Type of the Paper (Article)

Ciberseguridad y Ciberdefensa en Colombia

Rubén Darío Laverde Castillo[1], Miguel Hernández Bejarano[2],*

[1] Fundación Universitaria Los Libertadores; rdlaverdec@libertadores.edu.co
[2] Fundación Universitaria Los Libertadores; mhernandezb@libertadores.edu.co
* Correspondence: rdlaverdec@libertadores.edu.co

Received: 11/10/2020; Accepted: 03/12/2020; Published: 31/12/2020

Abstract: En un mundo que se encuentra en constante cambio y donde de igual manera lo hacen las tecnologías, información, dispositivos y delitos, los cuales han sufrido un gran cambio en el transcurso de los años, esta evolución ha aumentado en gran medida el entorno de la ciberdefensa y la ciberseguridad, logrando así una gran evolución y crecimiento constante, presentando de esta manera mayores desafíos, cada vez con mayor grado de dificultad. Actualmente millones de personas en el mundo utilizan los servicios y la información que les brinda el ciberespacio al igual que las compañías y es ahí donde se debe asegurar y llevar acciones de vigilancia y análisis masivos de datos, ese es el motivo de este articulo y con la intención de mostrar las amenazas a las que se puede enfrentar una empresa en cuanto a ciberseguridad y algunos posibles métodos para impedir estas amenazas.

Keywords: Ciberseguridad, Ciberdefensa, Inteligencia, Estrategias de Seguridad Nacional, ciberespacio.

1. Introducción

Es necesario mostrar algunas estrategias de ciberdefensa y conocer la evolución de la ciberdefensa, su estructura y cambio a lo largo del tiempo, para poder manifestar de esta manera una problemática que se vive en este sector tan vulnerable y lleno de tantos riesgos que puede conllevar la utilización continua de aparatos electrónicos y el internet, llegando así a un punto en el cual se pueda aclarar el peligro que se corre en cuanto a ciberseguridad, la importancia de su utilización y como evitar riesgos innecesarios para poder mantener a salvo una empresa, toda su información y a sus funcionarios.

El desarrollo de esta problemática en seguridad se realizó con el interés de conocer porque es importante y de igual manera ver el crecimiento e implementación de los mecanismos de ciberdefensa, también para poder conocer los riesgos que puede tener la información de una entidad.

Es necesario implementar algún mecanismo de seguridad en entidades no solo gubernamentales sino también en entidades privadas, donde se tenga un alto flujo de información de carácter privado como contraseñas, cuentas bancarias etc. Para así poder disminuir un poco más las posibles vulnerabilidades que se puedan generar y su impacto.

1.1 La ciberseguridad

Se puede explicar cómo la capacidad de un estado u organización para disminuir los peligros cibernéticos al que pueden estar expuestos los ciudadanos, en sectores vulnerables como transacciones financieras, protección de información y propiedad intelectual. [1]

1.2 La ciberdefensa

Se define como la capacidad del estado para prevenir y contrarrestar cualquier incidente o amenaza cibernética que afecte la soberanía nacional, en el uso de la internet con fines terroristas, actos de espionaje y guerra cibernética, en los últimos años la ciberseguridad y ciberdefensa han cobrado mayor interés en la agenda política global, y gracias a que las tic se vuelven cada vez más esenciales para el desarrollo social y económico, crece la importancia de la infraestructura tic y las amenazas cibernéticas evolucionan a un ritmo acelerado. [1]

Para poder continuar es necesario hacer una aclaración entre estos conceptos y sus diferencias, la ciberdefensa va encaminada a la protección y seguridad de una nación, usada por sus fuerzas militares para así poder salvaguardar su integridad y poder neutralizar todas las amenazas a las que este expuesta, por otra parte la ciberseguridad nos muestra todas aquellas acciones que se pueden llevar a cabo no solamente en un estado sino también en el sector privado, para poder mantener una seguridad que permita minimizar ataques cibernéticos que pueda sufrir una persona o cualquier tipo de entidad.

