Recomendaciones para estimular la Seguridad Digital Ciudadana

Recommendations to stimulate Citizen Digital Security

Gabriel Andrés Rapalino Aycardi – Joseph Pérez Castro
Universidad Simon Bolivar, Barranquilla

Resumen Las personas cada día se hacen más activas en el uso de la tecnología, ya que esta nos ofrece una serie de herramientas que se adaptan a las necesidades de las personas y a su vez son muy fáciles de usar, el guardar y buscar datos o información es algo que engloba muchas de las actividades que realizan las personas que las utilizan, y más aún cuando ya casi todos los dispositivo y maquinas pueden conectarse a internet. Las personas ignoran que así como la tecnología avanza a grandes pasos, la inseguridad en ella también lo hace, y aunque existan políticas y protocolos que vienen por defecto en las maquinas o dispositivos para evitar cierto tipo de inconveniente, no nos hacen inmune a los posibles sucesos que diariamente ocurren en el mundo digital, teniendo en cuenta que el eslabón más débil de la cadena analizada es el portador del dispositivo, y nosotros queremos de la mejor manera hacer que las personas se concienticen ante la situación, ya que si ellas no hacen el esfuerzo de por lo menos tener precaución con lo que ellos guardan o hacen en sus dispositivos nadie más lo hará, y para evitar todo tipo de inconveniente gracias a la inseguridad existente en el mundo digital se creara una plan de acción el cual se adaptara a las personas que usan estas tecnologías de la mejor manera, haciendo uso de las mismas, se promoverá el aumento de la seguridad y el uso de las mismas, para que se reduzca el índice de amenazas o ataques por parte de los Ciberdelincuentes y aumenten las acciones o métodos de defensa o respuesta ante este tipo de sucesos.

Palabras clave: Seguridad digital, Políticas de seguridad digital, Ciber defensa, Ciber ataques, Ciber Delincuentes.

Abstract People every day become more active in the use of technology, as this offers us a series of tools that adapt to the needs of people and in turn are very easy to use, saving and searching for data or information is something that encompasses many of the activities carried out by the people who use them, and even more so when almost all the devices and machines can connect to the internet. People ignore that just as technology advances at a great pace, the insecurity in it also does, and although there are policies and protocols that come by default in the machines or devices to avoid a certain type of inconvenience, they do not make us immune to the possible events that occur daily in the digital world, taking into account that the weakest link in the chain analyzed is the carrier of the device, and we want to make people aware of the situation in the best way possible, because if they do not do the effort to at least be careful with what they keep or do in their devices no one else will do it, and to avoid any kind of inconvenience thanks to the existing insecurity in the digital world an action plan will be created which will adapt to the people who use these technologies in the best way, making use of them, will promote the increase of security and the use of them, so that they Educate the index of threats or attacks by cybercriminals and increase the actions or methods of defense or response to this type of events.

Key words: Digital security, Digital security policies, Cyber defense, Cyber attacks, Cyber offenders.

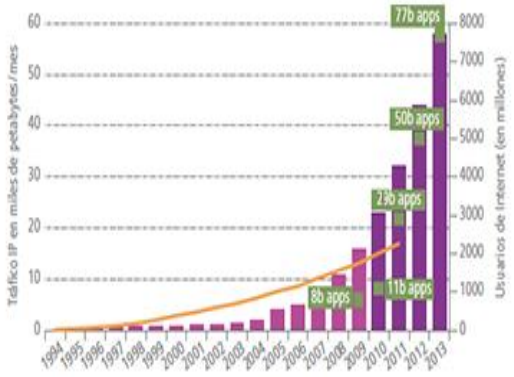
I. Introducción

"Todos los días, en todas partes, la tecnología digital está generando nuevas posibilidades, nuevas formas de trabajar y de brindar entretenimiento, de operar y de interactuar. Estamos rodeados de identidades digitales y de datos que deben ser intercambiados a través de redes con organizaciones, personas y dispositivos." (NV, 2015)

A diario, se conectan miles de personas a la red al mismo tiempo, usando redes sociales o medios de comunicación que el dispositivo conectado a la red les ofrece; estos dispositivos, a su vez, guardan datos de vital relevancia para su propietario, el peligro que corre este usuario es muy alto y la gente no parece consciente de este enorme riesgo. La seguridad digital debe ser respaldada, no solo por las acciones del gobierno, también debe ser apoyada por las organizaciones y las personas que hacen parte de esa sociedad, claro está que este

apoyo colectivo no se está dando de la mejor manera, pues las personas no están tomando en serio esta situación vulnerable y dejan pasar por alto muchos aspectos de seguridad digital. Existen diversas formas de robar y el robo físico de las maquinas o dispositivos es solo una de estas, y es más probable sufrir un robo virtual o pérdida inesperada de datos, que el ser robados de manera física por parte de algún ladrón o, incluso la pérdida del dispositivo. Dicho de esta manera, es difícil creer (para los que ignoran este hecho), pero no por ello significa que no los sufrirá, pues solo cuando las personas viven este tipo de momentos, es cuando se ponen al día con todos estos temas relacionados con seguridad digital. (Rotta, 2016)

Figura 1 – Crecimiento del tráfico IP, de los usuarios de Internet y de las descargas de aplicaciones en todo el mundo (1994-2013)



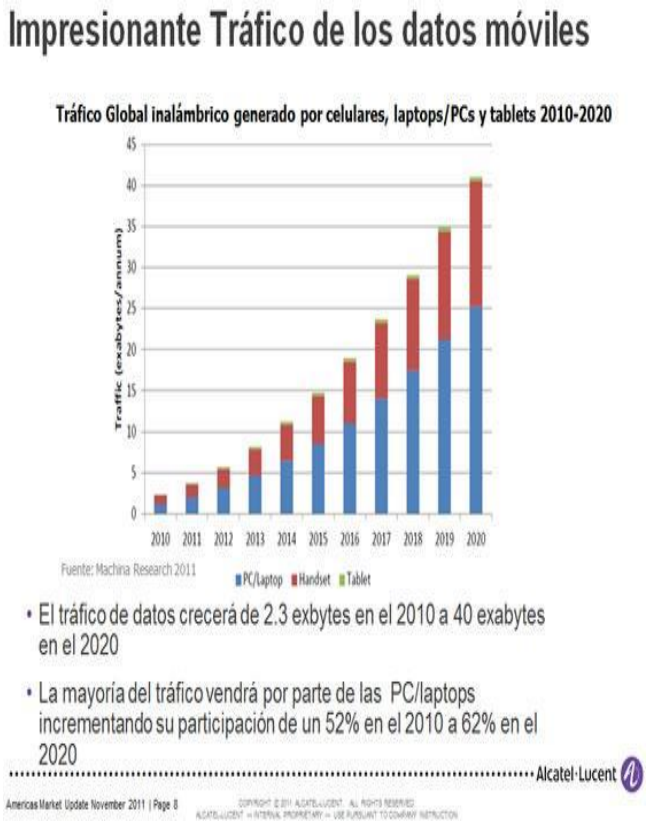
Fuente: UIT, a partir de datos de la UIT, Cisco VNI, Andrew Odlyzko, RHK, Telegeography, IDC, ABI Research y Chetan Sharma Consult
Nota – Las cifras correspondientes al tráfico IP y a las descargas de aplicaciones para 2010, así como las cifras para 2013 sobre los usuarios son estimativas.

