)**

Tomando como ejemplo el caso anterior, conteste las siguientes preguntas:

1. **Que se necesita, para la investigación?**
2. **A que elementos se les puede hacer análisis forense?**
3. **Que se puede investigar en este tipo de casos?**

MALWARE (2.658)

"**Malware**" es una forma abreviada del término inglés "malicious software" (software malicioso) y hace referencia a virus, spyware, gusanos, etc. El **malware** está diseñado para causar daños a equipos independientes o conectados en red



MALWARE (2.658)

EL TIEMPO

Porno, culpable del 18% de los casos de infectados por 'malware' móvil

Los troyanos bancarios disfrazados de reproductores de video porno son muy utilizados.

Por: REDACCIÓN TECNÓSFERA | 07 de febrero 2018 , 02:37 p.m.

El contenido para adultos, sin lugar a dudas, es una de las puertas de entrada más atractivas para los programas maliciosos que acechan en la red.





MALWARE (2.658)

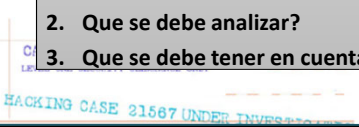
- **Caso ejemplo (trabajo en grupos de 2 o 3 personas)**

Una empresa sufrió un robo en la cuenta corriente de su banco por valor de $150.000.000. Lo primero que hizo la empresa fue llamar al banco a verificar que había pasado, y este le respondió que todas las transacciones realizadas fueron validas y se hicieron desde con el usuario que tienen asignado por el banco para realizar sus movimientos digitalmente, el banco dice que puede existir la posibilidad que su red o computadores estén infectados con un Malware. El computador habilitado para estos tramites esta en el área contable y no le tienen medidas de seguridad para su ingreso.

Ellos alegan que esa transacción no la hicieron, que van a realizar la respectiva denuncia.

Para la investigación en este tipo de casos:

1. **Que se debe solicitar?**
2. **Que se debe analizar?**
3. **Que se debe tener en cuenta para la investigación?**





Injuria y/o Calumnia a través de redes sociales (1.607)

Vanguardia.com — Colombia

Inicio Bucaramanga Santander Deportes Judicial Colombia Mundo Política Economía Opinión Entretenimiento Vanguardia TV

Martes 06 de Febrero de 2018 - 04:20 PM

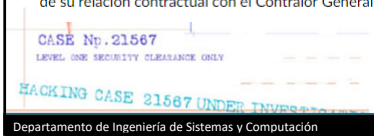
Usted tendrá que responder por la información que publique en redes sociales

Los usuarios de las redes sociales deberán responder por sus publicaciones, así como lo hacen los medios de comunicación y los periodistas. Corte Constitucional señaló que quienes cometan un delito en redes deberán asumir sus responsabilidades.

¿Qué fue lo que pasó?

El fallo de la Corte Constitucional se produjo luego de una acción de tutela interpuesta por la abogada antioqueña Carmen Olfidia Torres Sánchez, quien le atribuyó al concejal de Medellín Bernardo Alejandro Guerra Hoyos, la vulneración de sus derechos fundamentales a la honra, al buen nombre y a la intimidad.

Según la abogada, Guerra Hoyos difundió en su sitio web oficial y en su cuenta personal de Twitter "información falsa relacionada con el proceso penal al cual fue sometida en Estados Unidos en 2011, y de su relación contractual con el Contralor General de Antioquia Sergio Zuluaga Peña".





Injuria y/o Calumnia a través de redes sociales (1.607)

EL TIEMPO | ¿Quién castiga la injuria y la calumnia en internet?

Por: ANA MARÍA VELÁSQUEZ DURÁN | 29 de agosto 2017 , 08:42 a.m.

Una deuda con una compañera de trabajo llevó a que la reputación en internet y redes sociales de Claudia Ardila, de 27 años, quedara en el piso. Comentarios en los que la catalogaban de 'ladrona' y 'mentirosa' comenzaron a aparecer en grupos de Facebook y WhatsApp. "Se crearon perfiles falsos en los que enviaron mensajes que decían que estaba robando a mucha gente. Hay comentarios con groserías en los que me tratan de farsante", cuenta Ardila.

Esta campaña digital en su contra le ocasionó perjuicios personales y profesionales. "No tengo empleo y no puedo pedir una recomendación de mi otro trabajo. Las empresas, a veces, cuando hacen los procesos de selección, buscan en redes y encuentran comentarios", dice.

Sin embargo, de acuerdo con Ramírez, "**las personas piensan que la ley no las cobija y que por el hecho de estar en redes sociales hay una libertad de expresión que nadie regula**, pero hay pronunciamientos de la Corte Constitucional que señalan que la libertad de expresión no puede ir por encima de los derechos de los demás, es decir, el buen nombre, la honra o la presunción de inocencia". El experto agrega que "un trino con una manifestación en contra de alguien resulta ser más nocivo que algo dicho en otros medios, pues se va a replicar infinidad de veces y es más difícil frenarlo".



Injuria y/o Calumnia a través de redes sociales (1.607)

EL TIEMPO

TECNOLOGÍA | NOVEDADES APPS DISPOSITIVOS TUTORIALES VIDEOJUEGOS

'Publicaron mensajes insinuando que soy homosexual y no lo soy'

Le explicamos los mecanismos que debe tener en cuenta para defenderse en el mundo virtual.

Por: Camilo Peña Castañeda | 21 de junio 2018 , 09:57 a.m.

"Crearon un perfil falso con mi nombre en Facebook. Desde allí comenzaron a agregar a varios conocidos de la empresa en donde trabajaba. Luego, publicaron mensajes insinuando que soy homosexual y no lo soy". Este es el relato de Samuel*, quien con zozobra e incertidumbre dice que su reputación y su nombre han sido vulnerados en internet.





Injuria y/o Calumnia a través de redes sociales (1.607)

Facebook se encuentra en el primer lugar con el 50%.

Le sigue Instagram con el 25%.

Luego se ubica WhatsApp con el 20%.

Y en último lugar se encuentra Twitter con el 5%.



Fuente: CCP





Injuria y/o Calumnia a través de redes sociales (1.607)

NOTICIAS CARACOL

COLOMBIA 4:16 PM · 19 DE ABRIL DE 2018

En fallo inédito, ordenan a Facebook borrar perfil falso que tenía desesperado a alcalde colombiano

"Se creó un perfil falso denominado Jorge Rodríguez (Mesitas denuncia). **A través de este espacio de la red social comenzó toda serie de injurias y calumnias"**, así lo cuenta Carlos Núñez, alcalde de Mesitas del Colegio, quien fue favorecido por el tribunal.

Inicialmente, el mandatario llevó su caso a Facebook, pero la respuesta fue negativa.

Entonces lo llevó, vía tutela, al Tribunal de Cundinamarca, que amparó los derechos del alcalde y ordenó a Facebook retirar el perfil falso en 48 horas.





Injuria y/o Calumnia a través de redes sociales (1.607)

Ámbito Jurídico

¿Se pueden cobrar deudas a través de las redes sociales?

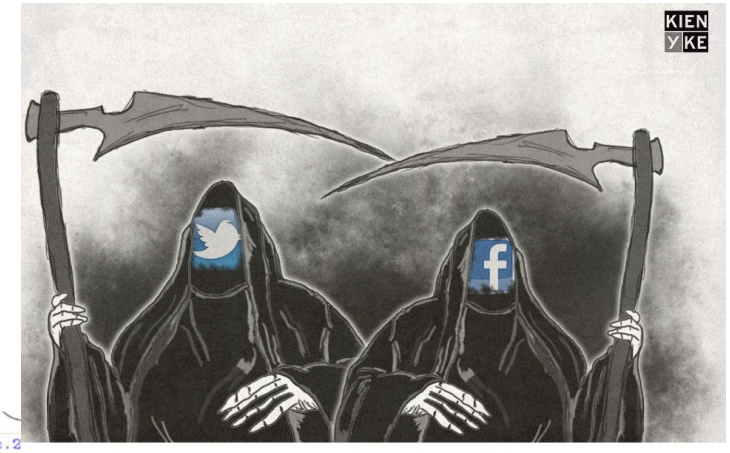
18 de Julio del 2018

Mi esposo no me pasa la cuota de alimentos hace más de tres años. Lo denuncié penalmente y en el juzgado de familia, pero igual no me ha dado dinero, además alardea en redes sociales de sus viajes y lujos. ¿Podría escribir públicamente en Facebook que no le da de comer a sus hijos, para ver si, por lo menos, le da vergüenza?

En Colombia, no se pueden cobrar obligaciones por redes sociales, así lo dejo claro la Sentencia T-050 del 2016, que dice: "El derecho a la propia imagen, a partir de los diversos aspectos desarrollados por la jurisprudencia constitucional, (i) comprende la necesidad de consentimiento para su utilización, (ii) constituye una garantía para la propia imagen como expresión directa de la individualidad e identidad de las personas, (iii) constituye una garantía de protección de raigambre constitucional para que las características externas que conforman las manifestaciones y expresiones externas de la individualidad corporal no puedan ser objeto de libre e injustificada disposición y manipulación de terceros, (iv) es un derecho autónomo que puede ser lesionado junto con los derechos a la intimidad, a la honra, al buen nombre de su titular, y cuyo ejercicio está estrechamente vinculado a la dignidad y libertad de la persona, (v) implica la garantía del manejo sobre la propia imagen cuyo ejercicio se traduce en una manifestación de la autodeterminación de las personas, y (vi) exige que las autorizaciones otorgadas para el uso de la propia imagen en el marco de la libertad en las relaciones contractuales no sean entendidas como una renuncia al derecho mismo".



Amenazas a través de redes sociales (1.203)



Amenazas de muerte en las redes sociales

3 de abril del 2018

Amenazas a través de redes sociales (1.203)

Álvaro Uribe, Gustavo Petro, Piedad Córdoba, Juan Manuel Santos, por nombrar algunos personajes de la política nacional; **James Rodríguez y Maluma**, del mundo deportivo y la farándula, también han sido víctimas de esta práctica virtual.

