CIBERSEGURIDAD COMO BASE FUNDAMENTAL EN LAS OPERACIONES DE LA CADENA LOGÍSTICA EN COMERCIO INTERNACIONAL SEGÚN EL SGCS BASC

PAOLA INFANTE MOYANO

TUTOR:

ING. ARLES PRIETO MORENO

UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE RELACIONES INTERNACIONALES, ESTRATEGIA Y SEGURIDAD

RELACIONES INTERNACIONALES Y ESTUDIOS POLÍTICOS

BOGOTÁ

2018

ÍNDICE

Resumen:

El presente trabajo muestra la importancia que tiene la ciber-seguridad dentro de las operaciones de la cadena logística en comercio internacional. Basándose principalmente en destacar los activos de información que tiene una empresa y en muchas ocasiones ignora cómo protegerla de posibles robos o modificaciones también conocidos como ciber-ataques.

Por otro lado, presenta una lista de las vulnerabilidades a la que está expuesta la información no solo de una empresa sino también personal, esta misma puede ser usada con fines ilícitos lo que puede conllevar a pérdidas económicas para las empresas y procesos judiciales para las personas que se ven involucradas. Ante estas problemáticas se proyecta al SGCS BASC como una herramienta para mitigar y prevenir las amenazas.

Por último, el trabajo contiene una reflexión desde la perspectiva internacionalista y de la importancia que la elaboración del mismo tiene no solo para empresarios sino para la población en general.

Palabras clave:

Ciber-seguridad, ciber-ataques, ransomware, seguridad de información, BASC, malware, comercio internacional, cadena logística.

Abstract:

The advancement of technology over the years has made the unthinkable for many a reality. Activities such as online purchases, communications over long distances by technological means, the connection of various places in the world, artificial intelligence as support in daily life and even the nano technology that has begun to venture into the field of medicine.

All of the above is considered a great advantage of technology, but it is important not to leave aside its disadvantages, even more focusing on another global trend which is globalization and the opening of markets.

In international trade, especially in supply chains, various processes are developed by technological means; from the simplest file to an entire load control program that with the smallest failure in the systems can not only generate problems in the operations, but also millionaire losses and even the total completion of operations by a company.

This is why this work will reveal what is cyber security and what is its role in international trade, also mention the most known cyber attacks and that can be presented in the logistics chain and how these can be prevented or controlled by means of the SGCS BASC, understanding it as a security program in international trade

Key words:

Cyber security, cyber-attacks, ransomware, information security, BASC, networks, malware, international trade, logistics chain.

Objetivos:

Objetivo general:

Analizar la importancia de la *ciber seguridad* como base fundamental de las operaciones de la cadena logística en comercio internacional según el SGCS BASC.

Objetivos específicos:

- Investigar la información que explique el contexto de *ciber seguridad* en el comercio internacional, recolectándola de diversas fuentes confiables y actualizadas.
- Aplicar de la norma BASC el ítem de seguridad de la información, en el campo de la ciber seguridad desde la cadena de suministros en el comercio internacional.
- Presentar recomendaciones por parte de BASC y análisis al campo de la *ciber seguridad* en la cadena de suministros.
- Analizar los beneficios del desarrollo del presente documento desde la perspectiva internacionalista.

Justificación

La importancia de este trabajo radica en la necesidad de conocer cuáles son los riesgos que corre la información en la red. Cada día se comparte más y más información personal en el Internet, pero no se sabe quién pueda usar esa información para actividades ilícitas que logran perjudicar en gran medida e incluso conllevar a problemas judiciales.

Por otro lado, las empresas también pueden ser víctimas de ciertas actividades ilícitas y cada día surgen nuevos medios para robo o mal uso de la información, por lo que es necesario que conozcan esta problemática y se mantengan actualizaos en la materia para hacer frente a la situación. Para esto también se propone el SGCS BASC como herramienta para evitar *ciber-ataques* y como una medida para mitigarlos.

Finalmente, es un estudio necesario para los interesados no solo del área de las relaciones internacionales, sino para toda la comunidad educativa en general, ya que es un conocimiento que les permite nuevas competencias para poner en práctica en su vida profesional en virtud de que es un saber actualizado e innovador.

La selección del presente tema se da en virtud de los pocos estudios que hay en esta área o subdisciplina , si bien se puede llegar a conocer que es un *ciber-ataque* no se ha relacionado cómo puede afectar la cadena de suministro y como puede actuar BASC frente a esto, los principales beneficiados de la elaboración del documento son todas aquellas empresas que posean activos de información y lectores que deseen profundizar en el tema, la ausencia de este estudio implica el desconocimiento de una problemática actual en la cadena de suministro y como la aplicación de BASC es necesaria para evitarlo.

Introducción

El avance de la tecnología a través de los años ha permitido que lo impensable para muchos fuese una realidad. Actividades como las compras por Internet, las comunicaciones a largas distancias por medios tecnológicos, la conexión de diversos lugares del mundo, la Inteligencia Artificial como apoyo en el diario vivir e incluso "la nano tecnología que ha empezado a incursionar en el campo de la medicina" (El Espectador, 2018) ha llevado a que la raza humana se encuentre en la era futurista que se proyectaba hace muchos años.

