¿QUÉ TAL ESTA COLOMBIA EN CUESTIÓN DE CIBERSEGURIDAD?

VICTOR ANTONIO HOYOS BUITRON
CODIGO 2600940

ASESOR
JUAN MANUEL SILVA

UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD

ESPECIALIZACIÓN EN ADMINISTRACIÓN DE LA SEGURIDAD

BOGOTÁ, COLOMBIA

2015

Contenido

Introducción

La ciberdefensa, se puede ver desde diferentes perspectivas y las mismas dependen de la utilidad o del elemento a proteger; por ejemplo en el caso de las actividades militares y defensa de la nación, desde esta perspectiva se busca proteger información clasificada de los llamados “haker`s” ya que dicha información contienen entre otros operativos militares, información del gobierno etc. que no debe ser pública ya que en la medida en que pierda la protección, así mismo se pone en riego el éxito de las actividades que han de desarrollarse en tiempo futuro.

Por otro lado, si se ve la situación desde la perspectiva de los ciudadanos comunes, estos también están expuestos a ser víctimas de delitos cibernéticos, por ende, entre más publica sea su información más expuestos están, por ejemplo a ser víctimas de robos, cuando de alguna forma se hace pública su información respecto de actividades financieras o monetarias. En el caso de los niños, no es adecuado exponerlos para evitar que caigan víctimas de delitos como la pornografía infantil.

En términos generales, el acceso a la tecnología y la red van avanzando de la mano, ya que tienen una relación directamente proporcional; es decir, que en la medida en que avance la tecnología también avanza la facilidad de acceso a la red de la internet. Así las cosas, toda la población está expuesta, cada una en su estado de ser víctima de delitos cibernéticos y por ende toda la población debe contar con condiciones mínimas de ciberseguridad y tener conocimiento suficiente al respecto.

Bajo ese orden de ideas, en el presente estudio se busca comprender cuál es la situación de ciberseguridad en Colombia.

Objetivos

Objetivo general

Establecer la situación actual en Colombia respecto de la ciberseguridad.

Objetivos específicos

- Establecer desde la revisión bibliográfica que es la ciberseguridad y los demás términos que le acompañan.
- Aclarar las actividades de ciberseguridad que se desarrollan actualmente en el territorio nacional de Colombia.
- Mostrar si a juicio del autor si las medidas de ciberseguridad existentes en la actualidad son funcionales y suficientes para los delitos que se pueden desarrollar por medio de la red de internet y el uso de los diferentes dispositivos tecnológicos.

¿QUÉ TAL ESTA COLOMBIA EN CUESTIÓN DE CIBERSEGURIDAD?

En la actualidad la ciberseguridad es un tema de gran importancia ya que en la medida en que se desarrolla la tecnología, la información se difunde con mayor facilidad por medio de la red, y esta misma se maneja de forma casi uniforme por todo el globo terráqueo. Esa situación no solo facilita la comunicación derrumbando fronteras, sino que también el flujo de información permite a los delincuentes el acceso a la misma y facilita sus actividades ilícitas. Por tal razón es necesario implementar medidas de protección para toda la población que de alguna forma tienen acceso al internet.

Bajo ese orden de ideas, es necesario indicar que el ciberespacio según (Clarke, 2011) es conformado por todas las redes informáticas del mundo y todas las actividades que las mismas desarrollan y controlan, por medio de la red de internet. Pero entonces que es eso de la internet, en este caso se toma el concepto de (Vallejos, 2012) en el que se entiende que es una colección de miles de redes de computadoras. También se le conoce como la superautopista de la Información. En síntesis y a manera de explicación de estos dos conceptos se puede decir que el ciberespacio es la red y el internet es el medio por el cual se construye la misma como si fuese el ciberespacio el automóvil que se moviliza por las autopistas.