Mindefensa
@mindefensa

He ordenado a @PoliciaColombia investigar amenazas de muerte
que a través de redes ha recibido @matadoreltiempo. Hablaré con él personalmente. Quienes se esconden en un teléfono o computador para estorbar la libre expresión también deben recibir el peso de la ley: #LCVillegas

9:08 AM - Apr 3, 2018

307 221 people are talking about this

Sobre el caso de Matador, el ministro de Defensa, Luis Carlos Villegas, se pronunció y ordenó una investigación para hallar el origen de la amenaza. Finalmente, el Código Penal colombiano, en su artículo 347, permite condenar estas acciones: "El que por cualquier medio atemorice o amenace a una persona, familia, comunidad o institución, con el propósito de causar alarma, zozobra o terror en la población o en un sector de ella, incurrirá por esta sola conducta, en prisión de cuatro a ocho años", reza el artículo.

Caricaturista colombiano se retira de redes sociales por "amenazas de muerte"

03 de abril de 2018 - 12:04

Julio César González, conocido como Matador, aseguró en Twitter que ha recibido "amenazas de muerte" por parte de seguidores del "uribismo" y el Centro Democrático

Amenazas a través de redes sociales (1.203)

JUSTICIA | 5/28/2018 6:43:00 PM

Usuaria en redes sociales, en líos por trino amenazante contra Uribe

La mujer, que se identifica como @andreinalvt, fue denunciada por varios tuiteros. La Fiscalía le abrió indagación preliminar de oficio por instigación para delinquir agravado.



Amenazas a través de redes sociales (1.203)

Ibagué | 21.Enero.2018 | Por:

Exclusivo Econoticias: Macabro caso de amenazas a través de redes sociales a una microempresaria ibaguereña



Amenazas a través de redes sociales (1.203)



Otro de los aspectos más curiosos del caso es que al ingresar el número de whatsapp en la búsqueda de facebook, aparece un perfil misterioso en el cual aparentemente no se ha hecho ninguna publicación desde el momento en que fue creado; lo único que se logra observar es la imagen principal con la famosa máscara viral en redes sociales.

HACKING CASE 21567 UNDER INVESTIGATION

Amenazas a través de redes sociales (1.203)



JUDICIAL 27 Jul 2018 - 11:48 AM

Fiscalía identificó autores de amenazas contra periodistas en redes sociales

Néstor Humberto Martínez dijo que se irá "con toda contra esas expresiones antisociales".



POR: MAURICIO COLLAZOS
@CollazosMao

El fiscal general, **Néstor Humberto Martínez**, reveló que ya fueron identificados las personas que estuvieron detrás de las **amenazas a través de las redes sociales** contra varios periodistas, como es el caso del director de la FM, **Luis Carlos Vélez** y la columnista **María Jimena Duzán**.

Publicidad

CASE LEVEL ONE SECURITY CLEARANCE ONLY
HACKING CASE 21567 UNDER INVESTIGATION

Amenazas a través de redes sociales (1.203)

JUDICIAL

La Fiscalía General de la Nación no permitirá más amenazas en las redes sociales

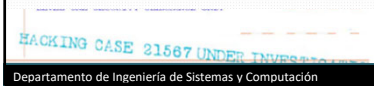
GUARDAR

Alejandro Valencia
Sábado, 28 de julio de 2018

Empresas como Facebook o Twitter colaboran con los objetivos del Fiscal Néstor Humberto Martínez

El fiscal general de la Nación Néstor Humberto Martínez compartido vía Twitter un comunicado en el que rechaza de forma contundente las amenazas que se han venido presentando por redes sociales a los periodistas y asegura que no va a permitir que se siga extendiendo esta tendencia.





Amenazas a través de redes sociales (1.203)

Las amenazas en redes sociales también dan cárcel

Abril 05, 2018 - 11:55 p.m. | *Por: Jessica Villamil Muñoz - reportera de El País*

"La gente sigue convencida de que lo que pasa en redes sociales no hace parte de la realidad". Así lo sostiene Amalia Toledo, coordinadora de proyectos de la Fundación Karisma, que trabaja en la promoción de los Derechos Humanos en el mundo digital.

Por eso, el exfiscal Élmer Montaña sostiene que el Artículo 347 el Código Nacional de Policía es claro frente al tema de las amenazas y "no importa si la amenaza es verbal o por Twitter".

"El que por cualquier medio atemorice o amenace a una persona, familia, comunidad o institución, con el propósito de causar alarma, zozobra o terror en la población o en un sector de ella, incurrirá por esta sola conducta en prisión de cuatro (4) a ocho (8) años y multa de trece punto treinta y tres (13.33) a ciento cincuenta (150) salarios mínimos legales mensuales vigentes".



Amenazas a través de redes sociales (1.203)

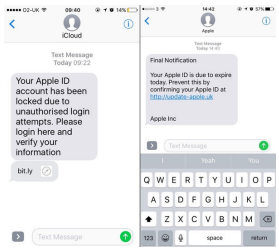
- **Caso ejemplo (trabajo en grupos de 2 o 3 personas)**

Que elementos se deben solicitar a las redes sociales, para determinar un autor o sugerir un posible investigado?

SMISHING (1.542)

El **smishing** (de **SMiShing**; a su vez, de SMS y fishing) es un nuevo tipo de delito o actividad criminal a base de técnicas de ingeniería social con mensajes de texto dirigidos a los usuarios de telefonía móvil. Se trata de una variante del phishing.

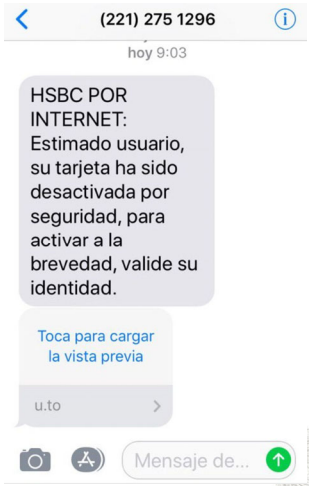
CARROYA.COM y RCN TV te felicitan por ser el feliz ganador de un MAZDA-6 comunicate ya INF:3172824971INF: 3196636413Cod-6625=5 GANASTE www.carroya.com



"Me llegó el mensaje de que me gané cinco millones de pesos. Como uno es todo ignorante, pues yo llamé, no le conté a nadie de mi familia porque les quería dar la sorpresa. Me pedían que llamara a un número de celular en donde me contestó un señor que me dijo que le hiciera dos recargas para que se pudiera hacer un estudio de mis datos y enviarme la plata. Yo como una boba caí y le hice dos recargas de 100.000 pesos. Según ellos me devolvían la plata. lo más grave es que me pidieron los datos para seguir el proceso, dirección, y cédula", cuenta Medina.

SMISHING (1.542)

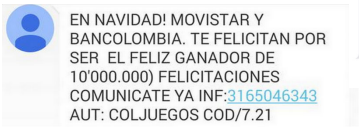




NO des clic en el enlace, te redirige a una página donde quieren ROBARTE los datos de tu tarjeta de crédito. ¡BÓRRALO DE INMEDIATO!



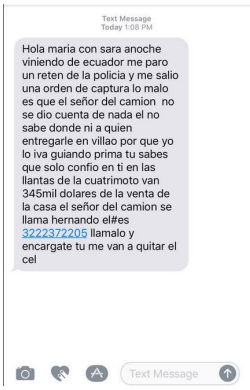
SMISHING (1.542)











Modalidad de #Estafa denominada #Smishing "TRASTEO MILLONARIO" evite responder ese tipo de mensajes.

SMISHING (1.542)

- **Caso ejemplo (trabajo en grupos de 2 o 3 personas)**

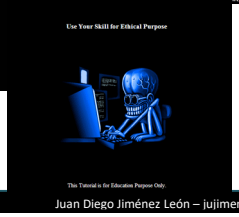
Que se deben solicitar, para realizar una investigación?

DEFACEMENT (1.062)

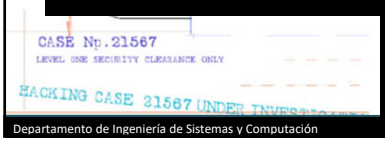
Es una palabra inglesa que significa desfiguración y es un término usado en informática para hacer referencia a la deformación o cambio producido de manera intencionada en una página web por un atacante que haya obtenido algún tipo de acceso a ella, bien por algún error de programación de la página, por algún bug en el propio servidor o por una mala administración de este.











DEFACEMENT (1.062)

Ola de ataques "defacement" en WordPress

By Tomás Sierra 7 febrero, 2017 Blog, Seguridad, WordPress 0 Comments

incibe-cert_ Alerta

Inicio / Alerta Temprana / Bitacora Ciberseguridad / Defacement y fuga de datos en la web Ticketfly

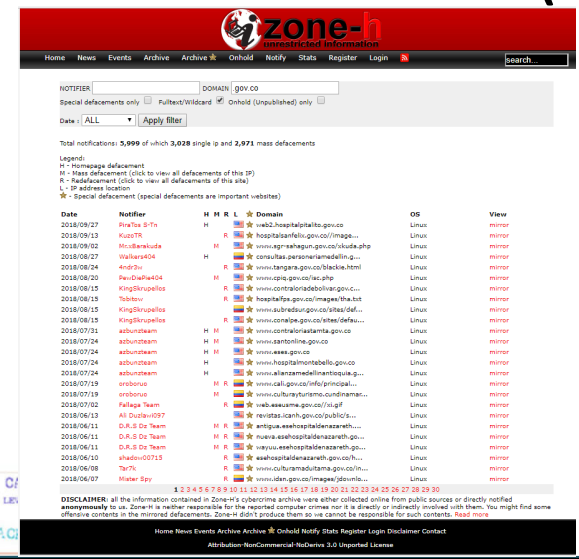
Defacement y fuga de datos en la web Ticketfly

31/05/2018





DEFACEMENT (1.062)



www.zone-h.org



DEFACEMENT (1.062)

- **Caso ejemplo (trabajo en grupos de 2 o 3 personas)**

Una universidad sufrió un Defacement a su pagina principal, y solicita una investigación, para determinar el posible autor del mismo.