(ITU, 2014)

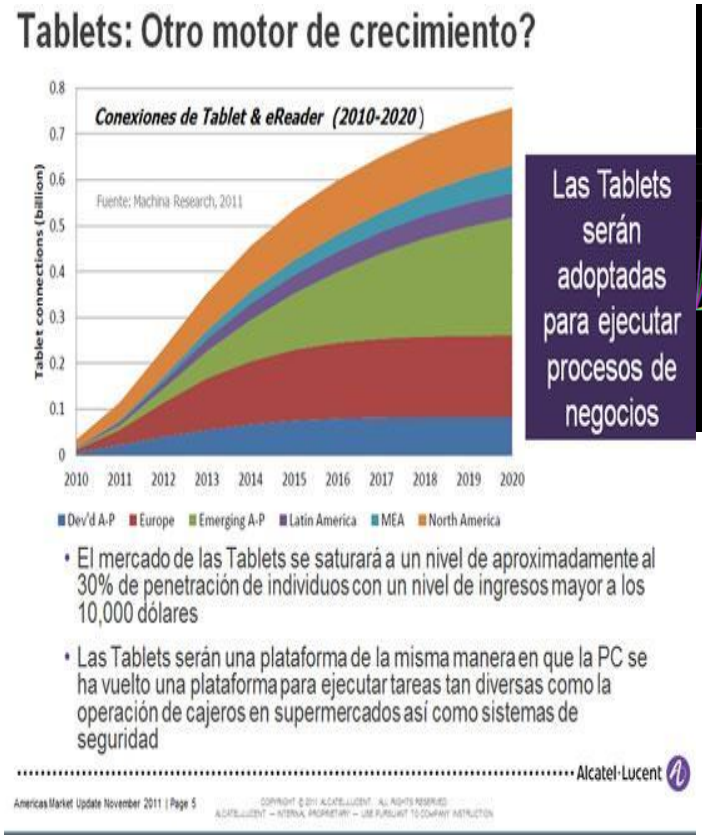
Desde la aparición de los dispositivos móviles, y posteriormente la aparición de los dispositivos móviles inteligentes (llamados así por su poder realizar muchas actividades, semejantes a las minicomputadoras) se da un aumento significativo en el uso de estas tecnológicas, más que por su simple utilidad en las funciones que estos dispositivos nos ofrecen, el aumento se da por la facilidad de comunicación que se obtiene gracias a estos dispositivos, el gran cambio entre las nuevas y antiguas tecnologías se basa en el aumento de capacidad de almacenamiento de información, el aumento de la velocidad de traslado de datos, el aumento de velocidad de navegación, el aumento y mejoramiento del entorno gráfico y la optimización del modelo a nivel físico y de software que este tiene (este último se aplica en la mayoría de los casos).

Con el avance de las tecnologías ya es lógico el pensar que la producción de celulares inteligentes superan en gran cantidad a la de los computadores de cualquier categoría (minis, portátiles y de mesa) pero la gráfica nos demuestra que el Trafico Global de Datos está siendo dominado por los computadores, esto no significa que hay más computadores que celulares, esto nos demuestra que las computadoras manejan Datos Digitales mucho más cargados que los celulares, por ejemplo, un celular se puede gastar hasta 1GB (Giga Byte) en un día viendo videos o descargarlos en calidad media, utiliza redes sociales e incluso hasta juegos que requieran de internet, pero en un computador, por el solo hecho de descargar un programa puede llevar una variación de 7 a 32GB.

Aunque los datos que se descargan desde un pc y un celular pueden variar dependo del uso que se les den, de manera breve se deja claro en el ejemplo, que las computadoras generan más tráfico de datos que los celulares; Las Tablets no se quedan atrás, pues el que no sean competencia para los computadores o celulares no significa que el uso de estos dispositivos sea casi nulo, el detalle está en que estos dispositivos tienen un uso especial y es en el mundo de los negocios, las Tablets son utilizadas mayormente en el campo laboral ya que estas con mucha facilidad adaptan muchas aplicaciones y programas que san los computadores y que los celulares no pueden siquiera ejecutar

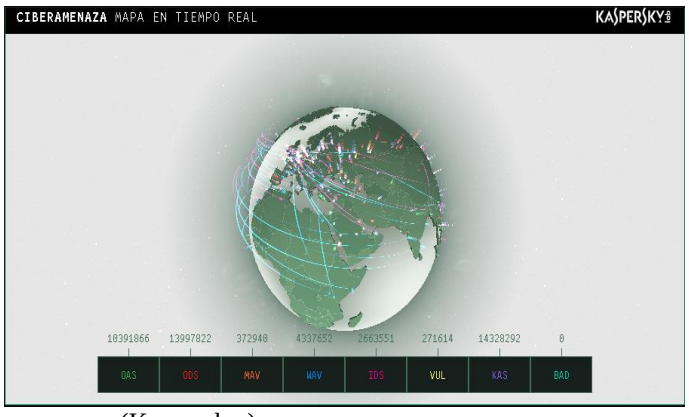


(P., 2011)

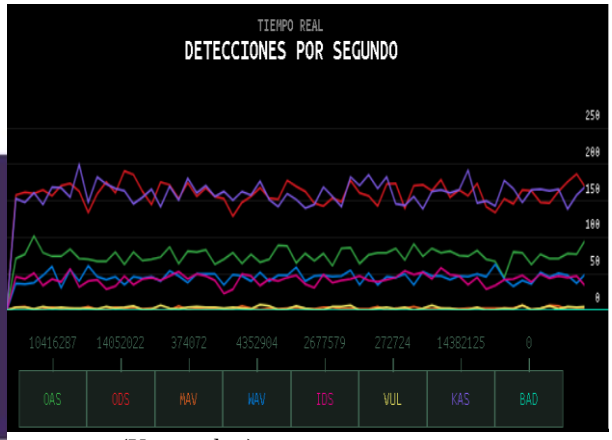


(P., 2011)

Existe una alarmante escala de ataques a nivel mundial, no solo por el hecho del número creciente de zonas geográficas que están siendo atacadas, sino también por el hecho que la densidad de estos ataques parece detenerse al paso del tiempo. El gráfico se basa en el monitoreo de las páginas web que se encuentran bajo el cuidado y/o dominio de la empresa especializada en seguridad digital Kaspersky identifica tanto el tipo de ataque como la cantidad de detecciones por segundo.



(Kaspersky.)



(Kaspersky.)

OAS (On-Access Scan) muestra el flujo de detección de malware durante el escaneo On- Access, por ejemplo, cuando los objetos son procesados durante las operaciones abrir, copiar, ejecutar o guardar operaciones.

ODS (On Demand Scanner) muestra el flujo de detección de malware durante el análisis bajo pedido, cuando el usuario selecciona manualmente la opción "Buscar virus" en el menú de contexto.

MAV muestra el flujo de detección de malware durante el escaneo MAV cuando aparecen nuevos objetos en una aplicación de email (Outlook, The Bat, Thunderbird).MAV escanea los mensajes entrantes y llama a OAS cuando guarda los adjuntos a un disco

WAV It checks the ports specified in the Web Anti-Virus settings. WAV (Web Anti-Virus) muestra el flujo de detección de malware durante el análisis Web Anti-Virus donde la página HTML de un sitio web se abre o un archivo es descargado.
IDS (Sistema de Detección de Intrusos) muestra el flujo de detección de los ataques a las redes.

VUL (Vulnerability Scan) muestra el flujo de la detección de vulnerabilidades.