1.3 El ciberespacio

El ciberespacio es una zona artificial diseñada por los sistemas de información y telecomunicaciones, esta principalmente constituido por las redes de cómputo y telecomunicaciones, interconectados directa o indirectamente a nivel mundial. Dicho esto podemos decir que el ciberespacio no es únicamente internet, es más que los mismos sistemas y equipos, hardware y software e incluso más que los usuarios, se trata de una nueva zona, un espacio con sus propias leyes, que a diferencia de los demás espacios ha sido creado por el hombre para ayudarlo en su desarrollo y evolución. [2]

La utilización de los servicios y la información que puede proveer el ciberespacio genera una gran dependencia, por ejemplo, en Colombia para el año 2010 solamente el 2% de la población tenía acceso a internet, luego en el 2016 se llegó a un 79% de la población que tenía acceso a este medio. [3]

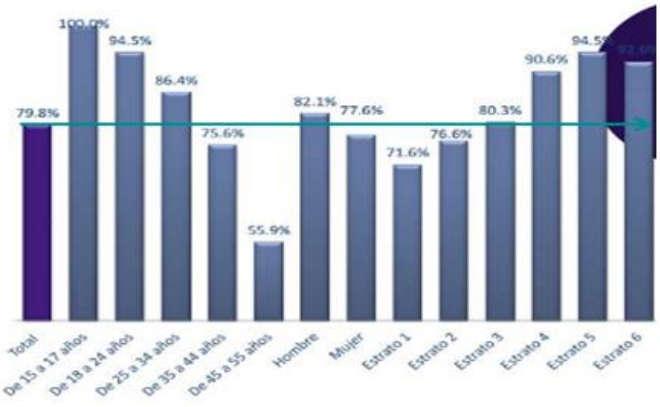

Fig. 1. Usuarios de internet en Colombia 2016. [3]

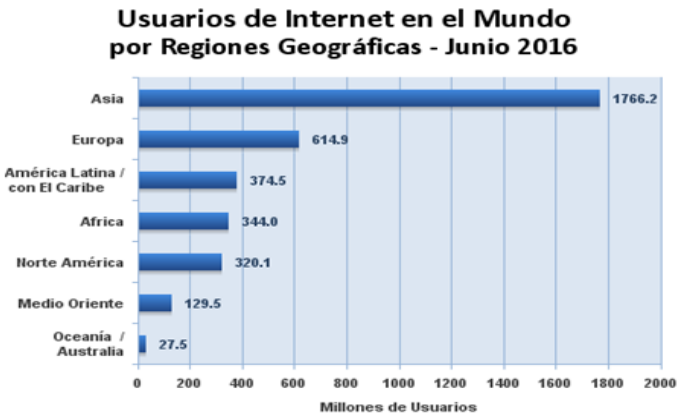

Fig. 2. Usuarios de internet en el mundo 2016 [3]

Actualmente el número de usuarios a aumentado considerablemente y con eso lo han hecho también las amenazas cibernéticas que pueden afectar a la población general y a las organizaciones, en los últimos años múltiples amenazas han surgido las cuales atacan la infraestructura interconectada, la cual tiene una vulnerabilidad muy alta y el peligro se encuentra en que si son atacadas se puede no solo llegar a paralizar una compañía sino también a todo un país pues se puede atacar una central eléctrica dejando un país y corriente eléctrica o atacar las fuentes principales de internet dejándolo incomunicado.

Por ejemplo en Colombia desde el año 1999 se han reportado numerosos ataques a dominios colombianos, en el año 2012 el sitio http://attrition.org/ reporto 50 ataques a diferentes sitios oficiales, el número de ataques aumento exponencialmente con el tiempo, en el 2016 se reportaron más de 50 ataques solo en el mes de agosto, dentro de estos ataques algunos fueron: espionaje, robo, sabotaje de servicios, terrorismo informático, operaciones de información, además de muchas más. [3]

Gracias a los países industrializados que se encuentran en la cima de la tecnología, que buscan obtener el dominio del ciberespacio, bien sea para generar ataques como para la defensa, y para ello aparecen los ciberguerreros los cuales pueden emplear distintos métodos de acceso a un sistema para así poder hacerse de su información.

Ahora bien con el desarrollo y crecimiento del internet de las cosas y gracias al uso de una mayor cantidad de dispositivos conectados a una red, la cual puede terminar haciendo parte de una red corporativa, se incrementaría considerablemente el riesgo que la información confidencial de una compañía puede correr, pues al estar tan expuesta no pasara desapercibida ante ciberatacantes atentos a cualquier descuido de los usuario.