Que se necesita solicitar para realizar la respectiva investigación?

SEXTORSION (1.034)

La **sextorsión** o **extorsión sexual** es una forma de explotación sexual en la cual una persona es chantajeada con una imagen o vídeo de sí misma desnuda o realizando actos sexuales que generalmente es compartida con fines de que se haga viral mediante sexting. La víctima es coaccionada para tener relaciones sexuales con alguien, entregar más imágenes eróticas o pornográficas, dinero o alguna otra contrapartida, bajo la amenaza de difundir las imágenes originales si no accede a las exigencias del chantajista





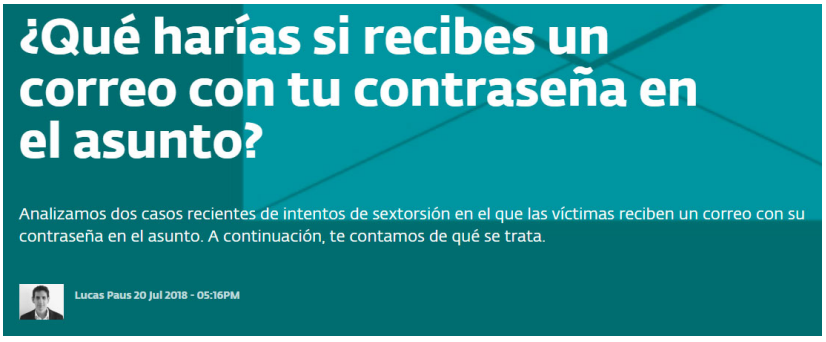
SEXTORSION (1.034)







SEXTORSION (1.034)





SEXTORSION (1.034)

Subject: *"Vayamos directo al grano. Sé que tu contraseña es ********. Más importante aún, sé tu secreto y tengo pruebas de ello. No me conoces personalmente y nadie me contrató para que te investigue."*

De: Terrence Tzu
Enviado: martes, 17 de julio 7:41 p. m.
Asunto: [redacted]
Para: [redacted]@hotmail.com

Nombre de la victima y su clave

It is just so unfortunate. I do know [redacted] is your password. More to the point, I am aware about your secret and I have evidence of your secret. You don't know me and no one employed me to investigate you.

It is just your hard luck that I found your misadventures. In fact, I setup a malware on the adult videos (porno) and you visited this web site to have fun (you know what I mean). While you were watching videos, your internet browser started out functioning as a Rdp (Remote control desktop) having a key logger which gave me accessibility to your display and also web camera. Right after that, my software program gathered your entire contacts from your messenger, fb, and email.

I then gave in much more time than I should've looking into your life and generated a two view video. First part shows the video you were watching and second part shows the video of your webcam (its you doing inappropriate things).

Honestly, I'm ready to forget details about you and allow you to move on with your daily life. And I will offer you 2 options which will make it happen. The above option is to either ignore this letter, or perhaps pay me $3200. Let us understand above 2 options in details.

Option 1 is to ignore this e mail. Let us see what is going to happen if you opt this option. I will certainly send your video recording to all of your contacts including relatives, co-workers, and so forth. It will not protect you from the humiliation you and your family will need to feel when family and friends uncover your unpleasant videos from me.

Second Option is to pay me $3200. We will name it my "privacy tip". Here is what happens if you pick this choice. Your secret remains your secret. I will delete the video immediately. You continue on with your lifetime that none of this ever happened.

CASE Np.21567
LEVEL ONE SECURITY CLEARANCE ONLY
HACKING CASE 21567 UNDER INVESTIGATION

SEXTORSION (1.034)

- **Que se debe obtener como evidencia?**
- **En que dispositivo se busca?**
- **Que se debe investigar?**

SEXTORSION (1.034)

Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames

Bitly: In May 2014, the link management company Bitly announced they'd suffered a data breach. The breach contained over 9.3 million unique email addresses, usernames and hashed passwords, most using SHA1 with a small number using bcrypt.

Compromised data: Email addresses, Passwords, Usernames

LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords

MySpace: In approximately 2008, MySpace suffered a data breach that exposed almost 360 million accounts. In May 2016 the data was offered up for sale on the "Real Deal" dark market website and included email addresses, usernames and SHA1 hashes of the first 10 characters of the password converted to lowercase and stored without a salt. The exact breach date is unknown, but analysis of the data suggests it was 8 years before being made public.

Compromised data: Email addresses, Passwords, Usernames

tumblr: In early 2013, tumblr suffered a data breach which resulted in the exposure of over 65 million accounts. The data was later put up for sale on a dark market website and included email addresses and passwords stored as salted SHA1 hashes.

Compromised data: Email addresses, Passwords

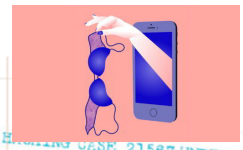
SEXTORSION (1.034)

No es una Sextorsion es un engaño o estafa.

SEXTING

El término "**sexting**" proviene de la unión de los términos ingleses "**sex**" y "**texting**" y se refiere al envío de contenidos eróticos o pornográficos por medio de teléfonos móviles.

El "sexting", supone el envío de imágenes estáticas (fotografías) o dinámicas (vídeos) de contenido sexual de mayor o menor carga erótica entre personas que voluntariamente consienten en ello y, que forma parte de su actividad sexual que se desarrolla de manera libre.



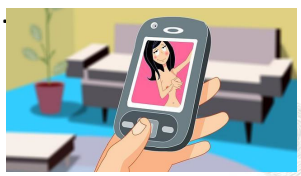
El principal riesgo que entraña el sexting es que una vez que el contenido es enviado, el remitente pierde el control del mismo.

SEXTING

Riesgos:

Se puede caer en **chantajes** (a éste se le conoce en específico como **sextorsión**) o también se pudiera caer en **ciber-acoso (cyber-bullying).** Ambos casos pudieran tener consecuencias graves.

El problema aquí es que este tipo de fotografías fueron tomadas o por la persona misma que aparece en la fotografía (selfie) o con su consentimiento, por lo que las acciones legales suelen complicarse, dependiendo de la jurisdicción.



SEXTING

EL TIEMPO | SUSCRIBIRME

BOGOTÁ

El 'sexting', una amenaza que se extiende por la ciudad

Entre el 2016 y lo que va del 2018, la Policía ha recibido 403 denuncias por 'sextorsión' en Bogotá.

Por: Óscar Murillo Mojica | 18 de febrero 2018 , 07:09 p.m.

Buena, bonita y bogotana (BBYB). Este es el sitio web con el que un hombre amenazó a su pareja, una joven universitaria. Si no continuaba su relación con él, **las fotos y videos íntimos que ella le había enviado en medio de la relación amorosa, iban a aparecer en esta página, que es de contenido sexual explícito.**

No contento con esta presión, el despechado joven incluso amenazó a la estudiante con llenar la universidad de fotos suyas completamente desnuda.





SEXTING







RANSOMWARE (779)

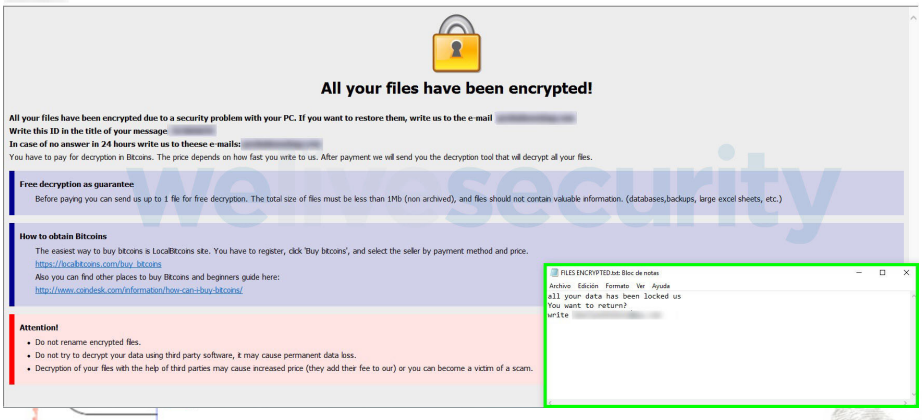
- El **ransomware** (también conocido como rogueware o scareware) restringe el acceso a su sistema y exige el pago de un rescate para eliminar la restricción. Los ataques más peligrosos los han causado **ransomware** como WannaCry, Petya, Cerber, Cryptolocker y Locky.