KAS (Kaspersky Anti-Spam) muestra el tráfico sospechoso y no deseado descubierto por las tecnologías de Filtrado de Reputación de Kaspersky Lab.

BAD (Detección de Actividad Botnet) muestra estadísticas sobre direcciones IP de víctimas de ataques DDoS y servidores botnet C&C. Estas estadísticas fueron adquiridas con la ayuda del sistema de inteligencia DDoS.

La grafica muestra una serie de ataques que no solamente son causa de alguna persona, incluso también tiene un detector de Spam, que bien sabido no es un virus, pero es una molestia para cualquier usuario, y al ser una gráfica que da toda esa información en tiempo real ella irá cambiando a cada segundo.

En Colombia los lineamientos políticos sobre seguridad digital se basan en los documentos Conpes. El Conpes del 2016 (3584) sigue por el camino que deja el Conpes anterior, de 201. 1En primer lugar, se establecerá un marco institucional evidentemente en torno a la seguridad digital. Para esto, se crearán las máximas instancias de coordinación y orientación superior en torno a la seguridad digital en el gobierno, y se establecerán figuras de enlace sectorial en todas las entidades de la rama ejecutiva a nivel nacional debido a que el incremento del uso de los dispositivos móviles con acceso a internet trae consigo una serie de riesgos asociados con la seguridad digital. Hasta aquí fue lo que se hizo en el Conpes de 2011 En segundo lugar, se crearán las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, mediante mecanismos de participación activa y permanente, la adecuación del marco legal y regulatorio de la materia y la capacitación para promover comportamientos responsables en el entorno digital. Como tercera medida, se fortalecerá la defensa y seguridad nacional en el entorno digital, a nivel nacional y transnacional, con un enfoque de gestión de riesgos. Por último, se generarán mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico.

Para poner en marcha esta política, se ha construido un plan de acción que se ejecutará durante los años 2016 a 2019 con una inversión total de 85.070 millones de pesos. Las principales entidades ejecutoras de esta política son el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional, la Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación identificar estrategias como Garantizar la integridad y seguridad de los individuos y del Estado, a nivel nacional y trasnacional, bajo un entorno digital creciente, dinámico todo esto de la mano de las leyes en Colombia.
El país desarrolló y aprobó la Ley 1273 de 2009 que creó nuevos castigos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes, para proteger específicamente aspectos tales como la protección de datos personales, como la confiabilidad, integridad y disponibilidad; estos son los tres pilares de la seguridad de la información. En la seguridad de la información, no solo intervienen los aspectos tecnológicos, sino también los procesos, los ambientes (centro de cómputo, ubicación de oficinas) y principalmente las personas.

En Colombia ya se establecieron leyes que datan de 2009, que rigen la seguridad informática en Colombia. El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 "Por medio del cual se modifica el Código Penal, se crea 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. (Código penal, s.f.)
En diferentes países también se ha tomado este tema muy en serio, de tal forma que también le han dado un foco de gestión de problemas y de integridad, porque claro, a la final todo esto es para ayudar a los afectados, para que sepan cómo pueden evitar, o manejar riesgos digitales.

II. Objetivos

Crear y divulgar recomendaciones para el uso de la Tecnología Digital, para evitar el Hacking y poder defenderse contra todo tipo de amenaza para los datos de nuestros dispositivos.

Objetivos generales

- Crear recomendaciones de uso para personas con edades definidas
- Basándonos en hechos registrados y con los más recientes relacionados con la Seguridad Digital crearemos planes de acciones realizables para usuarios comunes sin un conocimientos profundos sobre tema.
- Fomentar por medio de redes sociales u otro tipo de medio de comunicación las recomendaciones de una manera entendible para cualquier receptor.

III. Metodología

Este es un proyecto de investigación de los estudiantes de ingeniería de sistemas de octavo semestre que se basa en dar sugerencia en lo que se debe hacer y lo que no se debe hacer al momento de navegar por el internet y de utilizar dispositivos conectados a la red. Todo esto con el fin de saber si estoy en una página segura, si es información correcta etc. Esto es un proyecto es una mezcla de conocimientos cualitativos y cuantitativos por lo que se realizó una encuesta sobre el tema "Que tan seguro crees que estas" que nos dejará ver cómo está la sociedad en general sobre tema que es tan importante para todos por lo que se viene mostrando en el mundo con tantos ataques y no sabemos cómo defendernos.

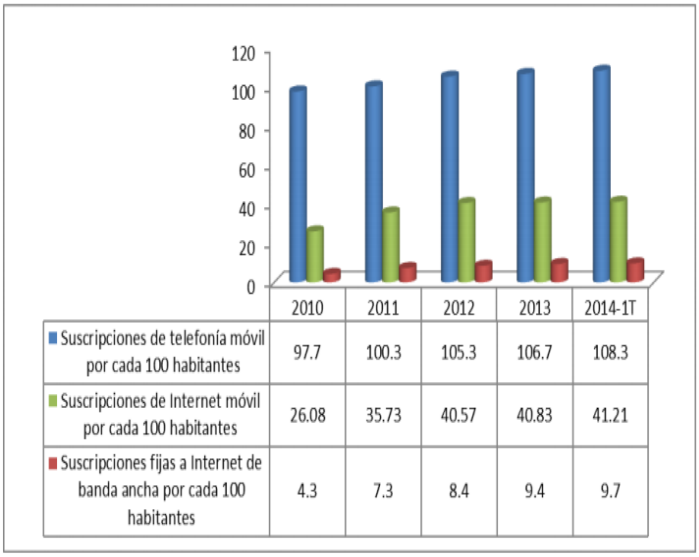
Pero también queremos que la comunidad en general esté al tanto de este tema que es de importancia para todos hemos creado una página web que lleva por nombre NAVEGA SEGURO la cual ofrece información de calidad y actualizada sobre el tema, pero eso no es todo; como todos sabemos estamos en la era de las redes sociales, así que hemos creado también un twitter para estar más cerca de la comunidad el cual lleva en mismo nombre ya mencionado y una página en Facebook, para complementar la estrategia de divulgación.

IV. Evolución

Los resultados relacionados con el pilar de Infraestructura y acceso a las TIC, el cual incluye indicadores de suscripciones

de telefonía móvil, Internet banda ancha e Internet móvil por cada 100 habitantes (Gráfica No. 1.), muestran en primer lugar que, el mercado de telefonía móvil es un mercado maduro en el que la penetración asciende a 106.7 suscriptores por cada 100 habitantes. En segundo lugar, las suscripciones fijas a Internet banda ancha por cada 100 habitantes, han aumentado a lo largo del tiempo pasando de un 5.9% en el 2010 a un 9.5% en el 2013. Finalmente, las suscripciones de Internet móvil por cada 100 habitantes que están compuestas por dos tipos de acceso, los accesos pos suscripción y los accesos por demanda, han aumentado cerca de 15 puntos porcentuales comparando el año 2010 con el año 2013, y se evidencia una tendencia positiva a lo largo del periodo analizado. Entre el año 2012 y 2013 el aumento de la penetración el Internet móvil fue del 0.3%. Esto se debe a que los abonados a Internet (acceso por demanda) han presentado un comportamiento decreciente, mientras que los suscriptores a Internet (acceso por suscripción) han presentado tasas de crecimiento anuales superiores al 40%, lo que implica un de sustitución de los usuarios en la modalidad de tipo de acceso a Internet móvil.