1.4 Ciberguerreros como actuan

Los ciberguerreros son todos aquellos individuos que gracias a sus conocimientos y estudios son capaces de diseñar ciberarmas y también programas, algunas de sus herramientas y métodos de atacar son:

Stuxnet. Es un programa malicioso que permite la intrusión en los sistemas que controlan infraestructuras como oleoductos, plantas nucleares o fuentes eléctricas, con el fin de sabotear el funcionamiento de esas infraestructuras, que en el caso de un oleoducto se puedan producir daños que permitirían la perdida y derrame del petróleo o si se trata de una planta nuclear incrementar la temperatura de los silos nucleares generando fallas que podrían causar una explosión o dejar a todo un país sin electricidad. [4]

DDos. DDos (Distributed Denial of Service) son los ataques más comunes que puede tener una página web, la cual consiste en saturar los servidores web para hacer que estos colapsen, para esto se utilizan computadores que están infectados con virus (botnets) haciendo que se cree una red de computadoras infectadas, los usuarios no se dan cuenta que hacen parte del ataque. [4]

Botnets. Son robots de la red, utilizadas para dirigir ataques DDos, este tipo de ataque se da cuando un correo basura o spam es abierto por una persona, al estar infectado de virus hace que la máquina este a merced de los hackers o ciberguerreros para así poder espiar instituciones gubernamentales o corporaciones. [4]

Zeus. Es un virus mejor conocido como troyano que se encarga de entrar a las computadoras de los funcionarios con el fin de obtener contraseñas, información bancaria, con el fin de realizar suplantación y robos a cuentas bancarias y sabotaje a las compañías. [4]

También es posible encontrar algunas modalidades entre las cuales podemos encontrar:

Suplantación de proveedores. En este tipo de ataque los ciberdelincuentes toman la identidad de una empresa reconocida, logrando comunicaciones bien sea por medio de correos electrónicos o vía telefónica, también es posible que usen facturas por cobrar o contratos falsos y de esta manera lograr adelantar pagos de mercancía que aún no han sido entregados o pago de saldos pendientes. [5]

Suplantación de clientes. En esta modalidad es normal suplantar entidades del gobierno o empresas reconocidas, para así realizar pedidos a empresas que no poseen una fuerte seguridad y de esta manera generar pedidos en su nombre logrando plazos de pago de 15 a 30 días, tiempo que utilizaran para huir sin dejar rastro. [5]

Para estas dos últimas modalidades de ciberdelitos podemos encontrar algunas señales de alerta como pueden ser:

Recibir correos donde los supuestos proveedores solicitan adelantos del pago o pedidos de mercancía.

Por medio del uso de correos electrónicos a las víctimas se les notifica el cambio de cuentas bancarias o lugar de entrega de la mercancía, también es normal el uso solamente de teléfonos celulares y nunca por medio de teléfonos fijos.

En muchas ocasiones se utilizan correos como medio de actualización de datos dando nuevos teléfonos y direcciones, para eso son utilizados correos gratuitos de Yahoo, Hotmail o Gmail y no con dominio como @empresa.com o con el nombre de la empresa.

También se pueden generar cambios de último momento dando nuevas cuentas, direcciones o alargamiento en el tiempo de pago de mercancías. [5]

También existen un mínimo seis vulnerabilidades importantes en el diseño mismo de internet las cuales pueden ser:

Enrutamiento entre ISP (Internet Service Provider) o proveedor de servicio de internet conocido como protocolo de puerta de enlace o (BGP Border Gateway Protocol).

En internet casi todo lo que se hace está disponible sin codificar.

Capacidad lanzar de manera rápida tráfico de datos maliciosos creado para atacar los computadores.

Es una gran red con características de diseño descentralizado.

El sistema de direcciones que es utilizado para llegar a una ubicación determinada en la red.

La ICANN o la organización internacional no gubernamental conocida como Corporación de Internet para la Asignación de Nombres u Números. [6]

También es posible clasificarlos por el modo de operación del atacante. Existen malware cuyo principal objetivó al momento de atacar es alterar el funcionamiento normal del computador sin el consentimiento del usuario. El modo habitual de trabajo de estos malware es remplazar archivos

ejecutables por otros infectados y su daño va desde la destrucción de datos almacenados en el computador o solo generar molestias al momento de usarse el computador. [7]

- Worms
- BOTs
- Adware
- Cookies
- Phishing
- Ingeniería social
- Denegacion de servicio
- Spoofing: de DNS, de IP, de DHCP. [7]

Software y hardware. También es necesario tener en cuenta la importancia del software y el hardware en el ciberespacio, pues con la ayuda de estos es posible controlar los dispositivos que son utilizados para conectarse al ciberespacio y es a causa de las fallas que pueden presentar estos sistemas que los ciberguerreros, hacker y demás delincuentes pueden llegar a ocasionar daños, los principales creadores del software que utilizan estos dispositivos son Microsoft, Oracle, IBM y Apple además de otras compañías, llegando a afirmar que el software es el intermediario entre el usuario y la maquina haciendo que la maquina realice las intenciones del usuario. [6, pp. 124-156]

2. Muestra de redes detectadas y en operación de un monitorea en tiempo real el 30 de octubre 2016

Con la ayuda de la página web www.trendmicro.com es posible observar la cantidad de servidores activos durante los últimos 4 días mostrando también los ordenadores que fueron víctimas durante ese mismo periodo de tiempo.