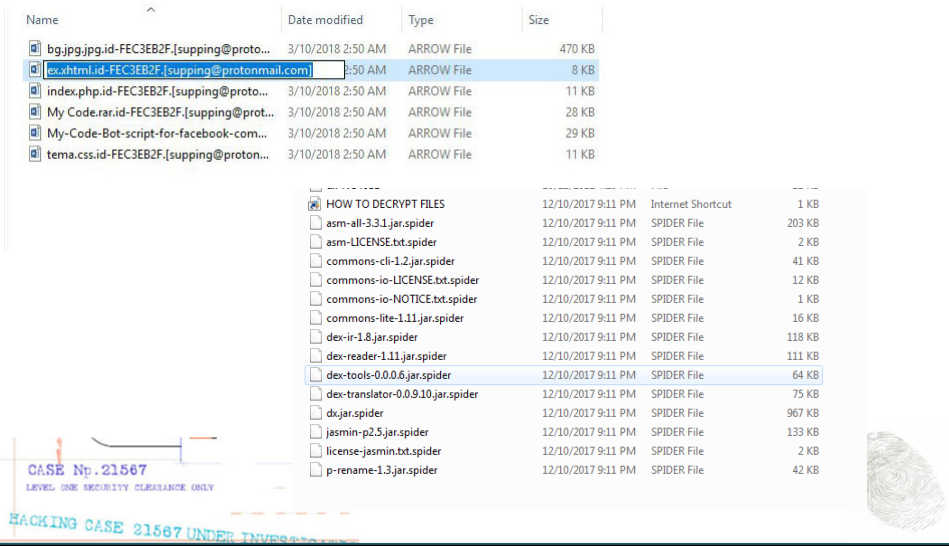
RANSOMWARE (779)



RANSOMWARE (779)



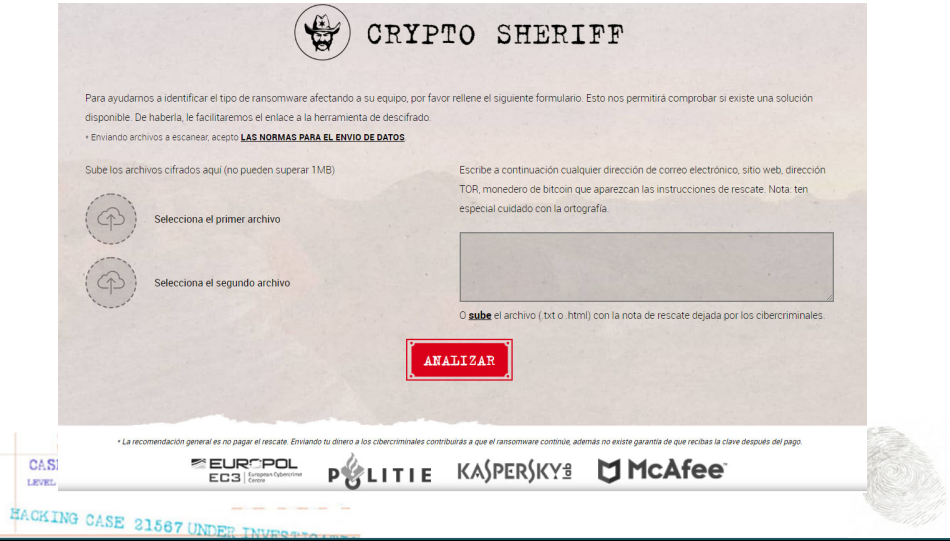
RANSOMWARE (779)

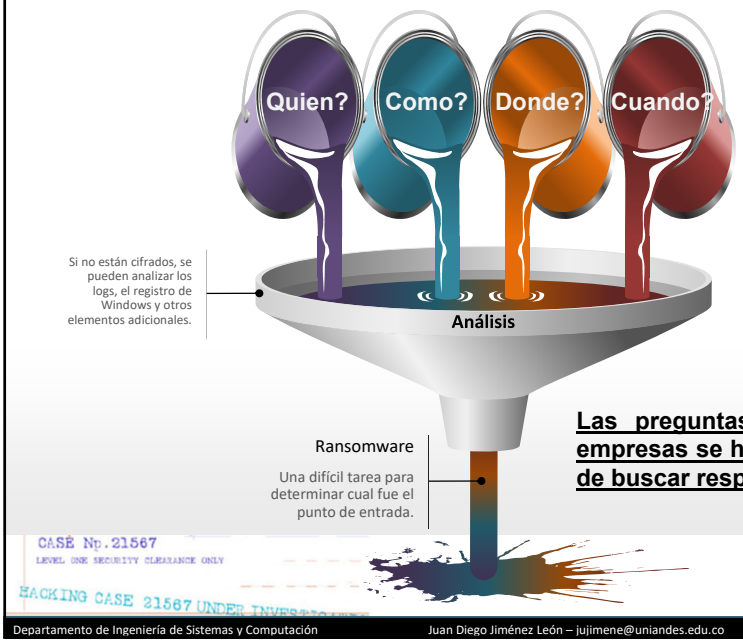


RANSOMWARE (779)



RANSOMWARE (779)





Las preguntas que todas las empresas se hacen al momento de buscar responsables

RANSOMWARE (779)

EL TIEMPO

NOVEDADES TECNOLOGÍA 24 DE JULIO DE 2018 , 05:11 P.M.

Colombia, entre países más afectados por caso de secuestro de archivos

¿Qué pueden hacer cibercriminales cuando ejecutan el ransomware Crysis? Esto es lo que debe saber.

EL TIEMPO

Ataques con malware suben a niveles récord en lo que va del 2018

Según informe, las campañas de ransomware volvieron a aumentar en el primer semestre de este año.



Dinero

CIBERCRIMEN | 5/16/2018 10:26:00 AM

Ataques de ransomware ahora le apuntan a los dispositivos móviles

Aunque el número de ataques de ransomware se redujeron en un 72% durante el 2017, la amenaza durante el 2018 le apunta a los dispositivos móviles y el internet de las cosas.

CARTA NIGERIANA (734)

- La **estafa nigeriana**, **timo nigeriano** o **timo 419** se lleva a cabo principalmente por correo electrónico no solicitado. Adquiere su nombre del número de artículo del código penal de Nigeria que viola, ya que buena parte de estas estafas provienen de ese país.
- Esta estafa consiste en ilusionar a la víctima con una fortuna inexistente y persuadirla para que pague una suma de dinero por adelantado, como condición para acceder a la supuesta fortuna. Las sumas solicitadas son bastante elevadas, pero insignificantes comparadas con la fortuna que las víctimas esperan recibir.



CENTRAL BANK OF NIGERIA



CARTA NIGERIANA (734)

CENTRAL BANK OF NIGERIA

Tipos comunes de timo nigeriano:

- **Animales regalados,** Se anuncian en páginas de venta y regalo de animales. Normalmente ofrecen alguna raza de animal especialmente valorada como por ejemplo "Regalo Yorkshire". Cuentan que tienen que mudarse y necesitan regalar sus perritos o cualquier otro animal. Cuando algún interesado contesta que acepta, dicen que hay que enviarles el dinero para que puedan enviar por avión desde allí el animal.

- **El capitán militar en Irak,** Contestan a los anuncios de venta de lo que sea (terrenos, casas...) solicitando información. Al obtener respuesta, envían un correo electrónico alegando ser militares que necesitan invertir un dinero que han obtenido del crudo, pero que como militares que son lo tienen que entregar a alguien en quien puedan confiar.



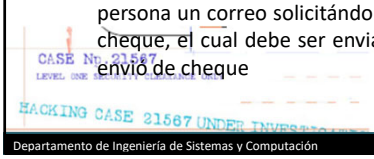


CARTA NIGERIANA (734)

CENTRAL BANK OF NIGERIA

- **La Tarjeta de Debito con 500 millones,** Los Estafadores encuentra a una víctima puede ser un doctor un ingeniero, y le proponen un negocio que ellos tienen una tarjeta de debito con una cantidad de 500 millones de dólares y que necesitan un punto de venta offline donde pasar esa tarjeta ellos le envían toda la documentación claves, correos y que dividirán el dinero a mitad. La persona buscara algún punto donde pasar la tarjeta y cuando realicen el intento siempre saldrá la operación fallida pero los dueños de la tarjeta dirán que si paso la tarjeta y que debe entregar la mitad del dinero o si no tiene que atenerse a las consecuencias.

- **La Lotería,** A la persona le llega un correo haciéndole saber que ha ganado un premio de Lotería, aun cuando no haya participado en sorteo alguno. Primeramente se le solicita a la persona sus datos personales. Luego llaman a la persona hablándole en idioma inglés -los timadores no suelen hablar castellano-, paso seguido le envían a la persona un correo solicitándole un importe por los gastos de transferencia del dinero o cheque, el cual debe ser enviado para que le puedan hacer la transferencia bancaria o envió de cheque



CARTA NIGERIANA (734)

- **El tío de América,** Los supuestos albaceas de un desconocido y adinerado pariente anuncian su fallecimiento y notifican al destinatario su inclusión entre los beneficiarios del testamento. En este caso a menudo se utilizan técnicas de ingeniería social, por ejemplo haciendo coincidir el apellido del difunto con el del destinatario.

- **El prisionero español,** Uno de los timadores, contacta con la víctima para explicarle que está en contacto con una persona muy famosa e influyente que está encerrada en una cárcel española.

- **La venta del teléfono móvil (celular) en eBay,** los timadores localizan a usuarios particulares de eBay que ofrezcan teléfonos móviles. Ofrecen una puja muy alta en el último momento, ganando así la subasta. Luego contactan al vendedor para explicarle que desean enviar el móvil a un supuesto hijo que trabaja como misionero en Nigeria, y que necesitan conocer la cuenta Paypal del vendedor para pagar



CENTRAL BANK OF NIGERIA

CARTA NIGERIANA (734)

- **La compensación,** El mensaje informa a la víctima de que el Estado nigeriano le compensará por haber sido víctima de la "Estafa Nigeriana", aunque la potencial víctima no lo haya sido. Las sumas ofrecidas van desde US$850.000 a US$1.000.000.
- **Compraventa de un vehículo por internet,** En este caso las víctimas son buscadas entre quienes tienen sus vehículos a la venta en internet. El vendedor recibe un email de un comprador, en un país diferente al del vendedor, interesado en el coche. El potencial comprador suele aceptar comprar el coche sin negociar el precio, ver el coche o probarlo.
- **El préstamo,** Consiste en que una persona brinda la facilidad para que cualquier persona pueda acceder a un préstamo fácilmente, sin garantías. Aprovechándose de la necesidad de la persona,





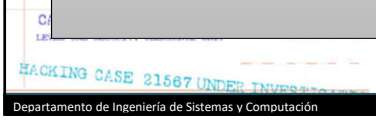
CENTRAL BANK OF NIGERIA

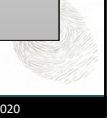


CARTA NIGERIANA (734)

- **Caso ejemplo (trabajo en grupos de 2 o 3 personas)**

- **Dentro de este tipo de ciberdelito, que elementos se deben investigar?**
- **Hay probabilidades de llevar una investigación a feliz termino?**





PORNOGRAFIA INFANTIL (676)



PORNOGRAFIA INFANTIL (676)

Pornografía Infantil leve o suave:

En este tipo de pornografía no hay actividad sexual explícita pero implica imágenes "seductoras e insinuantes" de niñas, niños o adolescentes. Incluye la exhibición de cuerpos desnudos de niñas, niños o adolescentes en distintas posturas eróticas, pero no su participación en actividades sexuales socioeróticas.