Gráfica No. 1. Suscripciones de telefonía móvil, Internet banda ancha y móvil por cada 100 habitantes Fuente: Cálculos CRC, con base en datos SIUST – Colombia TIC.



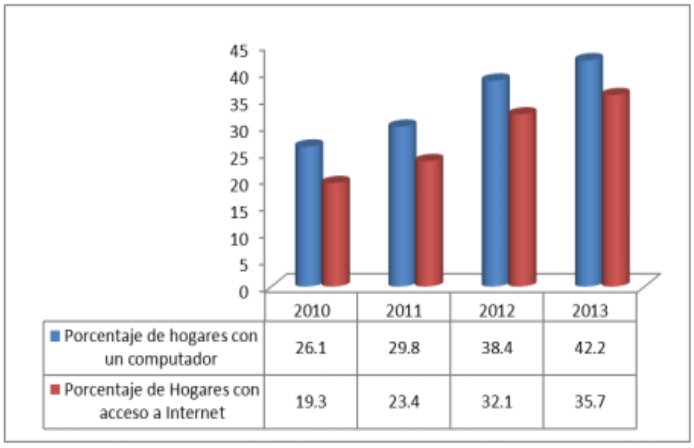
	2010	2011	2012	2013	2014-1T
Suscripciones de telefonía móvil por cada 100 habitantes	97.7	100.3	105.3	106.7	108.3
Suscripciones de Internet móvil por cada 100 habitantes	26.08	35.73	40.57	40.83	41.21
Suscripciones fijas a Internet de banda ancha por cada 100 habitantes	4.3	7.3	8.4	9.4	9.7

Fuente: Cálculos CRC, con base en datos SIUST – Colombia TIC.

(informacion, s.f.)

Acceso y Uso de las TIC por Hogares e Individuos

En cuanto al acceso y uso de las TIC por hogares e individuos se tiene en la Gráfica No. 4 que en el año 2013, el 42.2% de los hogares tenían computador de escritorio, portátil o tableta. En este sentido, el aumento en la tenencia de computadores se ha traducido en un aumento en el acceso a Internet que en el 2013 alcanzó un nivel del 35.7% frente a un 19.3% en el 2010, 16.4 puntos porcentuales por encima.
Grafica No. 4. Porcentaje de hogares con computador y acceso a Internet



	2010	2011	2012	2013
Porcentaje de hogares con un computador	26.1	29.8	38.4	42.2
Porcentaje de Hogares con acceso a Internet	19.3	23.4	32.1	35.7

:e: Encuesta Integrada de Hogares 2010 y 2011 y Encuesta de Calidad de Vida 2012 y 2013 (DANE).

(informacion, s.f.)

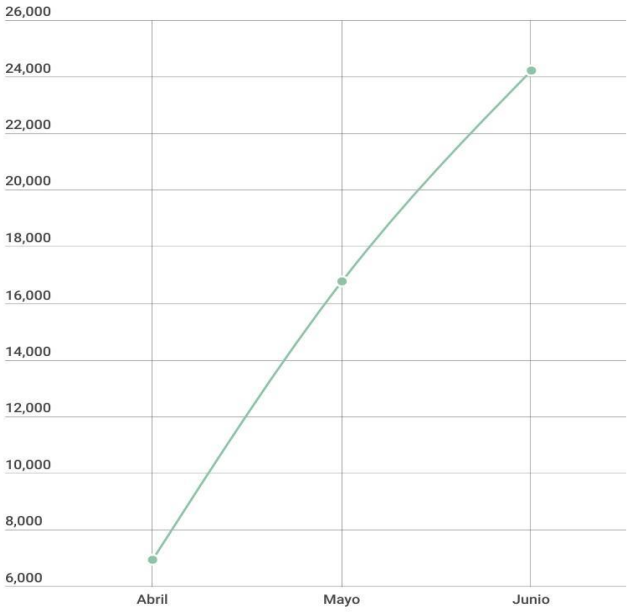
Las TIC en Colombia

En materia de apropiación de dichas tecnologías, Colombia exhibe indicadores aceptables y con clara tendencia de mejora en ciertos aspectos. El país se ha mantenido estable en el ranking mundial del NRI1 , indicador que de mide el grado de preparación que tienen las sociedades para beneficiarse de las TIC, ubicándose en el puesto 60 (de 133 países) en el periodo 2009-2010, y localizándose en el puesto 7 dentro de Latinoamérica. Este índice considera tres categorías: entorno, preparación y uso y en todos estos tres componentes Colombia ha mejorado su posicionamiento internacional. Respecto al componente de entorno de este indicador, Colombia ha subido notablemente su posición en el ranking, situación que evidencia el buen ambiente regulatorio, fiscal y normativo, toda vez que los factores que más impacto tienen sobre este componente son los de carga de la regulación gubernamental, el alcance y los efectos de los impuestos, la tasa total de impuestos y el tiempo para hacer cumplir los contratos.

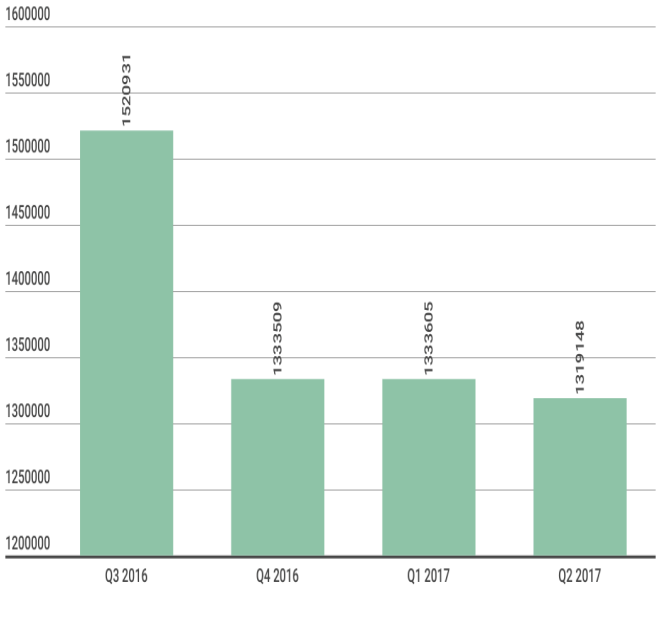
El país también ha mejorado en el componente de uso, especialmente por cuenta del Gobierno a través de los servicios de gobierno en línea2, aspecto en el cual Colombia se ubica en la posición 9 del NRI a nivel mundial. Especial distinción debe hacerse en este aspecto ya que en 2010 el país ascendió 21 puestos en el Reporte de Gobierno Electrónico Global de la ONU, ubicándose en primera posición dentro de los países de la región y sobrepasando incluso a Chile.

Evolución de las amenazas informáticas

Según los datos de KSN, las soluciones de Kaspersky Lab neutralizaron 342 566 061 ataques lanzados desde recursos de Internet ubicados en 191 países del mundo. Se registraron 33 006 783 direcciones URL únicas que provocaron reacciones del antivirus web. Se neutralizaron intentos de ejecución de programas maliciosos que roban dinero mediante el acceso en línea a cuentas bancarias en los equipos de 224 675 usuarios.



Estadística de las amenazas móviles
En el segundo trimestre de 2017, Kaspersky Lab detectó 1 319 148 paquetes de instalación maliciosos. Esta cifra ha permanecido prácticamente inalterada en comparación con los dos trimestres anteriores.