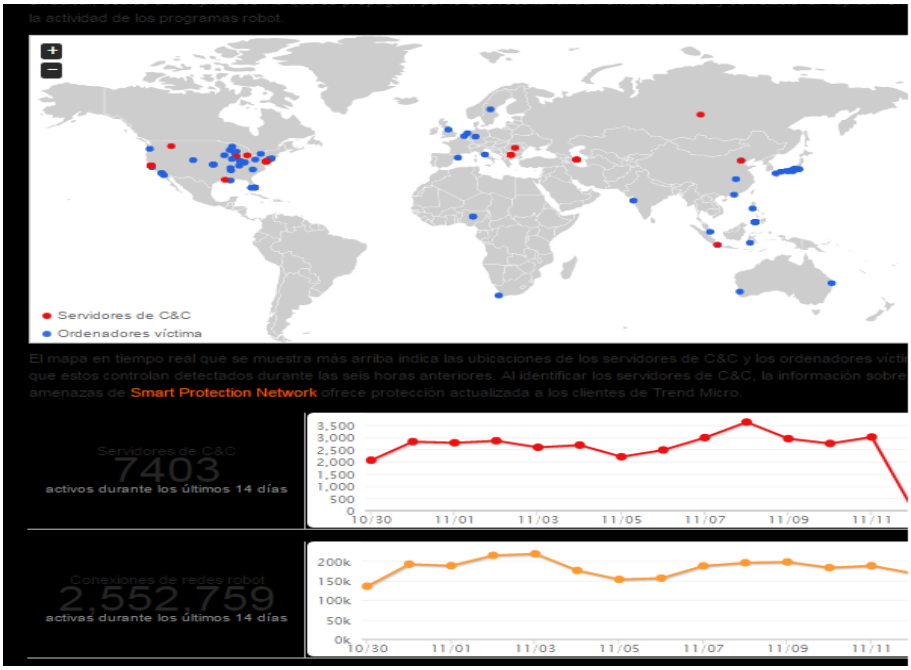

Fig. 3. Computadores atacados [8].

También permite la recopilación de más información concerniente a ataques la cual se presentara a continuación:

2.1 Actividad de las amenazas actuales

Blog destacado

blog.trendmicro.es

Últimas publicaciones

¡2014: qué año fue!
25 FEB, 2015

Arid Viper: Ciberconflicto Gaza contra Israel
19 FEB, 2015

Trend Micro alerta de un nuevo exploit de día cero en Adobe Flash
03 FEB, 2015

Economía sumergida

Activo	Valor en el mercado negro
Pasaporte/Certificado de residencia (documento escaneado)	20 $
Tarjeta de crédito (ambas caras, como documento escaneado)	25-30 $
Carnet de conducir (documento escaneado)	20 $
Certificado de residencia (documento escaneado)	10 $
Otros documentos originales (documento escaneado)	Desde 4 $
Tarjetas de crédito de EE.UU.: USA/Master Card/VISA	1 $/unidad
Tarjeta de crédito: Dinamarca, Grecia, Irlanda, Letonia, Holanda, Noruega, Suecia, Canadá	3 $/tarjeta
"Servicio de introducción" de información sobre la tarjeta	5 $
Cuentas de PayPal pirateadas	30% del saldo actual en la cuenta de PayPal

Fig. 4. Amenazas [8]**.**

2.2 URL y spam maliciosos

La siguiente imagen mostrara las vulnerabilidades presentadas por los principales proveedores, clasificados por el número de vulnerabilidades presentadas.

Las diez principales vulnerabilidades

Los diez principales proveedores clasificados por el número de vulnerabilidades distintas comunicadas.

Puesto	Proveedor	Vulnerabilidades comunicadas el T3 de 2012	Proveedor	Vulnerabilidades comunicadas el T2 de 2012
1	Apple	163	Oracle	97
2	Moodle	93	Linux	76
3	Google	72	Google	74
4	Oracle	71	Microsoft	55
5	Mozilla	57	Mozilla	48
6	Cisco	55	Cisco	45
7	IBM	53	IBM	37
8	Ffmpeg	53	Adobe	27
9	Adobe	42	Apple	26
10	Microsoft	35	HP	24

Fig. 5. SPAM maliciosas [8]**.**

2.2.1 Las diez principales URL maliciosas

También es posible encontrar las principales URL maliciosas encontradas durante ese periodo de tiempo.