Pornografía Infantil dura o fuerte:

Consiste en la exhibición explícita de actividades sexuales socioeróticas penetrativas en las que participan niños, niñas o adolescentes.
El material se produce, se distribuye y puede ser comprado, compartido o utilizado por personas que recurren a este tipo de imágenes como recurso en actividades sexuales autoeróticas o socioeróticas.
También puede ser usado para seducir y enganchar a futuras víctimas de abuso sexual. Esas nuevas víctimas pueden ser otros niños, niñas y adolescentes a quienes se les hace ver lo que se representa en el material pornográfico como "normal" o "natural" para que más adelante estén dispuestos a participar en actividades sexuales similares y así utilizarlos para producir más material ilegal.

Tomado de: http://redpapaz.org/prasi/index.php/que-es/que-es-la-pornografia-infantil-2

PORNOGRAFIA INFANTIL (676)

Made for minds.

ACTUALIDAD MULTIMEDIA TV APRENDER ALEMÁN

MÉXICO DECIDE POLÍTICA ECONOMÍA CULTURA CIENCIA Y ECOLOGÍA ALEMANIA HOY

ACTUALIDAD / ALEMANIA HOY

SOCIEDAD

Darknet: el infierno de la pornografía infantil

El mayor servidor de material pornográfico del mundo estaba en Alemania. En Junio de 2017, se logró desactivarlo con el fisca Ungefuk, quien dijo a DW que "Darknet incita a cometer delitos".

ENTRETENIMIENTO INTERNET

Netflix acusado de pornografía infantil gracias a una película argentina

29 JUNIO 2018

Desearás al hombre de tu hermana sigue en Netflix.

El filme dirigido por **Diego Kaplan** arranca con una escena inocente entre dos mujeres muy jóvenes que pronto toma tintes sexuales; lo que ha detonado la denuncia de varios usuarios.

Colombia, tercer país que provee pornografía infantil al mundo

04/04/2018 | 5:22 pm

CASE Np.21567
LEVEL ONE SECURITY CLEARANCE ONLY
HACKING CASE 21567 UNDER INVESTIGATION

PORNOGRAFIA INFANTIL (676)

EL ESPECTADOR Martes 02 De Octubre

Noticias Opinión Economía Deportes Entretenimiento Vivir Cromos Tecnología Blogs Colombia

TECNOLOGÍA

OPINIÓN

¿En Colombia es punible la pornografía infantil virtual?

Tecnología 23 Mar 2018 - 6:22 PM
Por: Juliana Vargas / @Jvargasleal

En un fallo reciente, la Corte Suprema de Justicia definió lo que erar "actividades sexuales" en el contexto penal, levantando críticas a si paso. Pero el concepto de "actividad sexual" no es el único problem existe en relación con este delito, pues también se debe esclarecer q debe entender por "representaciones" de menores de edad.

La Corte provocó revuelo cuando decidió que, para que se cumpliera la tipificación de esta conducta punible, se requería que las imágenes correspondieran a conductas sexuales explícitas y estuvieran dirigidas a provocar la excitación sexual; es decir, la conducta sólo era punible cuando se encontrara dentro de un contexto lascivo. La exhibición de "los meros desnudos, las poses sugestivas y las imágenes de los genitales o de la región púbica" por sí solos no debían considerarse pornografía.

Semana

Martes, 2 de octubre de 2018 | Suscríbase | Newsletter

NACIÓN | OPINIÓN | ECONOMÍA | VIDA MODERNA | GENTE | CULTURA | MUNDO | TECNOLOGÍA | EDUCACIÓN | DEPORTES | SOSTENIBILIDAD | FOROS SEMANA | EDICIÓN IMPRESA

TENDENCIAS > HEROTUANGO DOSIS PERSONAL IVÁN MÁRQUEZ EPM IVÁN DUQUE ELN PREMIO NOBEL CARLOS MATTOS ARMANDO BENEDETTI VER MÁS

NACIÓN | 6/16/2018 7:38:00 PM

Así detectan a los consumidores de pornografía infantil en Colombia

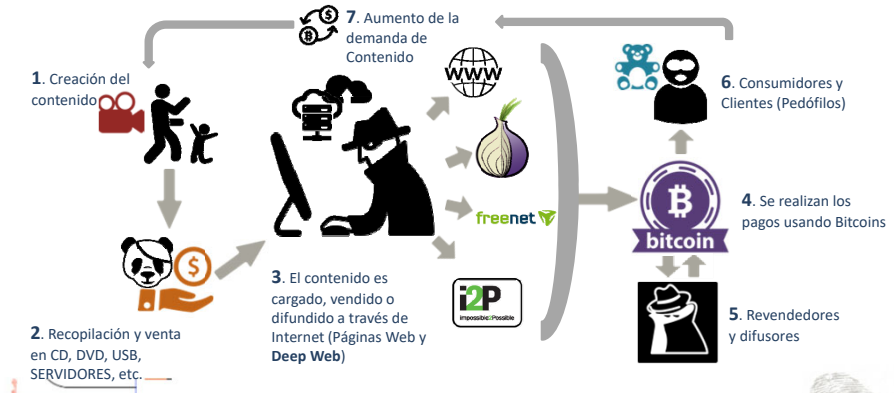
Luego de que una agencia de Estados Unidos generó una alerta por la carga de archivos de pederastia a internet, la Dijín capturó a 3 supuestos pedófilos en Bogotá y Bucaramanga.

La alarma sobre tres supuestos pedófilos colombianos llegó desde la Agencia de Inmigración y Aduanas de Estados Unidos, que tiene agentes dedicados a combatir los delitos contra los niños. Ellos detectaron que desde el país se habían cargado a internet 287 archivos, imágenes y videos, de contenido sexual explícito de niños.

CASE Np
LEVEL ONE SECURITY CLEARANCE ONLY
HACKING CASE 21567 UNDER INVESTIGATION

PORNOGRAFIA INFANTIL (676)

MATERIAL DE ABUSO SEXUAL DE NIÑAS, NIÑOS Y ADOLESCENTES



PORNOGRAFIA INFANTIL (676)

- **Caso ejemplo (trabajo en grupos de 2 o 3 personas)**

Teniendo en cuenta todos los elementos posibles que puedan estar involucrados en este tipo de casos, determine que acciones se deben realizar para lograr identificar e incriminar a este tipo de personas.

CYBERBULLING (852)

MUNDO

El suicidio de una niña modelo por ciberbullying conmociona a Australia

Amy "Dolly" Everett tenía 14 años y era el rostro de una célebre marca de sombreros. Su familia hizo un llamado para que los padres dialoguen con sus hijos sobre sus relaciones y el acoso: "Hablen, aunque les tiemble la voz"

EL FRENTE.com.co

Inicio | Colombia | Política | Justicia | Opinión | Metro | Santander | Economía | Mundo

Mundo - Noticias

El Cyberbullying provocó suicidio de una niña en Chile

Tweet | Me gusta 0 | Compartir



Las relaciones virtuales son la moneda social que necesitamos hoy para sobrevivir. Lo asegura Pavle Zagorscak experto en *ciberbullying* e investigador de la Universidad Libre de Berlín.



CYBERBULLING (852)

EL TIEMPO | **Cyberbullying, ¿Qué es y por qué es tan preocupante?**

Por: Linda Patiño | 02 de mayo 2018 , 04:20 p.m.

El ciberacoso se trata de un fenómeno social que puede afectar a cualquier persona, en su colegio, en su trabajo o de forma aleatoria. **Su misión es atemorizar, dañar y reducir al otro y se vale de las nuevas tecnologías** para lograrlo.

La diferencia con el matoneo tradicional es que con internet lo que antes era un humillación frente a un salón hoy puede convertirse en la burla de moda para millones de personas en el mundo. Según los expertos, **la posibilidad de hacerse viral y el anonimato de los agresores son los elementos que marcan la diferencia y causan más daños**.



Las relaciones virtuales son la moneda social que necesitamos hoy para sobrevivir. Lo asegura Pavle Zagorscak experto en *ciberbullying* e investigador de la Universidad Libre de Berlín.



CYBERBULLING (852)

- **Caso ejemplo (trabajo en grupos de 2 o 3 personas)**

Teniendo una denuncia de unos padres, que dicen que su hijo esta siendo acosado por un grupo de compañeros, a través de redes sociales, correos electrónicos y celular.

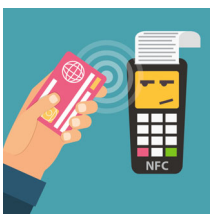
Que tipo de evidencia puede ser aportada en este tipo de casos?

SKIMMING (406)

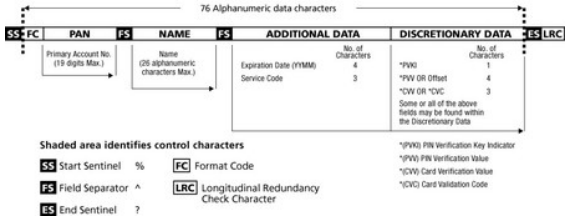
El skimming o clonación es una modalidad delictiva que se utiliza para **copiar la información contenida en la banda magnética** de tarjetas de cajero automático, débito o crédito. Puede ocurrir en el momento de uso del ATM o bien cuando se pasa la tarjeta por un POS en un comercio.