Debido al tráfico de información tan importante que se da atreves del ciberespacio, es necesario conocer que no todos los usuarios de estos servicios buscan un medio de comunicación eficiente cuando hay grandes distancias que recorrer, también están quienes buscan por medio de la red acceder a información confidencial de cualquier tipo, con el fin de lucrarse, pero no de la forma correcta si no por medio de la ejecución de los llamados delitos informáticos o ciberdelitos. Que según (Policia Nacional de Colombia, 2015) no es otra cosa que los delitos o actos

delictivos que se desarrollan a través de la red y se pueden clasificar según la misma fuente de la siguiente manera:

- **Claves programáticas espías:** conocidas como troyanos, o software espías, son empleadas para de alguna forma sustraer información en forma remota y física, preferiblemente aquella que le permita al delincuente validarse en el sistema bancario, suplantando a la víctima.
- **Estafas a través de subastas en línea:** se presentan en el servicio de venta de productos, generalmente ilícitos, en línea o en la red; se pueden encontrar celulares hurtados, software de aplicaciones ilegales, además puede ser una vía de estafa ya que se suelen incumplir reglas de envió y de calidad de los productos solicitados.
- **Divulgación indebida de contenidos:** son conductas originadas en el anonimato ofrecido en el internet y el acceso público sin control desde ciber cafés; entre ellas se encuentran él envió de correos electrónicos anónimos, con fines injuriosos o calumnias, amenazas y extorsiones.
- **Pornografía infantil en internet:** a través de foros, chats, comunidades virtuales, transferencias de archivos, entre otras modalidades, los delincuentes comercializan material pornográfico que involucra menores de edad.
- **Violación a los derechos de autor:** utilizando reproductores en serie, los delincuentes realizan múltiples copias de obras musicales, videogramas y software.
- **Piratería en internet:** implica la utilización de internet para vender o distribuir programas informáticos protegidos por las leyes de la propiedad intelectual.

Aquí encontramos la utilización de tecnología par a par, correo electrónicos; grupos de noticias, chat por replay de internet, orden postal o sitios de subastas, protocolos de transferencia de archivos, etc.

Los anteriores son los delitos más cometidos, aunque no son los únicos, pero son estos precisamente los que afectan a la mayoría de la población y es esa la razón por la que es necesario desde todas las dependencias implementar medidas de seguridad que impidan de alguna forma que los usuarios de las redes informáticas caigan víctimas de delitos. Para eso se relaciona a continuación la ciberseguridad en Colombia desde varios puntos de vista, como los usuarios, las empresas que ofrecen servicios de conexión a internet y las autoridades.

- Usuarios según (Heuré, 2014)

Aunque pueda parecer frustrante, la responsabilidad de proteger las informaciones que se transmiten y que se difunden en la red no corresponde a los desarrolladores de soluciones antivirus, aunque. Los antivirus instalados detectan los virus y pueden ayudar a resolver el problema en caso de ataque, pero el primer responsable de la cadena de seguridad es el propio usuario.

Cuando un consumidor resuelve clicar sobre el vínculo de un correo electrónico del que desconoce la procedencia o decide descargar un archivo en línea, él es responsable de su elección. A lo mejor su antivirus le previene o le alerta sobre el inminente peligro, pero no podrá bloquearlo. Así pues, el usuario es el eslabón inicial de la lucha contra la cibercriminalidad. Ahora bien, hasta este día continúa siendo vulnerable.

Para un ciudadano intermedio es difícil creer que puede caer víctima de la cibercriminalidad o que puede jugar un papel dentro de la ciberseguridad. Suele pensar que no importa a los criminales, que no posee ninguna información sensible y que su "cibercomportamiento" no influirá en el orden general. ¿Por qué? Porque tiene la costumbre de proteger sus bienes materiales, porque la información que hace circular por el ciberespacio no se considera todavía como algo que tiene que ser objeto de seguridad. La mayor parte del tiempo compartimos esas mismas ciberinformaciones oralmente con nuestros amigos o nuestros compañeros de trabajo. Cuando se trata de una foto, del importe de una factura o de una contraseña, nuestras informaciones circulan entre las personas de nuestro entorno; entonces, ¿por qué perder el tiempo en tomar medidas de seguridad en Internet?

Eso muestra que en efecto el usuario que es la principal víctima también es el que más ignora la situación de riesgo a la que está expuesto, generando así, que el mismo le habilite de alguna forma el acceso a los delincuentes a su máquina y por ende a su información.

- Empresas de telecomunicaciones

En el caso de las empresas de telecomunicaciones que prestan sus servicios en el territorio nacional, las mismas deben cumplir con las medidas que indica el Min Tic, en el (Consejo Nacional de Politica Economica y Social, 2011).