Las 10 principales URL maliciosas bloqueadas por la infraestructura Trend Micro™ Smart Protection Network™ en el T3 de 2012

Puesto	URL maliciosa bloqueada	Descripción
1	trafficconverter.biz:80/4vir/antispyware/loadadv.exe	Distribuye malware, especialmente variantes de DOWNAD.
2	trafficconverter.biz:80/	Distribuye malware, especialmente variantes de DOWNAD.
3	www.funad.co.kr:80/dynamic/adv/sb/searchnqpopu.html	Introduce riesgos de seguridad en sistemas y/o redes comprometidos.
4	deepspacer.com:80/y2x8ms42fge0otk4y jhmzwu4ztu5y2e4mtfjngewztqxnjmyodczfdmxm a==	Aloja URL maliciosas registradas a nombre de un creador de spam conocido.
5	tags.expo9.exponential.com:80/tags/burstmediacom/audienceselectuk/tags.js	Participa en la distribución de software malicioso.
6	www.trafficholder.com:80/in/in.php	Sitio con tráfico conocido por distribuir malware.
7	mattfoll.eu.interia.pl:80/logos.gif	Distribuye troyanos.
8	www.funad.co.kr:80/dynamic/adv/sb/searchnq_popu.html	Introduce riesgos de seguridad en sistemas y/o redes comprometidos.
9	96.43.128.194:80/click.php	Distribuye troyanos.
10	am10.ru:80/code.php	Aloja adware y mensajes emergentes que redireccionan a sitios de phishing.

Fig. 6. URL maliciosas [8]**.**

2.2.2 Las diez principales ip maliciosas

Los diez principales dominios de IP maliciosos

Los 10 principales dominios maliciosos bloqueados por la infraestructura Trend Micro™ Smart Protection Network™ en el T3 de 2012

Puesto	Dominios de IP maliciosos bloqueados	Descripción
1	trafficconverter.biz	Distribuye malware, especialmente variantes de DOWNAD.
2	www.funad.co.kr	Introduce riesgos de seguridad en sistemas y/o redes comprometidos.
3	deepspacer.com	Aloja URL maliciosas registradas a nombre de un creador de spam conocido.
4	tags.expo9.exponential.com	Participa en la distribución de software malicioso.
5	bembed.redtube.comr	Distribuye malware y troyanos a través de vídeos.
6	dl.baixaki.com.br	Distribuye malware.
7	www.trafficholder.com	Sitio con tráfico conocido por distribuir malware.
8	oscex-en.url.trendmicro.co	Error en la dirección del sitio Web de la suite de seguridad Trend Micro OfficeScan.
9	mattfoll.eu.interia.pl	Distribuye troyanos.
10	www.luckytime.co.kr	Aloja malware.

Fig. 7. IP maliciosas [8]**.**

2.2.3 Los diez creadores principales de spam

Los diez principales creadores de spam

Los 10 principales países emisores de spam en el T1 de 2012

Puesto	País
1	Arabia Saudí
2	India
3	Turquía
4	Estados Unidos
5	Perú
6	Brasil
7	Corea del Sur
8	Vietnam
9	Colombia
10	China

Fig. 8. Creadores de SPAM. [8]**.**

2.2.4 Las diez principales crimeware

Los diez principales crimeware

Los diez principales crimeware bancarios y relacionados del T2 de 2011

Puesto	Nombre de detección del crimeware
1	MAL_BANKER
2	BKDR_QAKBOT.SMG
3	BKDR_PAPRAS.SME
4	TROJ_SPYEYE.SMEP
5	MAL_BANKER2
6	MAL_BANKER11
7	WORM_QAKBOT.QRZ
8	BKDR_QAKBOT.SMC
9	TSPY_BANKER.ES
10	WORM_QAKBOT.BS

Fig. 9. CRIMEWARE [8]**.**

3. Entidades encargadas de la ciberdefensa y la ciberseguridad en Colombia

3.1 Ministerio de Defensa Nacional

El objetivo del Ministerio de Defensa (Mindefensa) es ayudar a la protección de la democracia, mediante la utilización de la seguridad y la defensa, además de la aplicación adecuada y focalizada de la fuerza y desarrollo de capacidades que salvaguarden la integridad de la nación. [9]

Según el decreto 1512 de 2000 art 5, también debe participar en el desarrollo y ejecución de políticas de defensa y seguridad nacional para garantizar la soberanía nacional, la integridad territorial y la aplicación de las condiciones necesarias para el derecho de libertades públicas y asegurar que los habitantes de Colombia vivan en paz. [10]

Con esta información es fácil comprender que esta institución es la encargada de ejecutar y desarrollar todos los aspectos concernientes a la ciberseguridad y ciberdefensa en Colombia, y con la ayuda de las fuerzas militares y la policía se encargan de la defensa de la nación.