En las tarjetas que utilizan PIN, los delincuentes ejecutan otros métodos para conocerlo; en ocasiones instalan pequeñas cámaras de vídeo o simplemente espían por encima del hombro del cliente. Una vez obtenida la información, elaboran una tarjeta idéntica a la original operando ilegítimamente sobre las cuentas o el crédito de la víctima





SKIMMING (406)



Es en la primera pista donde se concentra **toda la información que un skimmer ansía**. Los primeros caracteres son los que contienen el número de la tarjeta. Tras un primer separador se encuentra el nombre completo del titular de la misma y de seguido se encuentra la fecha de caducidad y el último dato relevante para hacer compras por internet con cualquier tarjeta, código de seguridad o CVV.

CASE N.21567
LEVEL ONE SECURITY CLEARANCE ONLY
HACKING CASE 21567 UNDER INVESTIGATION

SKIMMING (406)



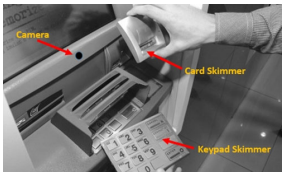






Figure 13: This figure shows the 10 real skimmers provided to us from the NYPD. The Skim Reaper successfully detected all of these skimmers.

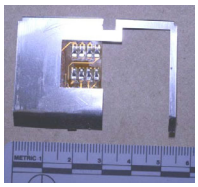
HACKING CASE 21567 UNDER INVESTIGATION

SKIMMING (406)



SKIMMING (406)









SKIMMING (406)

- **Caso ejemplo (trabajo en grupos de 2 o 3 personas)**

Al parecer a través de un malware o algún tipo de modificación de software instalado en algunos datafonos de un banco, están robando los datos de tarjetas.

- **Que es necesario realizar en este tipo de casos?**
- **Es skimming?**

GROOMING

- El grooming se puede definir como «el **ciberacoso** ejercido deliberadamente por un **adulto** para establecer una **relación y un control emocional** sobre un **menor** con el fin de preparar el terreno para su **abuso sexual**».
- Supone el **conjunto de técnicas de engaño y persuasión** que utiliza un adulto para ganarse la confianza y disminuir las inhibiciones del menor y obtener de él un beneficio de índole sexual, que es la finalidad que persigue (grooming es una palabra inglesa que significa "engatusamiento").



GROOMING

Existen dos variantes:

1. Casos de grooming en los que **no existe una fase previa de relación y generación de confianza**: En este caso el acosador logra el material (fotos y videos con contenido sexual) mediante la obtención de contraseñas o hackeo de cuentas, o de las fotos que los jóvenes han subido en determinados lugares de Internet. Con este material sexual comienza el chantaje y la extorsión, amenazando con divulgar dicho material si la víctima no le facilita más material o accede a un encuentro.



GROOMING

2. Casos en los que el acosador establece una **fase previa donde busca la confianza del menor** para que le entregue material. En este caso, el material es entregado por el menor y la confianza se vuelve el instrumento indispensable utilizado por el groomer.



GROOMING

Grooming, una amenaza cada vez mayor para los menores en Colombia

Recomendado del editor | 21 Feb 2018 - 09:35 Am

Quien usaba a su propia hija

Este ingeniero industrial de 40 años fue capturado por las autoridades en el barrio Ciudad Jardín (Cali) a comienzos de marzo. Su principal característica consistió en crear un perfil falso en Facebook, en el cual utilizaba el nombre y las fotografías de su propia hija de 11 años.

Gracias a esta página ganaba la confianza de niñas de edades similares a quienes, a través de engaños, les pedía fotografías desnudas o en ropa interior. Una vez recibía las imágenes, amenazaba a sus víctimas con publicarlas a menos que se encontraran personalmente con él en algún lugar público de la ciudad.

El hombre las obligaba a ir a moteles de Cali, donde ingresaba en un automóvil de vidrios polarizados, con el cual impedía que los empleados de esos establecimientos pudieran percatarse de la edad de sus acompañantes. Al momento de su arresto, tenía dos computadores, dos discos duros y varias memorias USB con material pornográfico.

Las víctimas de este sujeto pertenecían a 10 colegios de las ciudades de Cali y Yumbo. La captura se produjo gracias a la denuncia de la madre de una de sus víctimas, quien se percató de la situación y acudió a las autoridades.





GROOMING

El imitador de cantantes

Este hombre de 23 años –sin identificar aún por parte de las autoridades– contaba con dos perfiles falsos en Facebook, a nombre del cantante Maluma. A través de estas presencias en línea se ganaba la confianza de niñas de entre 9 y 12 años, a quienes pedía fotografías y videos en que aparecieran desnudas o en ropa interior.

Una vez las menores de edad le enviaban el material que él solicitaba, las amenazaba con publicar las imágenes o enviárselas a sus padres a menos que accedieran a sostener relaciones sexuales con él.

En el momento de la captura, la Policía realizó la incautación de 15 discos duros, 5 tabletas, 9 celulares, 15 memorias micro SD y 2 memorias USB, que utilizaba para almacenar y distribuir las imágenes.

La captura se realizó gracias a la denuncia de una madre de una menor que fue víctima del delincuente. El capturado se encuentra a disposición de la Fiscalía, que le dictó medida de aseguramiento en una prisión. Afronta una pena de entre 10 y 20 años por el delito de pornografía infantil.





GROOMING

- **Caso ejemplo (trabajo en grupos de 2 o 3 personas)**

Un delincuente con dos perfiles falsos

Periodista de 27 años de edad. Entre los años 2011 y 2015, utilizó dos perfiles falsos de Facebook, en los cuales se presentaba como una mujer llamada *Juliana Salazar*, para contactar a estudiantes de colegios de estratos altos, de entre 13 y 16 años. Después de ganar su confianza les pedía fotos en las que estuvieran desnudos o en diferentes poses sugestivas.

Luego, a través de otro perfil falso a nombre de *Andrés Monsalve*, extorsionaba para no revelar estas fotografías y videos. En estos casos, les pedía más imágenes o que accedieran a encontrarse con él. Las autoridades estiman que cerca de 150 niños habrían sido víctimas de esta persona.

Uno de los padres de las víctimas denunció ante las directivas del colegio está situación, lo que motivó la presentación de una denuncia ante la Fiscalía General. El ente investigador contactó a expertos en delitos informáticos de la Policía Nacional.

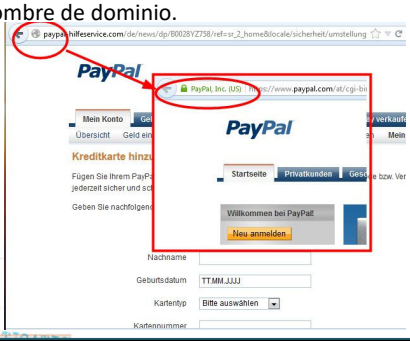
El acusado se encuentra en libertad condicional, pues pasaron los 60 días establecidos por la Ley para el inicio del juicio, desde la presentación del escrito de acusación.

Sin conocer el desenlace final del tema, desde el punto de vista de la evidencia a recolectar, que elementos sugiere se pueden recolectar en este tipo de casos y que se debe solicitar a las redes sociales?

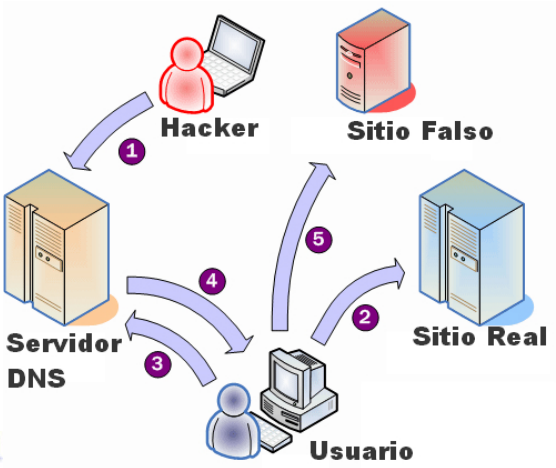
PHARMING

Pharming es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta.

Un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio.



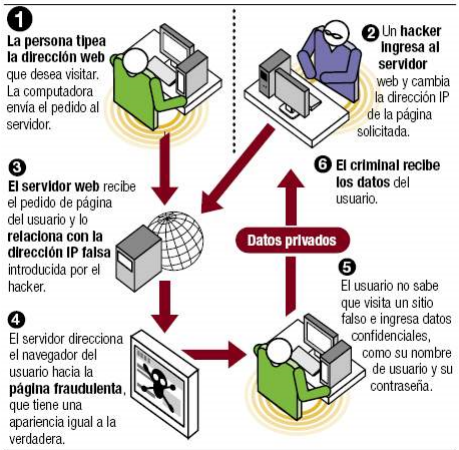
PHARMING



PHARMING

¿Qué es el pharming?

Es una modalidad delictiva que consiste en la apropiación de información valiosa y confidencial de una persona a través de páginas de Internet falsas.



Fuente: Divindat PNP EL COMERCIO

Acceso Abusivo a Sistema informático

EL TIEMPO

Hacker mejoró notas de los estudiantes de la Universidad del Tolima

Tras el ataque informático, las calificaciones de los 18.000 estudiantes eran la más alta.

Por: Ibagué | 01 de febrero 2018 , 05:26 p.m.

De acuerdo con la Universidad del Tolima, durante la temporada de vacaciones, un hacker modificó las notas de todos los alumnos, el histórico de calificaciones, promedio semestral y hasta los datos de los estudiantes egresados.

“Al verificar la plataforma vimos que las calificaciones de los 18.000 estudiantes, en las modalidades presencial y distancia, estaban en cinco”





PORNOVENGANZA

EL TIEMPO

'El día que mis fotos íntimas llegaron a internet'

En lo corrido de este año se han interpuesto 110 denuncias por casos de imágenes sexuales en la red.

Por: Ana María Velásquez Durán | 08 de agosto 2017 , 10:50 a.m.