En esa medida cada una cuenta con herramientas diferentes en algún elemento, pero que cumplen prácticamente la misma función como lo describe (Movistar, 2015): “ha creado una solución que explora el ciberespacio en busca de información que permita generar alertas tempranas sobre situaciones e incidentes

que afectan la seguridad de la información de sus empresas, que pueden afectar el desarrollo normal de las operaciones de negocio; o atacar la reputación y la marca de los negocios de los clientes" eso en busca de generarle al usuario los siguientes beneficios:

- El servicio se presta en producción desde el momento de la contratación, y su puesta en marcha es rápida y ágil al prestarse éste desde la red.
- Externalización del problema: la lucha contra los ataques es un proceso que requiere tiempo y gran especialización de recursos. El SOC ofrece un servicio global 24x7 con experiencia contrastada, que trabaja para atajar y resolver estas situaciones que se pueden presentar en las empresas.
- Reducción del tiempo de vida de cada ataque y descubrimiento de información valiosa: Las últimas estadísticas del servicio muestran cómo se cierran un 83% de los casos en menos de 24 horas y un 22% de estos en menos de 12h.

Así las cosas, se puede decir que las empresas que prestan servicios de telecomunicaciones en Colombia están participando activamente en el proceso de protección a los usuarios, colaborando con las autoridades, con el fin de detectar a los ciberdelincuentes e imponerles los cargos jurídicos a los que haya lugar.

- Autoridades Colombianas contra la ciberdelincuencia

Las autoridades Colombianas, encabezadas por el Min Tic generaron un documento donde están comprendidas todas las actividades que se deben desarrollar respecto de lo que es la ciberdefensa y ciberseguridad (Consejo Nacional de Politica Economica y Social, 2011). "*Dicho documento busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar*

una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país.

Adicionalmente, recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema.

La problemática central se fundamenta en que la capacidad actual del Estado para enfrentar las amenazas cibernéticas presenta debilidades y no existe una estrategia nacional al respecto. A partir de ello se establecen las causas y efectos que permitirán desarrollar políticas de prevención y control, ante el incremento de amenazas informáticas. Para la aplicabilidad de la estrategia se definen recomendaciones específicas a desarrollar por entidades involucradas directa e indirectamente en esta materia. Así lo ha entendido el Gobierno Nacional al incluir este tema en el Plan Nacional de Desarrollo 2010-2014 "Prosperidad para Todos", como parte del Plan Vive Digital."

Ahora bien es importante reconocer que tanto esfuerzo poco a poco ha ido generando fruto, y el mismo se hace evidente en un artículo de la revista (Portafolio, 2015) donde: "Colombia está entre los mejores países del mundo en manejo de ciberseguridad de acuerdo con el ranking global de la UIT, que ubica al país en el quinto lugar en el ranking de las Américas por encima de Chile y México y ocupa el noveno lugar en el ranking mundial con países como Francia, España, Egipto y Dinamarca."

Todo este esfuerzo tiene fundamento en los antecedentes que aunque hay un sistema de ciberseguridad todavía se sigue presentando ese tipo de inconvenientes como dice (Tecnosfera, 2014) "Seis millones de personas fueron víctimas de alguna modalidad de crimen digital en Colombia el año 2013", según la firma de seguridad

digital Norton. se calcula que el costo de los delitos informáticos en 2013 alcanzó 874 mil millones de pesos.

Bajo ese orden de ideas en el mismo estudio se encontró que el robo de identidades digitales, datos bancarios y el matoneo digital ocupan los principales puestos entre los crímenes más recurrentes. Entonces se puede decir que cuatro de cada 10 consumidores de teléfonos inteligentes han sufrido de algún delito digital. La vulnerabilidad de los colombianos ante los ciberdelincuentes quedó figurada en su máxima expresión, cuando se reveló que hasta las cuentas de correo del presidente Santos fueron hackeadas.

Por esa razón y en respuesta al riesgo, las autoridades organizaron los medios para dar respuesta suficiente y contener a los cibercriminales y para eso en apoyo con el sector privado y las universidades, se forman centros de innovación y excelencia, que harán investigación y desarrollo de herramientas para mejorar la ciberseguridad o atenderán casos de ciberdefensa.