IV. Resultados

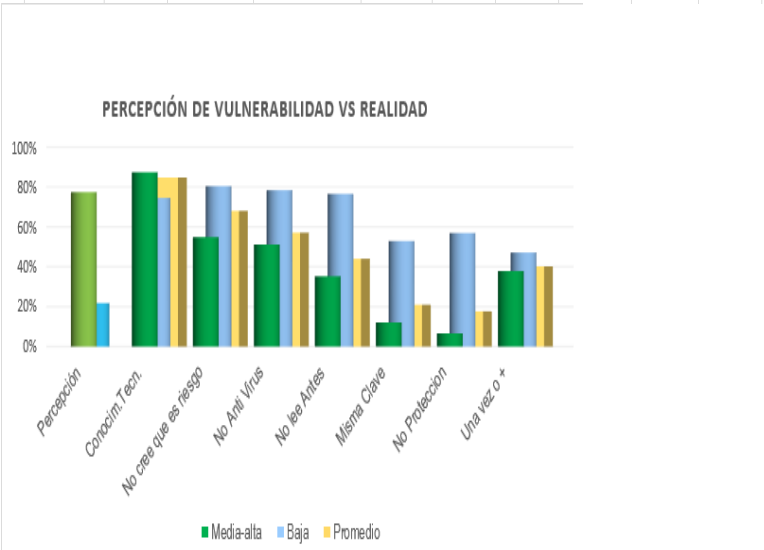
Se creó una encuesta con el fin de analizar las diversas falencias las cuales debemos atacar con las recomendaciones, con una serie de preguntas que de manera individual parecen no ser de mucha relevancia pero al unirlas tienen un patrón, ya que el responder que se tiene conocimiento con el tema tratado significa que debe tener cuidado o por lo menos tener idea de lo peligroso que es publicar información en internet, y poder así cruzar las respuestas y al analizarlas obtener una visión más amplia y clara de lo que está sucediendo con las personas.

Estos son los resultados de la encuesta.

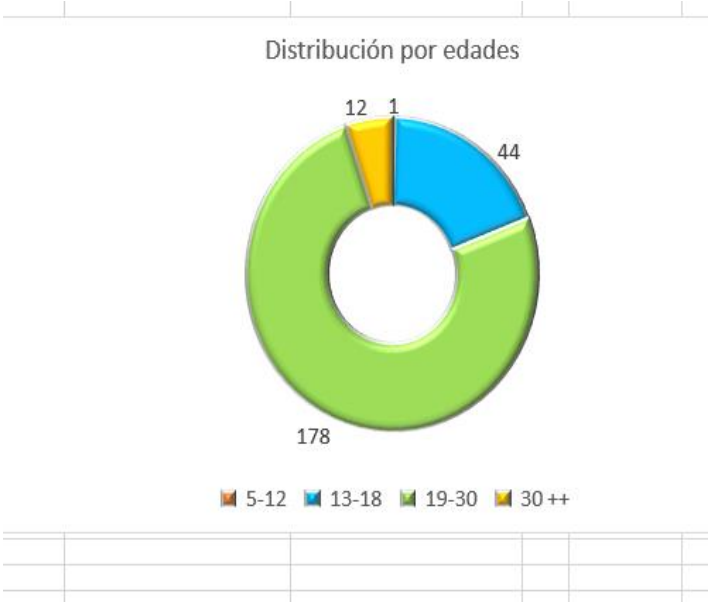
Media-Alta	3 a 5	Conocim.Tecn.	No cree que es riesgo	No usa AntiV	No lee Antes	Misma Clave	No Proteccion	Una vez o +
Cant	182	159	100	93	64	22	12	69
Porc ABS	77,4%	67,7%	42,6%	39,6%	27,2%	9,4%	5,1%	29,4%
Porc RELATIVO		87,4%	54,9%	51,1%	35,2%	12,1%	6,6%	37,9%
Baja	1 a 2							
Cant	51	38	41	40	39	27	29	24
Porc ABS	21,7%	16,2%	17,4%	17,0%	16,6%	11,5%	12,3%	10,2%
Porc RELATIVO		74,5%	80,4%	78,4%	76,5%	52,9%	56,9%	47,1%

Total	3,38							
Porcentaje		84,7%	68,0%	57,1%	44,0%	21,0%	17,6%	40,2%

	Percepcion	Percepción	Conocim.Tecn.	No cree que es	No Anti Virus	No lee Antes	Misma Clave	No Proteccion	Una vez o +
Media-alta	3 a 5	77,4%	87,4%	54,9%	51,1%	35,2%	12,1%	6,6%	37,9%
Baja	1 a 2	21,7%	74,5%	80,4%	78,4%	76,5%	52,9%	56,9%	47,1%
Promedio	3,38		84,7%	68,0%	57,1%	44,0%	21,0%	17,6%	40,2%



Evaluación y resultado de las preguntas, cruzando el número de personas que realizaron la encuesta con las respuestas que dieron en el test,



Resultado de la edad de las personas que hicieron el test, se deja claro que la edad de la mayoría de las personas que están involucradas para este proyecto promedia entre 13 y los 30 años, dando a entender que son estudiantes de bachiller, universitarios y/o trabajadores.

Resultado de las personas que dicen tener conocimientos respecto al tema tratado "Seguridad Digital" clasificada en orden por edades.

Análisis de resultados

Del 100% de las personas que realizaron la encuesta un 77,4% afirma tener una seguridad Media-Alta en sus dispositivos, esto sería algo significativamente bueno, las personas no solo son conscientes de que necesitan seguridad, sino que también la tienen y lo reconocen, pero este dato obtenido con esa pregunta no es muy positivo respecto al resto de las preguntas, ya que de este 77,4% que se tienen una seguridad Media-Alta 51,1% no tiene antivirus, utilizan ya sea contraseñas, PIN o seguridad dactilar o facial, este tipo de seguridad es funcional para eventos físicos, es decir, haciendo uso del dispositivo, sin programas ni otro tipo de método, a su vez esto significa que están vulnerables ante ataques digitales, virus maliciosos, de espionaje y demás, y tengamos presente que el 87,4% de estas personas con seguridad Media-alta acepto el tener conocimiento respecto al tema, y el 35,5% no lee los permisos de las aplicaciones, ignorando el hecho de que no consideran peligrosa la información que publican el resto de las conclusiones son muy alarmantes y nos dan más motivos para pensar, creer y afirmar que este proyecto es algo que las personas necesitan, y que no es algo inventado con fines académicos.

De la misma manera se tienen en cuenta las personas que tienen seguridad baja en sus dispositivos, el no tener seguridad ya sea con antivirus o aplicaciones para protección de su privacidad es algo que se puede esperar, pero lo que no es lógico de estas personas es que del 21,7% que conforma a la cantidad de las personas con seguridad baja el 74,5% de ellas tiene conocimientos del tema, esto significa que las personas creen que saben cuándo realmente no es así, o no se interesan porque creen que no les pasara algo malo en sus dispositivos, se nos abre otra puerta no solo para ayudar a las personas en ampliar su conocimiento, sino que para abrirles los ojos y darles a entender el peligro en el que se están exponiendo, pues si en algún momento algún virus ataca de manera global, estas personas serán las afectadas de manera segura, y también demostrarles que el instalar una aplicación sin leer los permisos también abre puertas a ciberdelincuentes, sin importar que estas aplicaciones vengan de la tienda oficial.