3.2 Ministerio de Tecnologías de la Información y las Telecomunicaciones

Según la ley 1341 de 2009 o ley de TIC, es la que se especializa en plantear, adoptar y fomentar las políticas y proyectos del sector de las tecnologías de la información y las comunicaciones. [11]

Debe encargarse de incrementar y facilitar el uso de las tecnologías de la información y las comunicaciones, además de sus beneficios para todos los habitantes del territorio nacional, promoviendo el uso efectivo y apropiado de las TIC, con el uso de políticas y programas para mejorar la calidad de vida de todos los colombianos y el desarrollo del país. [12]

3.3 Comando Conjunto Cibernético de las Fuerzas Militares

Dependencia de las fuerzas militares que se encarga de coordinar la respuesta a incidentes o ataques que afecten la seguridad nacional. Los principales objetivos de esta dependencia son:

- Analisis forense.
- Operaciones de ciberdefensa.
- Operaciones de inteligencia.
- Auditorias y evaluaciones de seguridad.
- Aseguramiento de portales FF.MM.

- Capacitación especializada en ciberseguridad y ciberdefensa. [13]

3.4 Centro Cibernético Policial

Es la dependencia de dirección de investigación criminal INTERPOL y se encarga de programas, proyectos, desarrollo de estrategias y todas las actividades necesarias para la investigación criminal de delitos que afectan la seguridad de la información y los datos. Los principales objetivos de esta dependencia son:

- La implementación del centro cibernético policial.
- Respuestas en línea a incidentes de ciberseguridad.
- Coordinación internacional Interpol-Europol.
- Atención de incidentes informáticos DIJIN.
- Implementación de equipos de respuesta a incidentes informáticos de la policía nacional.
- Laboratorios móviles de informática forense.
- Laboratorios de investigación de malware (sector bancario).
- Analisis forense a equipos.
- Atención, judicialización de incidentes cibernéticos.
- Unidad de investigación tecnológica UDITE. [14]

3.5 Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT)

Tiene El compromiso de regularizar la ciberseguridad y la ciberdefensa nacional la cual está estipulada dentro de la gestión de defensa y seguridad del ministerio de Defensa Nacional, cuyas labores pertenecen a la coordinación necesaria para el resguardo del estado colombiano frente a acontecimientos de ciberseguridad que comprometan la integridad nacional. Los objetivos de esta entidad son:

- Coordinar y asesorar a entidades tanto de nivel público como privado, ante incidentes informáticos.
- Ofrecer servicios de prevención ante posibles amenazas informáticas contra la nación.
- Actúa como punto de contacto internacional.
- Promover el desarrollo de capacidades, así como la creación de sectores para la gestión operativa de los incidentes de ciberseguridad.
- Promover y desarrollar procedimientos, y guías de buenas prácticas y recomendaciones de ciberseguridad y ciberdefensa en las infraestructuras de la nación.
- Promover el sistema de gestión de conocimiento de ciberseguridad y ciberdefensa encaminado al mejoramiento de estos servicios.
- Apoyar a los organismos encargados de la investigación y la seguridad del estado para la prevención de amenazas donde se impliquen las tecnologías de la información y las comunicaciones. [15]

4. Leyes normativas de las políticas de ciberseguridad y ciberdefensa en Colombia

- Ley 527 de 1999, por medio de la cual se define el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, también establece las entidades de certificación. [16]
- Ley 599 de 2000, código penal colombiano, normas de la ley penal. [17]
- Ley 603 de 2000, control de la legalidad de software y derechos de autor. [18]
- Ley 1273 de 2009, delitos informáticos, declara preserva y protege los derechos que tenemos de ingresar a los sistemas informáticos seguros. [19]

- Ley 1341 de 2009, sociedad de la información y las TIC, protección de y usuario y todo lo concerniente a la calidad de servicio. [20]
- Ley 1581 de 2012, protección de datos personales, esta ley tiene como objetivo el derecho constitucional que tienen todas las personas sobre los datos personales registrados en cualquier base de datos. [21]
- También se implementan normativas especializadas como los encontrados en el documento Conpes 3701 de 2011, este documento busca generar lineamientos de seguridad y ciberdefensa orientado al desarrollo de estrategias que contrarresten el incremento de las amenazas informáticas que afecten el país. [22]
- Norma técnica NTC-ISO/IEC colombiana 27001, esta norma implementa tecnología de la información, técnicas de seguridad, sistemas de gestión de la seguridad de la información. [23]