Después de unos meses de relación, Nikki Rettelle, una mujer estadounidense de 35 años, descubrió que su novio había violado su privacidad de la manera más absoluta: instaló cámaras en su casa para grabarla a escondidas y tenía decenas de tarjetas de memoria con fotos y videos de ella viendo televisión, descansando y, a menudo, desnuda.

Aunque se alejó, meses después se enteró de que su expareja creó perfiles falsos de ella en redes sociales, diseñó dos sitios web dedicados exclusivamente a alojar los contenidos más íntimos, envió correos y mensajes con esas imágenes a su familia y amigos, hackeó su computador, sobrepuso su rostro a fotos de cuerpos desnudos y acompañó todo con su información personal: nombre completo, lugar de trabajo, correo y dirección.

Nikki fue víctima de un flagelo que, aunque es conocido como 'porno de venganza' alude en realidad a la distribución de imágenes sexuales de una persona sin su consentimiento. Numerosas voces han alegado que el uso de la expresión 'porno' abre huecos legales en jurisdicciones en las que la pornografía es legal. A su vez, 'venganza' sugiere una retaliación y desplaza la culpa, al menos en parte, hacia la víctima.

Ya sea que se hayan empleado cámaras ocultas o hackeado teléfonos o cuentas de correo, o que se trate de imágenes capturadas consensualmente en el contexto de una relación íntima, la Organización de Derechos Civiles Cibernéticos (CCRI por sus siglas en inglés) considera que se trata de una conducta delictiva. En otras palabras, **el consentimiento a la hora de 'hacer' las imágenes no cuenta, si no se consintió su publicación.**

Johana Rodríguez, una joven bogotana de 26 años que en 2011 fue víctima de este flagelo, creó una página en esta red social llamada 'Ayúdanos a Detener el Porno Vengativo'.

Rodríguez tuvo ver en internet contenido íntimo que había hecho con quien entonces era su novio. "La que era mi mejor amiga hackeó mi correo, descargó esos contenidos íntimos y se los envió a todos mis contactos masculinos. Después los publicó en la red para que se hicieran virales. Hoy en día todavía hay gente que me envía el video por Facebook, muchos lo guardaron en su computador", añade.

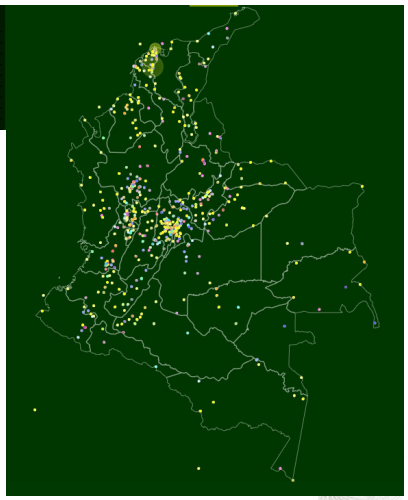


Denuncias Enero 1 – Octubre 2 2018

Modalidad	
Ranking	Modalidad
1193	Malware
1004	Estafa por compra ...
954	Suplantación de Id...
709	Phishing
707	Vishing
400	Smishing
346	Amenazas a través...
290	Ransomware
224	Sextorsión

Delito	
Ranking	Delito
2274	Artículo 246 – Estafa
1506	Artículo 269 E - Uso d...
842	Artículo 269 F - Violac...
418	Artículo 269 G - Supla...
313	Artículo 220 – Injuria
262	Artículo 347 – Amena...
259	Artículo 218 - Pornogr...
200	Artículo 244 - Extorsión
199	Artículo 269 I - Hurto ...

Sector		
Ranking	Sector	Color
1282	Financiero	
437	Industrial	
426	Educación	
424	Gobierno	
280	Menor de edad	
224	Medios de co...	
185	Tecnología	
22	Salud	



Artículo 269A. Acceso abusivo a un sistema informático
Artículo 269B. Obstaculización ilegítima de sistema informático
Artículo 269C. Interceptación de datos informáticos
Artículo 269D. Daño Informático
Artículo 269E. Uso de software malicioso
Artículo 269F. Violación de datos personales
Artículo 269G. Suplantación de sitios web para capturar datos personales
Artículo 269I. Hurto por medios informáticos y semejantes
Artículo 269J. Transferencia no consentida de activos



https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real/historico

CYBERCRIME PRICE LIST

ATTACK TOOLS

MALWARE	$200	REMOTE ACCESS TROJAN
	$50	PASSWORD STEALER
RANSOMWARE	$200	SOPHISTICATED LICENSE FOR WIDESPREAD ATTACKS
	$50	UNSOPHISTICATED LICENSE FOR TARGETED ATTACKS
	$1	PC MALWARE INSTALLATION
	$400	1 MILLION MALICIOUS SPAM
SOFTWARE	$100	REMOTE DESKTOP CONTROL TOOL
	$700	DISTRIBUTED DENIAL OF SERVICE ATTACK SOFTWARE
PAYMENT AND LOG-IN INFO	$5	CREDIT/DEBIT CARD FOR ONLINE USE
	$10	CREDIT/DEBIT CARD INFO THAT CAN BE CLONED ON PLASTIC
	$5	BANK ACCOUNT LOG-IN (USERNAME AND PASSWORD)
	$25	BANK ACCOUNT LOG-IN WITH ACCESS TO EMAIL, SECURITY ANSWERS, ETC.
	$1	EXISTING PAYPAL ACCOUNT

DATA

PERSONAL INFORMATION	$3	SOCIAL SECURITY AND DATE OF BIRTH VERIFICATION
	$150	CREDIT REPORT 750+ CREDIT SCORE
DATABASE RECORDS	$25	1 MILLION COMPROMISED EMAIL/PASSWORDS

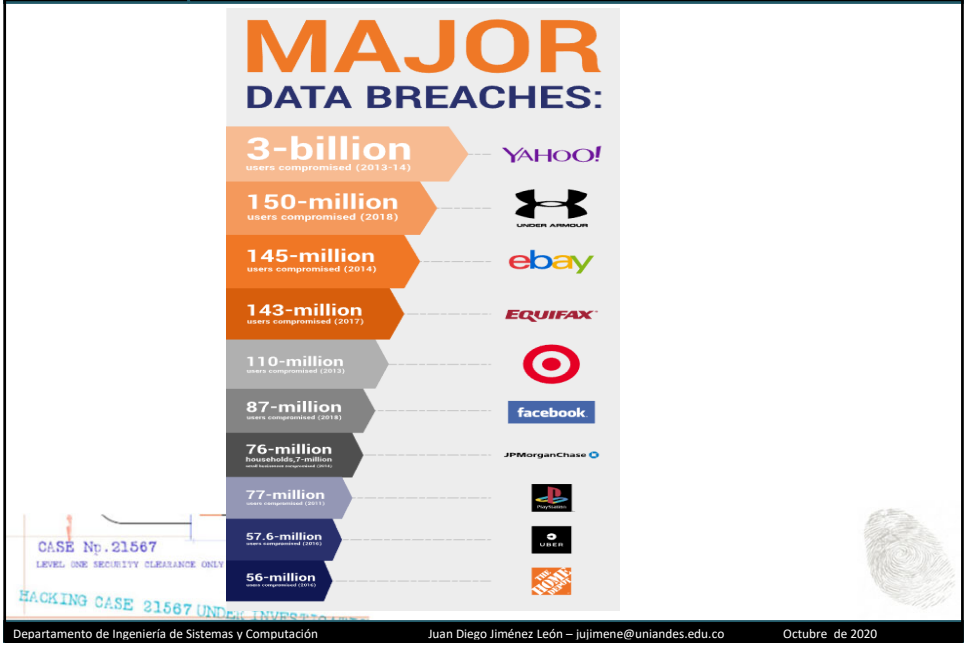


SERVICES	HACKING	$100	EMAIL ACCOUNT
		$100	SOCIAL MEDIA ACCOUNT
		$300	CMS WEBSITE (WORDPRESS, ETC.)
	USER OBFUSCATION	$150	BULLETPROOF HOSTING IN LAX JURISDICTION (CHINA, EASTERN EUROPE, ETC.)
		$20	VIRTUAL PRIVATE NETWORK (VPN)
	MALWARE	$1	PC MALWARE INSTALLATION
		$25	MALICIOUS FILE ENCRYPTION
	SPAM	$20	500 SMS (FLOODING)
		$400	1 MILLION MALICIOUS SPAM
		$20	500 PHONE CALLS (FLOODING)
		$200	1 MILLION EMAIL SPAM (LEGAL)
	FAKE DOCUMENTS	$25	DIGITAL COPY OF FAKE CREDIT/DEBIT CARD
		$25	DIGITAL COPY OF FAKE DRIVER'S LICENSE OR PASSPORT
		$15	DIGITAL COPY OF FAKE UTILITY BILL OR SOCIAL SECURITY CARD

CASE Np.21567
LEVEL ONE SECURITY CLEARANCE ONLY
HACKING CASE 21567 UNDER INVESTIGATION



CASE Np.2
HACKING CASE 21567 UNDER INVESTIGATION



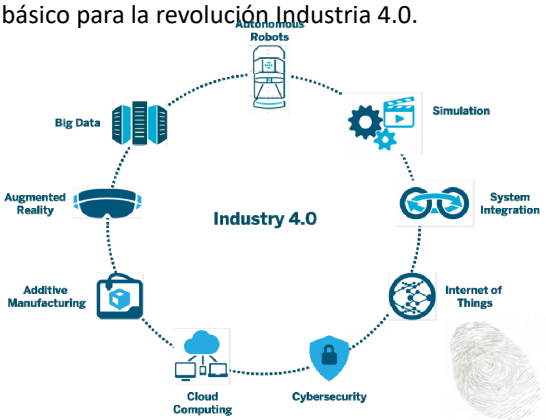
Temas

- ~~Tendencias Tecnológicas~~
- ~~Retos~~
- ~~Balance del Cibercrimen 2018~~
- ~~Ciberdelitos~~
- **Paradigmas Futuros**

IoT y CPS (Cyber-Physical System)

Las implementaciones de **IoT** y **CPS** están ganando especial atención por parte de los ciberdelincuentes. Además de su creciente uso para el ocio y la domótica, el IoT es un elemento básico para la revolución Industria 4.0.