Y parte importante de las nuevas funciones de labor que tiene la Agencia Nacional de Seguridad Cibernética son las de crear un nuevo esquema de reporte y monitoreo obligatorio de sucesos de seguridad informática tanto a nivel público como privado. Por lo tanto, las empresas prestadoras del servicio de acceso a internet, así como los operadores de telecomunicaciones, estarán en la obligación de entregar informes de tráfico y de actividad con carácter preventivo. Con este nuevo sistema de ciberseguridad y ciberdefensa, Colombia busca además entrar al Convenio de Budapest, un pacto firmado entre la Unión Europea, Estados Unidos, Canadá y Japón, el cual ha desarrollado un marco penal y regulatorio único para la prevención y lucha de los delitos cibernéticos.

Dentro de dicho marco de ciberseguridad se encuentra el proyecto de acuerdo (037, de 2013): *"Por medio del cual se establece la Estrategia de Ciberseguridad para enfrentar ciberdelitos y amenazas contra el Distrito Capital"* en el cual se exponen los siguientes motivos:

- *Ataque masivo de hackers contra la Registraduría.*

Conforme lo cita la fuente de El Universal, "Pese a que un informe del Cuerpo Técnico de Investigación de la Fiscalía (CTI), elaborado en mayo de 2010, determinó que hubo un ataque masivo de hackers al programa informático de la Registraduría Nacional durante las elecciones parlamentarias del 2010, que a la postre hizo colapsar al sistema de datos; la Fiscalía decidió archivar la investigación por considerar que las pruebas no eran suficientes. Dichos ataques provinieron del Ministerio de Defensa, el Departamento Administrativo de Seguridad (DAS) y, en especial, desde la Policía Nacional". Citó la fuente. Otros medios, denuncian casos similares así:

- *Se confirma el primer ataque de 'hackers' a la Registraduría*

Según cita el periódico El Espectador, "La Registraduría Nacional del Estado Civil confirmó el primer ataque de 'hackers' al sitio web de la entidad. El registrador Carlos Ariel Sánchez dió a conocer que en días pasados las consultas de bases de datos del Censo Electoral y la de jurados de votación, intentaron ser bloqueadas por Anonymus. Sin embargo, las operaciones de los 'hackers' no fueron tan exitosas pues se logró detectar a tiempo las direcciones IP desde donde se dieron los ataques y se pusieron en conocimiento de la Policía y de la Fiscalía".

Por otro lado, se han evidenciado con los recientes ataques a la Ciberseguridad en Bogotá, la fragilidad y las falencias que en esta materia se

presentan en el Distrito. Como se sustenta en el presente Proyecto de Acuerdo, Colombia y especialmente el Distrito Capital, presenta uno de los más altos índices de vulnerabilidad a ciberataques en América Latina, y lo peor, la tendencia de ataques cibernéticos es exponencialmente creciente al corto, mediano y largo plazo. Esta preocupante situación, exige medidas urgentes que permitan mitigar efectos, no solo en contra de la infraestructura de la ciudad, de la información del Distrito Capital, sino de la seguridad, integridad, vida y honra de los bogotanos".

En Colombia es muy preocupante la vulnerabilidad en cuanto a ciberseguridad, más aun cuando en el Distrito Capital se concentra más de la mitad del control de los sistemas de información del país. Por ello se evidencian algunos serios incidentes de ciberataques que a continuación se mencionan:

Según la revista Dinero**,** un artículo publicado en Septiembre de 2012, muestra que "Colombia es el segundo país más sensible a ciberataques. Las computadoras de un 35% de usuarios en la Región, fueron atacadas por lo menos una vez mientras navegaba por la web. Karpesky Lab informó que su análisis sobre la naturaleza del delito cibernético en América Latina, que examina los primeros nueve meses de 2012, reveló que las computadoras de un 35% de usuarios en la Región fueron atacadas por lo menos una vez mientras navega por la web". Se indica que los países más afectados son Chile, Colombia y Panamá ya que están en el grupo de alto riesgo (casi un 40% de máquinas atacadas mientras están en línea).

Por otra parte, según la revista Enter, "Colombia es subcampeón mundial en fraude y uno de los más vulnerables a ciberataques. La reputación empresarial de Colombia, que ha mejorado en los últimos años, sufrió un revés. A la lista de problemas que agobian al país, se suma que ahora se clasifica como el segundo en

todo el mundo en fraudes empresariales. Esto refleja un pésimo nivel de la seguridad en las empresas, tanto física como informática".