5. Divulgación, educación y formación en ciberseguridad

Para garantizar una adecuada comprensión y desarrollo de la sociedad en general y de los funcionarios públicos en temas de ciberseguridad, es fundamental dar a conocer todo tipo de información de este tema mediante la educación y formación de alto nivel y de calidad de todo el recurso humano, quien es en esencia quien produce, consume y transforma información, siendo reconocido el recurso humano como el eslabón más débil de la cadena de seguridad de la información, esta es la razón fundamental para promover tácticas orientadas a generar conciencia y responsabilidad, además de la necesidad de salvaguardar la información como activo fundamental de la sociedad. Este tipo de responsabilidad recae en todo individuo que hace parte del recurso humano que recibe los recursos y la información como materia indispensable para el desarrollo de sus funciones laborales, es fundamental actuar con ética y principios sobre la integridad, veracidad, confidencialidad y disponibilidad de la información al igual que del uso que se le da a esta, y es por esto que se vuelve una necesidad poner en manos de la sociedad las herramientas metodológicas, que permitan una preparación para responder debidamente ante a un suceso de naturaleza cibernética que ponga en riesgo la información del estado y de los ciudadanos. [24]

Un documento con una serie de controles que pueden actuar o utilizarse como un punto de arranque para aquellos que no saben cómo iniciar un control de seguridad, fue diseñado por una comunidad de más de cien agencias gubernamentales, empresas privadas y expertos, para así poder disminuir los ataques al aumentar el nivel de seguridad de los dispositivos, estos son los puntos críticos en los cuales se basa este documento.

- La defensa recibe una retroalimentación del delito: esto le da la experiencia necesaria sobre los ataques para poder aprender de estos eventos y poder construir defensas más efectivas.
- Priorizar: invertir en controles para poder proporcionar un mayor grado de reducción de riesgos.
- Métricas: utilizar métricas conocidas que nos permitan comunicar los resultados con la dirección, autoridades y el grupo de seguridad de la organización.
- Diagnóstico: mediciones continúas realizadas para evaluar y comprobar la eficiencia de las medidas,
- Automatización: proporcionar información fiable y consistente para la automatización de las defensas. [25]

6. Conclusiones

Es posible concluir que es de gran importancia tanto la ciberdefensa como la ciberseguridad, debido a todos los posibles peligros y vulnerabilidades presentes en el ciberespacio y de los cuales pueden ser víctimas las organizaciones y nuestra propia nación.

También es posible destacar que en Colombia existen políticas que, como estado, buscan enfrentar los desafíos y retos que plantean tanto la ciberdefensa como la ciberseguridad, para salvaguardar la seguridad de la nación y de la sociedad en general. Y para ello es indispensable contar con el sector privado, sector público y el sector militar, gracias a este conjunto que abarcan todas las ramas y posibles sectores atacados, es que Colombia según la clasificación mundial de la UIT en el 2014 en materia de ciberseguridad, logro situarse en el noveno lugar a nivel mundial no muy lejos de países como Francia, España, Egipto y Dinamarca. [26]

Es claro que los desafíos que se están presentando a nivel de seguridad son de gran magnitud y ameritan una gran respuesta por parte de los sectores involucrados, pues la globalización de la información y el desarrollo tecnológico exigen la implementación y utilización de este tupo de seguridad y la creación de mecanismos e instrumentos que la regulen además de la educación y divulgación de la información a toda la sociedad.

Referencias

[1] A. Rogers, «hbnamericas,» 31 marzo 2014. [En línea]. Available: http://www.bnamericas.com/es/news/tecnologia/colombiaelabora-politica-de-ciberdefensa-y-ciberseguridad. [Último acceso: 12 octubre 2016].

[2] L. Feliu Ortega, 21 enero 2013. [En línea]. Available: http://catedraisdefe.etsit.upm.es/wp-content/uploads/2013/01/Ponencia-Luis-Feliu.pdf. [Último acceso: 18 septiembre 2016].

[3] M. D. D. NACIONAL, «MINISTERIO DE DEFENSA NACIONAL,» OCTUBRE 2016. [En línea]. Available: https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdf. [Último acceso: 22 SEPTIEMBRE 2016].

[4] E. M. VARGAS, «http://repository.unimilitar.edu.co,» 2014. [En línea]. Available: http://repository.unimilitar.edu.co/bitstream/10654/12259/1/CIBERSEGURIDAD%20Y%20CIBERDEFENSA.%20TRABAJO%20DE%20GRADO.pdf.

[5] P. NACIONAL, «POLICIA NACIONAL,» 30 Marzo 2016. [En línea]. Available: http://www.ccp.gov.co/sites/default/files/clientes_y_proveedores_0.pdf. [Último acceso: 25 Octubre 2016].