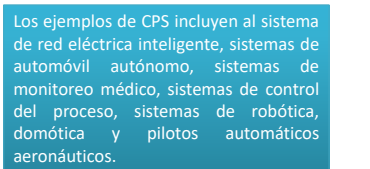
Un sistema cyber-físico (en inglés, cyber-physical system, abreviadamente CPS) es un mecanismo (sistema físico) controlado o monitoreado por algoritmos basados en computación y estrechamente integrados con internet.

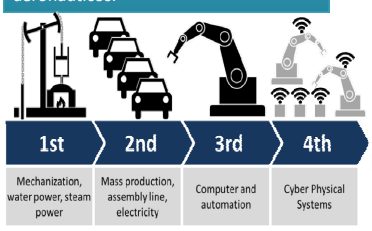




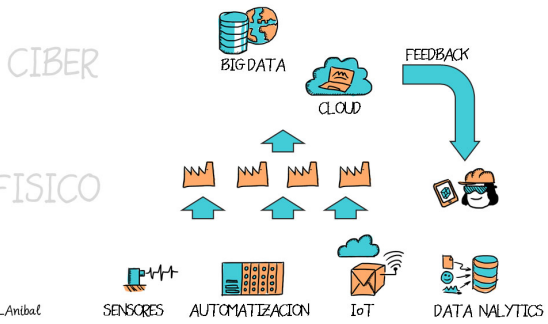
CPS (Cyber-Physical System)

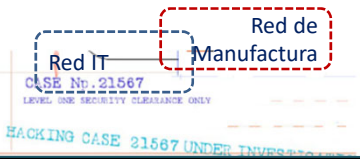
Los ejemplos de CPS incluyen al sistema de red eléctrica inteligente, sistemas de automóvil autónomo, sistemas de monitoreo médico, sistemas de control del proceso, sistemas de robótica, domótica y pilotos automáticos aeronáuticos.





@RD_Anibal





Forensic-by-Design Framework for Cyber-Physical Cloud Systems

A forensic-by-design framework allows the integration of forensics tools into the development of a cyber-physical cloud system that can help organizations recover from a cyber-physical attack.

Digital forensic investigation aims to answer the six key questions of an incident—what, why, how, who, when, and where.



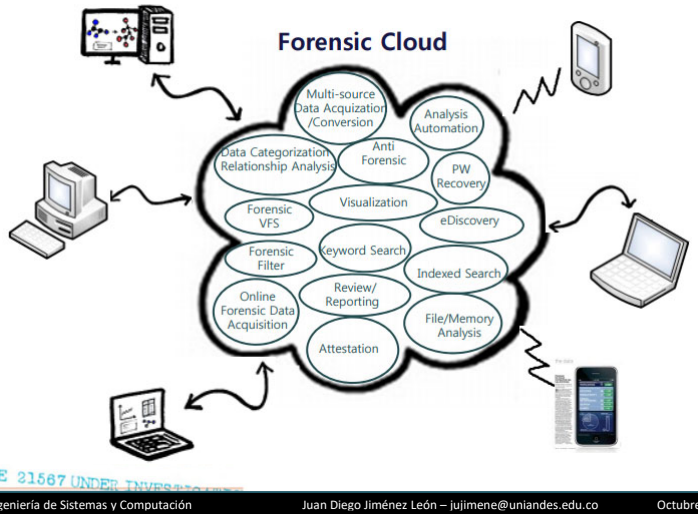
FaaS – Forensic as a Service
DFaaS – Digital Forensics as a Service

Desde esta perspectiva, uno de los aspectos más interesantes de la nube es la oportunidad de explotar un nuevo paradigma en el que se proporciona el análisis forense como una utilidad, a la manera forense como un servicio **(FaaS – Forensic as a Service).**





FaaS – Forensic as a Service

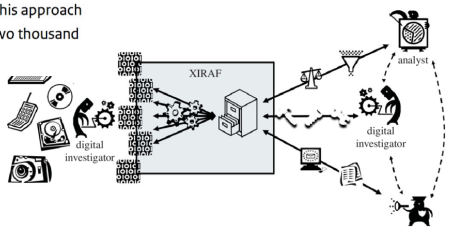


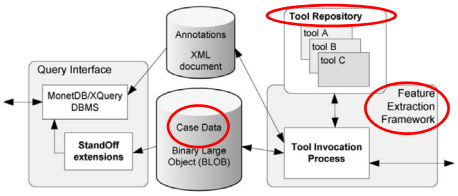
DFaaS – Digital Forensics as a Service

Hansken

Since December 2010, the Netherlands Forensic Institute provides a service-based approach for processing and investigating multiple terabytes of seized digital material: Digital Forensics as a Service (DFaaS). This previous implementation was called Xiraf, the current one Hansken. Now this approach has become a standard for hundreds of criminal cases and over two thousand investigators, both in The Netherlands and abroad.

Netherlands Forensic Institute
Ministry of Justice and Security



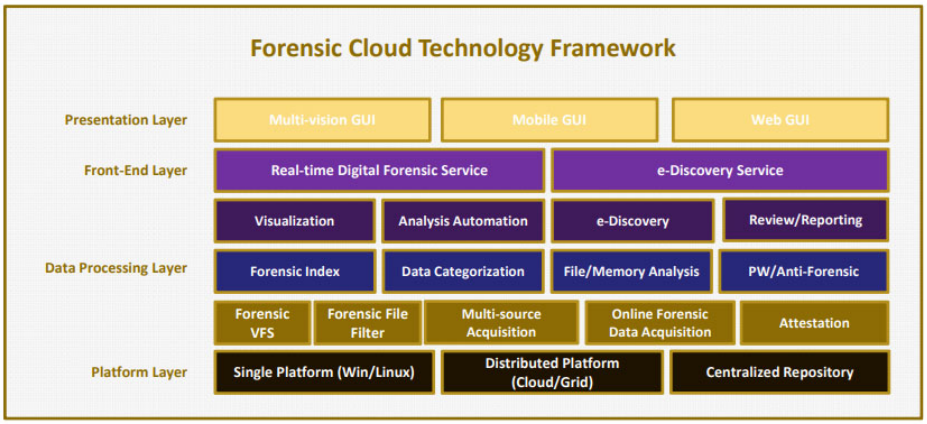


Netherlands Forensic Institute
Ministry of Security and Justice

Introducing
Hansken

LEVEL ONE SECURITY CLEARANCE ONLY
HACKING CASE 21567 UNDER INVESTIGATION

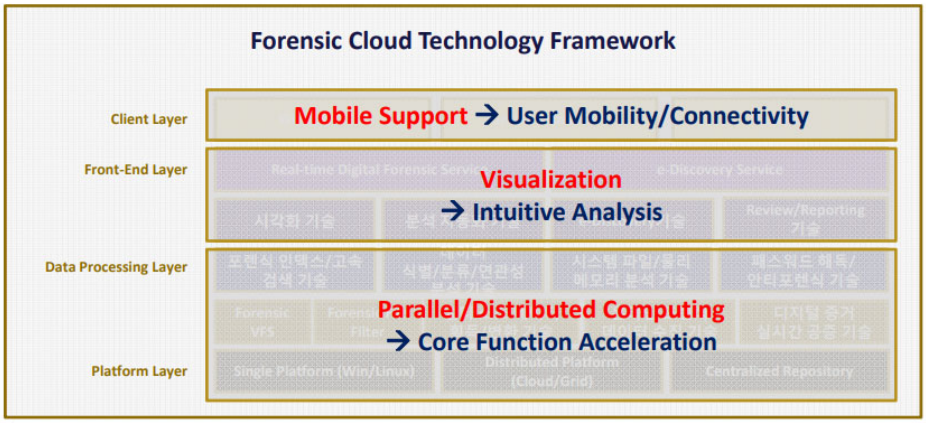
FaaS – Forensic as a Service
Forensic Cloud Technology Framework



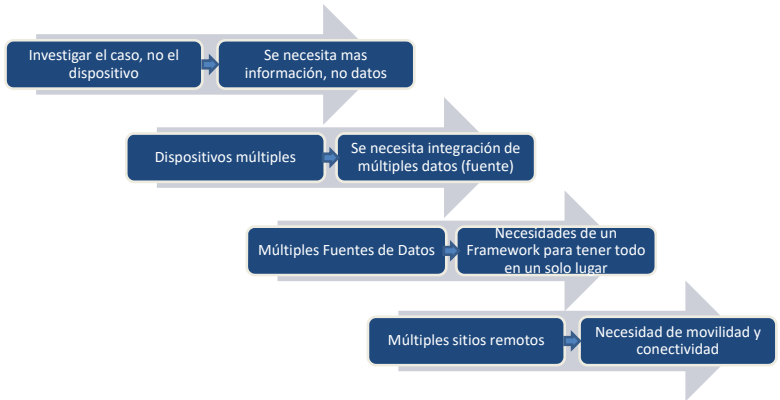
LEVEL ONE SECURITY CLEARANCE ONLY
HACKING CASE 21567 UNDER INVESTIGATION

FaaS – Forensic as a Service

Forensic Cloud Technology Framework



Nuevo punto de vista



El futuro de la informática forense

Análisis centrado en los datos → ... → Análisis centrado en la conducta

- Adquisición de evidencia de múltiples fuentes
- Análisis de relación
- Análisis Intuitivo
- Análisis automático basado en el perfil

Herramientas Forenses → ... → Servicios Forenses

- Plataforma distribuida/ paralela para el manejo de grandes volúmenes de datos
- Tener herramientas/ dispositivos que se adapten a los cambios
- Movilidad y conectividad del usuario