V. Discusión

Con base a los resultados obtenidos gracias a la encuesta que se realizó de manera virtual, se deja claro que las personas creen que tienen los conocimientos suficientes respecto al tema de seguridad digital, y además creen que lo que hacen diariamente con sus celulares, computadores y demás dispositivos que se pueden conectar a internet no los está poniendo en riesgo, y peor aún, muchos de ellos no hacen algo al respecto para proteger sus datos o demás información que poseen en estos dispositivos. Lo anterior mencionado es el resultado de una pequeña cadena social, y puede que el número de personas no sea relevante cuando se habla de una escala global, pero sería ilógico el no reconocer que lo anterior mencionado aplica también a nivel global, y más aún cuando el porcentaje de personas que tienen una edad entre 13 a 30 fueron las que tuvieron mayor participación en la encuesta, pues las personas en este rango de edad, a diferencia de los menores o de los que tienen más edad, son más apegados a la tecnología y deberían ser más conscientes de lo que está sucediendo en el inestable(en términos de ataques globales o locales) mundo digital.

En el problema tratado de seguridad digital se debe tener en cuenta los siguientes factores:

1. Aumento de tecnología: "Está creciendo el número de colombianos que tienen equipos que les permiten conectarse a Internet de Banda Ancha. Mientras en 2015, por cada 100 colombianos había 54,5 terminales, en el 2016 la cifra subió a 69,55*" (MinTIC, 2017), el avance tecnológico da paso a un sinfín de dispositivos que siguen creciendo diariamente, y Colombia no se queda atrás en este aumento, pues en un comunicado afirmó el ministro TIC, David Luna, "Conectamos un país y ahora estamos viendo como cada vez más colombianos tienen equipos para aprovechar las oportunidades de desarrollo y prosperidad que brinda internet, entre otros, gracias al esfuerzo de programas como Computadores para Educar" (MinTIC, 2017)

2. Aumento de usuarios conectados a la red: años atrás el tener internet era un lujo, pero actualmente es una necesidad, la facilidad en términos de comunicación, y las oportunidades que genera el estar en internet han aumentado, consigo también lo han hecho los peligros, pero esto no evita que cada día más personas están accediendo a la red, y esto se puede evidenciar gracias a un estudio realizado por MinTIC en 2014, ya que ellos afirmaron lo anterior dicho gracias a esta conclusión "Se pudo establecer que más hogares están conectados a Internet, el 64% de las casas en ciudades de más de 200 mil habitantes cuenta con conexión. El 71% de los encuestados accede a Internet desde su casa y el 20% en cafés Internet." (MinTIC, 2014), y aunque ese estudio fue ya hace 3 años, nos da para seguir pensando que esa escala ha seguido aumentando.

El problema de seguridad digital en su gran mayoría es tratado desde un punto de vista social, se hacen estudios, pruebas y conclusiones utilizando como referencia a las personas, pero este problema no conoce de personas, estratos o tipos, ya que así como las personas diariamente están al peligro de un ataque a sus dispositivos base a algún malware, las empresas e incluso el gobierno está a este peligro, aunque los protocolos de seguridad sean más estrictos, estas no se salvan o no están excluidas de los puntos de ataques para los virus informáticos, y en la mayoría de los ataques que se dan a nivel global o que son conocidos a nivel global los principales afectados son las empresas y/o gobiernos, pues a diferencia de una persona, las pérdidas que se dan son muy significativas y millonarias.

Ante tales amenazas, los países desarrollan cuerpos que se encargan del estudio y prevención de amenazas virtuales que se puedan presentar y que afecten en su campo de comercio tales como La Organización Mundial de la Propiedad Intelectual (OMPI) que se encuentra en la ciudad de Ginebra, Suiza, La Organización para la Cooperación y el Desarrollo Económico la integran (OECD) 29 países, El Consejo Nacional de Política Económica y Social CONPES fue creado por la Ley 19 de 1958 en Colombia, y muchos otros más, sea cual sea la razón de su origen, estos organismos no solo aportan soluciones a gobiernos o empresas, también dan soluciones, guías y apoyos a las personas, porque es el sector más poblado y a su vez el más vulnerable, como se menciona al inicio las personas creen estar capacitadas para asimilar este tipo de eventos, pero la verdad es que no están haciendo algo para ello, el nivel de seguridad en las personas es muy bajo y como respuesta a ello las personas creen que la responsabilidad cae en manos del gobierno o de estos entes que regulan la seguridad digital, la verdad es que esto debe ser una acción compartida, en donde los entes dan las normas y las personas deben cumplirlas, se debe hacer la aclaración de que si una persona no cuida sus datos nadie lo hará por ella, y que los peligros están en todas partes y no solo en países extranjeros, pues el más conocido ataque global llamado Wannacry afecto incluso a empresas ubicadas en Colombia cosa que se demostró a inicios de estudio para este artículo, y las personas también estuvieron en riesgo en ese momento y aun son propensos a recibir otro tipo de ataques.

4. CONVI. Conclusión

al terminar la etapa de investigación concluimos que: desde el periodo inicial se identificaron dificultades en la seguridad en los niños, jóvenes y adultos, apatía y poca información respecto al tema, sin embargo, desde las primeras publicaciones en twitter cambiaron su perspectiva y mostraron preocupación por lo vulnerables que somos frente a los ataques. Al planear y diseñar las estrategias para mejorar nuestros conocimientos sobre el tema, se optó por escoger un blog como herramienta pedagógica, publicaciones en redes sociales, teniendo en cuenta que todos tenemos acceso inmediato a la internet, lo que facilita el acceso a estas plataformas para incentivar a los usuarios a implementar nuestras observaciones.

Se logró evaluar el nivel de conocimiento que poseen los usuarios sobre seguridad digital en este proyecto de investigación, aplicamos una encuesta en la cual nos deja percibir lo errados que están los usuarios al pensar que están seguros sus datos, por lo tanto les hicimos saber de las herramientas necesarias para proteger su información de acuerdo a lo establecido por el gobierno con la creación del CONPES 3701 de 2011 para seguir creciendo en el entorno de seguridad digital.

5. R

6. R

Recomendaciones para adolescentes

-limita el acceso a tu información solo a las personas más cercanas a ti, no uses las redes para conocer gente ya que puede ser muy peligroso

-usa las herramientas de configuración de la privacidad de las redes sociales para mantener algún tipo de control sobre la información que coloques en el sitio si te resulta difícil recurre a la ayuda de tus padres o profesores

-en los perfiles de tus redes sociales no escribas información personal por ejemplo tu nombre completo, domicilio, número telefónico.

-coquetear en línea con personas extrañas puede graves consecuencias ya que algunas mienten y pueden hacerse pasar por niñas o niños cuando en realidad son personas adultas nunca puedes saber reamente con quien estas tratando

-conserva los mensajes electrónicos y toda la información indebida (como frases o imágenes ofensivas) servirán en caso de que sea necesario denunciar ante las autoridades

-no permitas el acceso o aceptes invitaciones de amistad de personas desconocidas, aunque se presenten como de la escuela, de algún club equipo deportivo arque perteneces o amistades de familiares

-nunca compartas información que sirva para identificarte o localizarte fuera de internet por ejemplo los lugares que frecuentas los días y la hora en que estas en la casa o los momentos en que te quedas a sola

Recomendaciones para seguridad de pc

*ESET es una compañía de seguridad informática la cual fue creadora de un mundialmente conocido Software antivirus llamado ESET NOD32.