En otro episodio de ciberdelincuencia se encontró que la Empresa de Acueducto de Bogotá sufre un ataque en Noviembre de 2012. Se reveló que la página web de la Empresa de Acueducto y Alcantarillado de Bogotá fue atacada, según fuente publicada por CMI, donde se informó "Un hacker ataca la página de EAAB**.** El sitio web donde se publican los procesos licitatorios que adelanta la Empresa de Acueducto de Bogotá EAAB – ESP ha sido víctima de ataque informático.

Esta situación se presenta tras la publicación del proceso contractual por 80 mil millones, para cumplir con compra de vehículos para la gestión y operación del servicio público de aseo, a partir del 18 de diciembre de 2012. El ataque informático completó tres días y se registra únicamente en la página oficial de contrataciones de la Empresa de Acueducto y Alcantarillado de Bogotá que hace parte del sitio web de la entidad www.acueducto.com.co."

En el mismo sentido, y referente al tema de los semáforos en Bogotá, se encontró que: Alcalde Petro duda de agresiones cibernéticas a la red de semáforos de Bogotá, manifestando su preocupación en cuanto a que sospechaba que la red de semáforos de la capital pudiera haber sido atacada para alterar algunos semáforos de la ciudad. Esta situación prende las alarmas en el Distrito, teniendo en cuenta que la Administración no ha tomado las medidas necesarias a fin de prevenir y contrarrestar este tipo de ataques cibernéticos.

Como estos son muchos los casos que están registrados por medio de las diferentes formas de denuncia existentes, por eso a continuación se muestra la

evolución de este tipo de inconvenientes en el distrito capital, donde se puede ver que hay un crecimiento exponencial en las amenazas de internet. (ver ilustración 1)

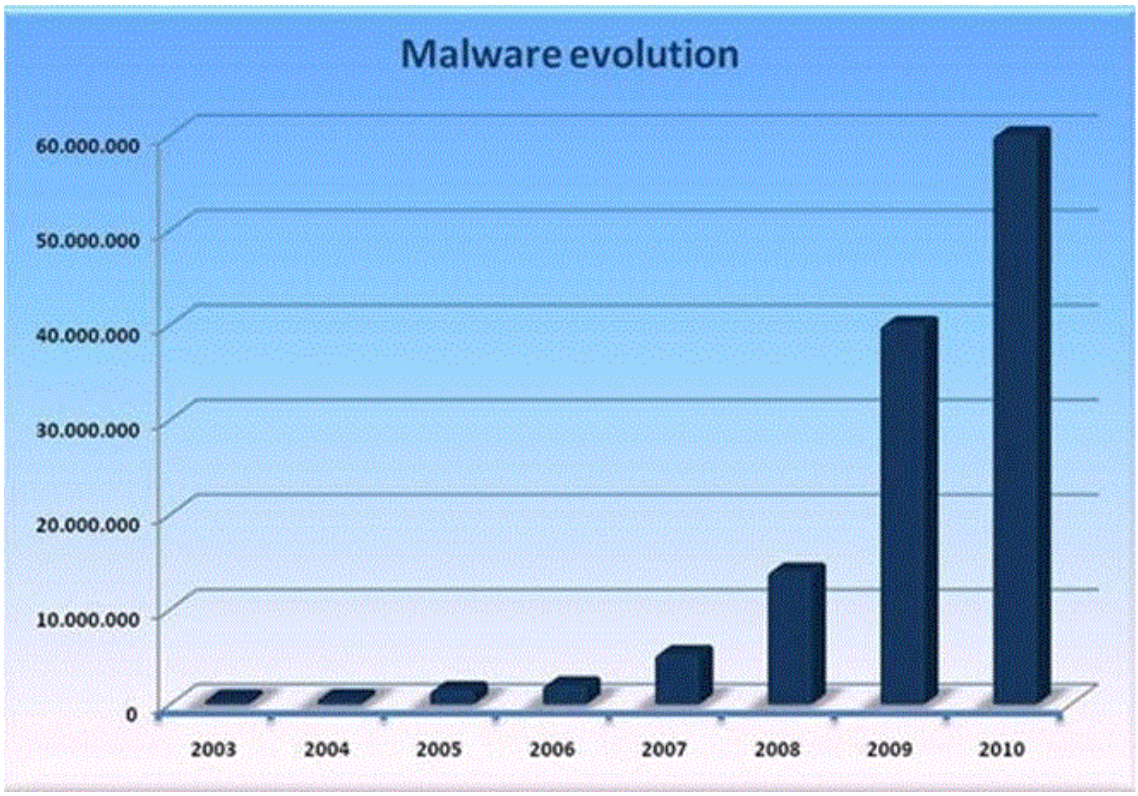

Ilustración 1 Proyección de Crecimiento de las amenazas en Internet en Bogotá.