[6] R. K. R. Clarke, «Guerra en la red: los nuevos campos de batalla,» Barcelona, planeta, 2011, pp. 17-56.

[7] CARI, «http://www.cari.org.ar,» NOVIEMBRE 2013. [En línea]. Available: http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf. [Último acceso: 27 OCTUBRE 2016].

[8] TREND MICRO, «TREND MICRO,» 30 OCTUBRE 2016. [En línea]. Available: http://www.trendmicro.es/informacion-seguridad/actividad-amenazas-actuales/url-y-spam-maliciosos/index.html. [Último acceso: 30 OCTUBRE 2016].

[9] d. D. Miniterio, «Ministerio de Defensa,» 2014. [En línea]. Available: https://www.mindefensa.gov.co/irj/portal/Mindefensa/contenido?NavigationTarget=navurl://37b759d0e31f2044d8e555a205cf4444. [Último acceso: 30 OCTUBRE 2016].

[10] P. D. L. REPUBLICA, «ACNUR,» [En línea]. Available: http://www.acnur.org/fileadmin/scripts/doc.php?file=fileadmin/Documentos/BDL/2002/01031. [Último acceso: 30 OCTUBRE 2016].

[11] D. C. CONGRESO, «MinTic,» 29 JULIO 2009. [En línea]. Available: http://www.mintic.gov.co/portal/604/w3-article-3707.html. [Último acceso: 1 NOVIENBRE 2016].

[12] MinTic, «mintic,» 26 AGOSTO 2016. [En línea]. Available: http://www.mintic.gov.co/portal/604/w3-propertyvalue-540.html. [Último acceso: 01 NOVIEMBRE 2016].

[13] colcert, «El Grupo de Respuesta a Emergencias Cibernéticas de Colombia,» [En línea]. Available: http://www.colcert.gov.co/?q=acerca-de. [Último acceso: 2 NOVIENBRE 2016].

[14] C. C. POLCIAL, «CENTRO CIBERNETICO POLCIAL,» 2016. [En línea]. Available: http://www.ccp.gov.co/. [Último acceso: 5 NOVIEMBRE 2016].

[15] colCERT, «GRUPO DE RESPUESTAS A EMERGENCIAS CIBERNETICAS DE COLOMBIA,» 2016. [En línea]. Available: http://www.colcert.gov.co/. [Último acceso: 4 noviembre 2016].

[16] d. r. e. MInisterio, «cansilleria.gov.co,» [En línea]. Available: https://www.cancilleria.gov.co/sites/default/files/tramites_servicios/apostilla_legalizacion/archivos/ley_527_1999.pdf. [Último acceso: 25 octubre 2016].

[17] d. c. congreso, «secretariasenado.gov.co,» [En línea]. Available: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html. [Último acceso: 25 octubre 2016].

[18] C. d. c. Decreto, «derechos de autor,» [En línea]. Available: http://www.derechodeautor.gov.co/documents/10181/182597/603.pdf/42c15f4a-afe5-4339-97ca-a61026450307. [Último acceso: 25 octubre 2016].

[19] c. penal, «mintic,» [En línea]. Available: http://www.mintic.gov.co/portal/604/w3-article-3705.html. [Último acceso: 25 octubre 2016].

[20] c. d. colombia, «mintic,» [En línea]. Available: http://www.mintic.gov.co/portal/604/articles-3707_documento.pdf. [Último acceso: 25 octubre 2016].

[21] C. D. COLOMBIA, «http://www.alcaldiabogota.gov.co,» 17 octubre 2012. [En línea]. Available: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981. [Último acceso: 25 cotubre 2016].

[22] c. n. d. p. e. y. s. Conpes, «mintic,» 14 julio 2011. [En línea]. Available: http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf. [Último acceso: 10 novienbre 2016].

[23] ICONTEC, 22 marzo 2006. [En línea]. Available: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf. [Último acceso: 16 novienbre 2016].

[24] d. T. d. l. I. y. l. c. Ministerio, «mintic.gov.co,» marzo 2014. [En línea]. Available: http://www.mintic.gov.co/portal/604/articles-6120_recurso_2.pdf. [Último acceso: 12 septiembre 2016].

[25] P. G. Sack, «http://biblioteca.libertadores.edu.co/,» 5 Diciembre 2015. [En línea]. Available: http://biblioteca.libertadores.edu.co:2087/stamp/stamp.jsp?arnumber=7374178.

[26] U. I. d. Comunicaciones, «Union Internacional de Comunicaciones,» 2014. [En línea]. Available: http://www.itu.int/es/council/2016/Pages/default.aspx. [Último acceso: 10 NOVIENBRE 2016].