-Contraseñas
Son la puerta de entrada a nuestro correo electrónico, perfil en redes sociales y demás servicios online que utilizamos en nuestro día a día en Internet. Recuerda: Usa siempre contraseñas largas (mínimo de ocho caracteres) en las que se combinen letras, números y caracteres especiales (_, &, -), y cámbialas cada cierto tiempo. Nunca emplees las mismas claves para diferentes perfiles y cuentas de correo.

-Ojo con las redes WIFI públicas
Si vas a utilizar una red WIFI pública (a la que accedes en cafeterías, hoteles u otros locales) es mejor evitar compras online y acceso a servicios que requieran introducir una contraseña. Evita cualquier tipo de dato personal porque puede ser recopilado por personas ajenas.

-Configura la seguridad de tu router
Al igual que ocurre con las contraseñas, debes cambiar de forma regular los datos de acceso a tu router para evitar el acceso de otras personas. Las claves para la contraseña son las mismas que hemos visto anteriormente.

-Sistema operativo actualizado
Cualquier experto en seguridad informática te confirmará que es una medida indispensable para evitar amenazas en Internet. Si tu software no está actualizado estás dejando la puerta abierta al malware que, tenlo claro, se actualiza y renueva cada día para infectar tu equipo.

-Antivirus instalado
Para garantizar una navegación segura en Internet y evitar las amenazas que afectan a tu seguridad informática es indispensable que tengas un programa antivirus y que esté siempre actualizado. Puedes encontrar referencias gratuitas en un apartado de este post

-Compras online en plataformas seguras
Eventos como el Black Friday o el CiberMonday ponen de manifiesto que cada vez compramos más en Internet, pero hacerlo con seguridad depende que siempre que realices una compra online lo hagas a través de plataformas fiables.

-Utiliza contraseñas seguras:
Asegúrate de usar contraseñas seguras. Sigue estos consejos:
•No utilices nombres, ni de personajes de ficción (Tampoco utilices otros datos como matrículas, teléfonos, DNI, etc.)
•Crea contraseñas únicas para cada sitio: Hay herramientas que te ayudarán a gestionar esta información.
•Es imprescindible que las contraseñas de las redes sociales sean únicas. Ej. Si te das de alta en una web menor en la que trabaja un indeseable, éste podría acceder a tu contraseña y a tu correo y con ello a todas tus contraseñas o cuentas (con la opción de ¿Olvidó su contraseña?)
•Mezcla caracteres como -·$%/&) con mayúsculas y minúsculas
•Cambia tu contraseña con frecuencia
•No reveles tus contraseñas a nadie

-Utilizar tecnologías de seguridad: las soluciones antivirus, firewall y antispam representan las aplicaciones más importantes para la protección del equipo ante las principales amenazas que se propagan por Internet. Utilizar estas tecnologías disminuye el riesgo y exposición ante amenazas.

-Actualizar el sistema operativo y aplicaciones: el usuario debe mantener actualizados con los últimos parches de seguridad no sólo el sistema operativo, sino también el software instalado en el sistema a fin de evitar la propagación de amenazas a través de las vulnerabilidades que posea el sistema.

-Utiliza https:// y no http://
Utiliza https:// en tu Facebook / Twitter / LinkedIn y no http://. En muchas ocasiones alguien podría estar “escuchando” la información que se transmite desde nuestro ordenador, por ejemplo, el tráfico Wifi. Hay muchas aplicaciones y foros en Internet que permiten que un “micro hacker de pacotilla”, se haga con nuestras contraseñas. La comunicación https:// viaja encriptada y es más difícil de descifrar y mucho más segura para las redes sociales.

-Se precavido cuando utilices un ordenador compartido:
Cuando utilices un ordenador que no sea tuyo, ya sea en un ciber café o en tu trabajo, asegúrate de:
•Cerrar la sesión cuando termines de usarlo
•No permitas que el navegador recuerde las contraseñas
•Limitar la información sobre tu cónyuge e hijos

-Usa herramientas para administrar la seguridad: Cuando quieras utilizar una aplicación de Facebook está, de forma

automática, te solicita que autorices su ingreso a tu perfil, con la condición que le permitamos realizar ciertas funciones, como por ejemplo publicar en tu muro, enviarte mensajes, tener acceso a tu lista de amigos, etc.
No tienes la posibilidad de decidir qué función quieres autorizar y cuál no, es todo o nada. Sin embargo, gracias a FBSecure, una extensión para los navegadores Chrome y Mozilla Firefox puedes elegir de forma individual que función puede realizar la aplicación y cual no

-Proteger el acceso a la información del dispositivo: "todos nos acordamos de introducir nuestro PIN cada vez que encendemos los dispositivos, pero pocos recordamos establecer la contraseña de seguridad para desbloquearlo cuando ya está activo". ESET recomienda introducir una contraseña de seguridad para acceder a la información del dispositivo. De este modo aumentan las barreras contra un posible robo de datos.

-Utilizar sólo conexiones fiables: ESET advierte a todos los usuarios de desconfiar de las conexiones wifi públicas y gratuitas. "Es mejor conectarte, en la medida de lo posible, a una red que tenga contraseña o cifrado", dice. En ocasiones, según el comunicado, las redes wifi gratuitas son "trampas puestas por “ciberdelincuentes” que interceptan el tráfico de red de todos los dispositivos que se conectan a ellas, teniendo acceso a todo tipo de información. Además muchas aparecen como redes y son conexiones punto a punto con otros PC

-Cuidar las conexiones entrantes: activar el bluetooth y la wifi sólo cuando se necesiten utilizarlos, de forma que no se conviertan en puertas abiertas a posibles intrusos. También recomiendan proteger con contraseñas el acceso al terminal a través de estas conexiones.

-Mantener en correcto funcionamiento las memorias extraíbles: si se comparten tarjetas, memorias USB o dispositivos similares para compartir archivos entre portátiles, tabletas, cámaras de foto y vídeo, etc. recuerda que es necesario analizarlas siempre con un antivirus para asegurarse de que no contienen ninguna amenaza que pudiera distribuirse a los diferentes periféricos.

-proteger el equipo: para aquello que siguen utilizando el portátil es necesario instalar un buen software de seguridad que detecte todo tipo de amenazas de forma proactiva que impida resultar infectado por cualquier de los millones de códigos maliciosos que cada día se mueven por Internet.

a. Recomendaciones para el manejo de Smartphone

-Baja siempre aplicaciones de las tiendas oficiales (Google Play y App Store) o de aquellas en las que esté acreditada la seguridad en las descargas.

-Código IMEI indispensable que siempre lo tengas a mano y a buen recaudo porque, gracias a él, podrás bloquear tu dispositivo en caso de pérdida o robo. ¿Sabes cómo obtener el código IMEI? Teclea *#06# para conocerlo y guárdalo por si las moscas.

-Servicios de mensajería. Todos usamos alguno y, al igual que ocurre con las redes sociales, conviene detenerse un momento para configurar las opciones de privacidad de WhatsApp o Telegram para ver qué información compartimos y, en este caso, qué elementos (vídeos, fotografías…) pueden descargarse de forma directa en nuestro móvil. Antes de pinchar en un enlace que te remitan por WhatsApp o Telegram asegúrate de que es fiable.

-Antivirus. Siempre instalado en nuestro dispositivo y con la opción de revisar todas y cada una de las aplicaciones que nos descarguemos para descartar cualquier posible amenaza en nuestro dispositivo móvil.