Fuente: acuerdo 037 de 2013

Con toda la informacion anerior es pocible establecer que en effecto Colombia es un pais suceptble de ataques ciberneticos debido a que por un lado, la poblacion no tienene ni la educasion ni la cultura suficiente para autoprotegerse, convirtiendose casi de forma automatica en victimas de dicho delito, permitiendo el acceso de personas indeseadas a su informacion personal como lo son: claves, fechas, facturas y demas datos que peuden de alguna manera ser utilizados para hacer efectivo el delito.

Por eso, es importante reconocer el merito que corresponde a los esfuerzos que hace el gobierno, no solo en cuestion de infraestructura y centros de proteccion,

por medio de las universidades, las empresas de telecomunicasiones y la normatividad, si no tambien en cuestion de capacitacion y concientizacion de la poblacion, que incluye a todos y todas las personas que tengan acceso a los sitemas de comunicasion, ya que todos se encuentran expuestos, de tal manera, que los niños, por el riesgo de ciberabuso, que puede llegar hasta la pornografia infantil y el ciberbulling, en los adultos las estafas, por medio del acceso a la informacion financiera y las empresas por filtro de informacion calificada y de fraude. Entre otros muchos. Y el cambio a sido significativo, ya que los antecedentes datan de el periodo anterior a la implementacion de las estrategias gubernamentales que han surtido efecto poniendo al pais en la actualidad en una buena hubicasion en las estadisticas que se mensionaron al comienzo de este documento.

Conclusiones

A partir de la información y reflexión anterior se llegó a las siguientes conclusiones:

- La principal víctima de los delitos cibernéticos es el usuario ya que su conducta de navegación en la red lo pone en riesgo de forma casi automática y mientras los mismos no tomen conciencia de dicha situación no habrá manera de protegerle por completo.

- El gobierno con toda su estructura en efecto están haciendo la tarea que les corresponde con el fin de contener a los ciberdelincuentes y su proceder ilícito, pero como todo es un proceso todavía hay cosas por hacer. Sin embargo se puede decir que van por un buen camino.

Bibliografía

037, n. (de 2013). *consulta la norma*.

Clarke, R. &. (2011). *Guerra en la red, los nuevos campos de batalla.* Barcelona.: Planeta.

Consejo Nacional de Politica Economica y Social. (14 de 07 de 2011). *Mintic*. Obtenido de COMPES: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Heuré, J. (18 de 11 de 2014). *cafebabel*. Obtenido de http://www.cafebabel.es/articulo/ciberseguridad-que-papel-juegan-los-usuarios.html

Movistar. (12 de 10 de 2015). *Movistar*. Obtenido de http://www.movistar.co/web/empresas/soluciones-digitales/seguridad/ciberseguridad

Policia Nacional de Colombia. (01 de 12 de 2015). *Delitos informaticos*. Obtenido de Policia Nacional de Colombia: http://www.policia.gov.co/portal/page/portal/UNIDADES_POLICIALES/Direcciones_tipo_Operativas/Direccion_Seguridad_Ciudadana/Planes_de_Seguridad/Recomendaciones_de_seguridad/delitos_informaticos

Portafolio. (08 de 01 de 2015). *portafolio.co*. Obtenido de http://www.portafolio.co/economia/colombia-repunta-manejo-ciberseguridad

Tecnosfera. (11 de 07 de 2014). *El tiempo*. Obtenido de http://www.eltiempo.com/tecnosfera/novedades-tecnologia/gobierno-prepara-plan-estatal-de-ciberseguridad/14233838

Vallejos, O. (2012). *INTRODUCCION A INTERNET.* buenos aires:

http://ing.unne.edu.ar/pub/internet.pdf.