-Copia de seguridad. Al igual que en tu ordenador, realiza de forma periódico copias de seguridad de tus contactos y documentos de interés para tenerlas disponibles en caso de problema con el móvil o de amenaza de seguridad.

Navega seguro

Nuestra página está diseñada para cumplir los objetivos planteados al inicio de del proyecto, nos enfocamos en las personas que utilizan dispositivos con conexión a internet y con las que en edad promedian entre las 13 y los 30, pues en esta generación son los más apegados a las rede sociales y los que más usan estos dispositivos, esto los hace más vulnerables ante ataque si no son conscientes de las peligros que los rodea, y también para aquellos que creen tener los conocimientos necesarios del problema tratado pero en realidad no los tienen y peor aún no los aplican.

Gracias a la colaboración de la Universidad Simón Bolívar pudimos crear esta página dentro de su dominio, para ingresar a la página se debe ir directamente al siguiente enlace: http://www.ingsistemasunisimon.co/~navegaseguro/

Imágenes: (Inicio)

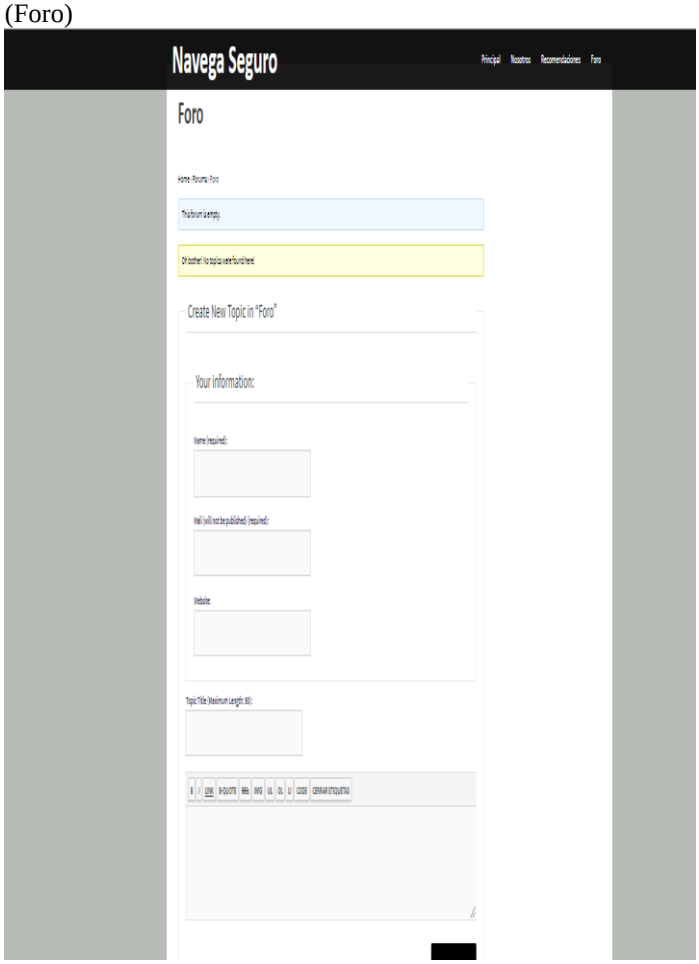

Navega Seguro
Principal
Nosotros
Recomendaciones
Bienvenidos a Navega seguro
Mejora tu seguridad Digital!
HACER TEST DE SEGURIDAD.


Navega Seguro
Principal
Nosotros
Recomendaciones
Foro
Nosotros
Con el fin de aumentar la seguridad digital de las personas se han creado una serie de tips que resultan siendo muy útiles y prácticos para aumentar la seguridad de la información que se maneja en los dispositivos que se conectan a Internet, esta información esta dirigida para las personas que son las mas propensas a recibir ataques ya que estas no saben como prevenir ataques o incluso muchas de ellas no saben como defenderse ante un ataque digital, apoyado de las políticas dadas por el documento CONPES intentamos concientizar a las personas para que estas aporten también a los demás órganos que cubren la seguridad digital en Colombia o en el mundo y mejorar las seguridad digital.
CIBERAMENAZA MAPA EN..
click aquí!
Lista de Links o Referencias
Pegs o Documentos
Videos
Pie
EQUIPO DE TRABAJO
Dc. Vladimir Quintero:
vquintero2@unisimonbolivar.edu.co
Ing. Gabriel Repalino:
gabriel_repa@hotmail.es
Ing. Joseph Perez:
josephperezcastro@gmail.com

(Nosotros)

(Recomendaciones)

(Foro)



Referencias bibliográficas

codigo penal, c. p. (s.f.).

ITU. (2014). Obtenido de ITuneNews: http://itunews.itu.int/es/5089-Evolucion-de-las-TIC-a-escala-mundial-.note.aspx

Kaspersky. (s.f.). Obtenido de https://cybermap.kaspersky.com/es/subsystems/

NV, G. (20 de 07 de 2015). Gemalto. Obtenido de Gemalto NV

P., O. R. (18 de 11 de 2011). Evaluamos. Obtenido de http://www.evaluamos.com/2011/internal.php?load=detail&id=12883

Rotta, S. L. (28 de 01 de 2016). Obtenido de http://www.elespectador.com/tecnologia/seguridad-digital-una-responsabilidad-social-articulo-613371

Semana. (22 de 08 de 2017). Obtenido de 492724

informacion, A. d. (s.f.). (Comision de regulacion de comunicadores) Obtenido de MinTIC: http://colombiatic.mintic.gov.co/602/articles-6807_archivo_pdf.pdf

F.A. Villa, J.D. Velasquez, y P. Sanchez, "Control del sobreajuste en redes neuronales tipo cascada correlación aplicado a la predicción de precios de contratos de electricidad", *Revista Ingenierías Universidad de Medellín,* 14 (26), 2015. http://www.scielo.org.co/pdf/rium/v14n26/v14n26a11.pdf

M. Molina Cárdenas, P. Pedroza Barrios, K. M. Gaitán Moreno, J. F. Salgado Arismendy y M. C. Ordóñez Ávila, «Diseño y Construcción del Prototipo de un Brazo Robótico con Tres Grados de Libertad, como Objeto de Estudio,» Ingeniare, vol. 10, nº 18, pp. 87-94, 2015.

J.R. García-González, P.A. Sánchez-Sánchez y L. Salcedo Diaz, "Retos y desafíos de la democracia en Colombia: una revisión desde la academia", Espacios, v38 (38), 2017.

E. De La Hoz, L. Lopez, y L. Perez, "Modelo de gestión de relaciones con los clientes en empresas de consultoría", *Revista Investigación e Innovación en Ingenierías, vol. 5 (2), 2017.*

G. Peñaloza, "Una mirada desde la Didáctica de las Ciencias al concepto de visión del mundo", *Revista Educación y Humanismo*, vol. 17(29), pp. 308-320., 2015

H. Madrid Álvarez, "Marketing Algoritmico Y Marketing Heuristico, Una Cotroversia", Investigación e Innovación en Ingenierías, vol. 3, no. 1, 2015. DOI: https://doi.org/10.17081/invinno.3.1.2038

R. Cabeza, "Localización de Datos de Contactos Personales Utilizando Técnicas de Minería Web y Redes Sociales", Investigación e Innovación en Ingenierías, vol. 4, no. 1, 2016. DOI: https://doi.org/10.17081/invinno.4.1.2020