Todo lo anterior es contemplado como una gran ventaja de la tecnología, pero es importante no dejar de lado sus desventajas, más aún enfocando estas mismas en otra tendencia mundial la cual es la globalización y la apertura de los mercados, donde puede apoyar o interrumpir esta expansión.

En el comercio internacional, especialmente en las cadenas de suministros, se desarrollan diversos procesos por medios tecnológicos; desde el archivo más sencillo a todo un programa de control de carga que con la más pequeña falla en los sistemas puede no solo generar problemas en las operaciones, sino también pérdidas millonarias e incluso la finalización total de operaciones por parte de una empresa.

Es por esto que el presente trabajo dará a conocer que es la *ciber seguridad* y cuál es su papel en el comercio internacional, además mencionará los *ciber ataques* más conocidos y que se pueden presentar en la cadena logística y cómo estos pueden ser prevenidos o controlados por medio del SGCS BASC, entendiéndolo al mismo como un programa de seguridad en las operaciones comerciales a nivel internacional.

Concepto de Ciber-seguridad y su papel en el comercio internacional

Como se ha mencionado anteriormente, la evolución en la tecnología y comunicación ha llevado a que se presenten diferentes dificultades en cuanto a seguridad de la información; es por ello que surge el concepto de *ciber- seguridad* para hacer referencia a estas problemáticas y como responder ante ellas.

Se puede definir a la *ciber-seguridad* como "la protección ejercida sobre los activos de información, por medio del control de amenazas que afectan la información tratada, almacenada y movida en los medios de información que se encuentren comunicados" (ICEMD, 2017).

Se entiende como la protección que se ejerce especialmente sobre una información que es de gran importancia para su poseedor; esta se logra por diversos medios como lo sugiere la Comisión Federal del Comercio: uso de un antivirus actualizado, control de claves, control de acceso, eliminar la información personal de manera segura, encriptación de datos, usar conexiones seguras, no abrir correos sospechosos, entre otros (CFC, 2018).

Ahora bien, el papel de la *ciber-seguridad* en el comercio internacional es de gran importancia, especialmente en la cadena logística de suministros, para ello es relevante exponer el concepto de cadena logística según la norma BASC: "es la secuencia de interacción entre los generadores de productos y servicios con sus proveedores, que contribuyen en la realización, comercialización y entrega de una mercancía o un servicio a un cliente final" (BASC, 2012).

Dentro de los movimientos que se desarrollan en la cadena logística, la mayoría de ellos cuentan con un soporte o un procedimiento documentado almacenado en medio virtual o magnético, desde la base de datos con los asociados de negocios, hasta las cuentas financieras de

una empresa; toda esta información que está presente en una cadena logística corre el riesgo de ser alterada, robada, eliminada, transferida, etc.

Por ello es necesario entender el papel de la *ciber seguridad* en las operaciones que desarrolla una empresa sino también conocer los riesgos que se pueden generar, como evitarlos o tratarlos y buscar cada día la mejora frecuente de los dispositivos o medios de almacenamiento de información con el fin de hacerlos cada vez más seguros y eficaces.

De igual manera busca que la información, "por medio de un programa de seguridad de los datos, se mantenga siempre confidencial, integra y disponible; ya que la información es concebida como uno de los activos más importantes que tiene una organización" (PFS , 2011). Por ejemplo, cuando se tratan de secretos industriales (como lo es la receta de Coca Cola) o comerciales (como movimientos financieros), que representan el éxito de las compañías o su continuidad de operaciones.

Es importante entender que el papel de la seguridad de la información dentro de las operaciones de importación o exportación se basa en los datos de alta importancia que se maneja, es clave comprender quees sensible toda información que involucre proveedores y clientes al igual que información económica. Las empresas necesitan nuevos medios para proteger su información y que estos atiendan a las amenazas que se dan cada día conforme evoluciona la tecnología.

Ahora bien, los riegos que se pueden presentar en cuando a la *ciber- seguridad*, son conocidos también como *ciber- ataques* en su mayoría perpetuados por hackers informáticos y estos se presentan de diversas formas de acuerdo a la finalidad de la vulneración de los controles de seguridad o finalidad de la información hurtada.

Ciber- ataques en la cadena logística

La problemática de los ciber-ataques es pan de cada día en la sociedad; no es una situación que sea ajena a un país porque en cada uno de ellos se presentan distintos tipos de ataques, por lo que BASC se centra en la cadena logística, especialmente en el continente Americano en el cual, el programa de seguridad BASC tiene mayor presencia.

Tabla 1: Intentos de ataques por usuarios conectados / América Latina

País	Porcentaje
Brasil	49,9%
Perú	41,9%
Bolivia	41,8%
Chile	40,0%
México	39,9%
Colombia	39,3%
Guatemala	37,5%
Ecuador	36,1%
Venezuela	36,0%
Uruguay	30,0%
Argentina	29,5%

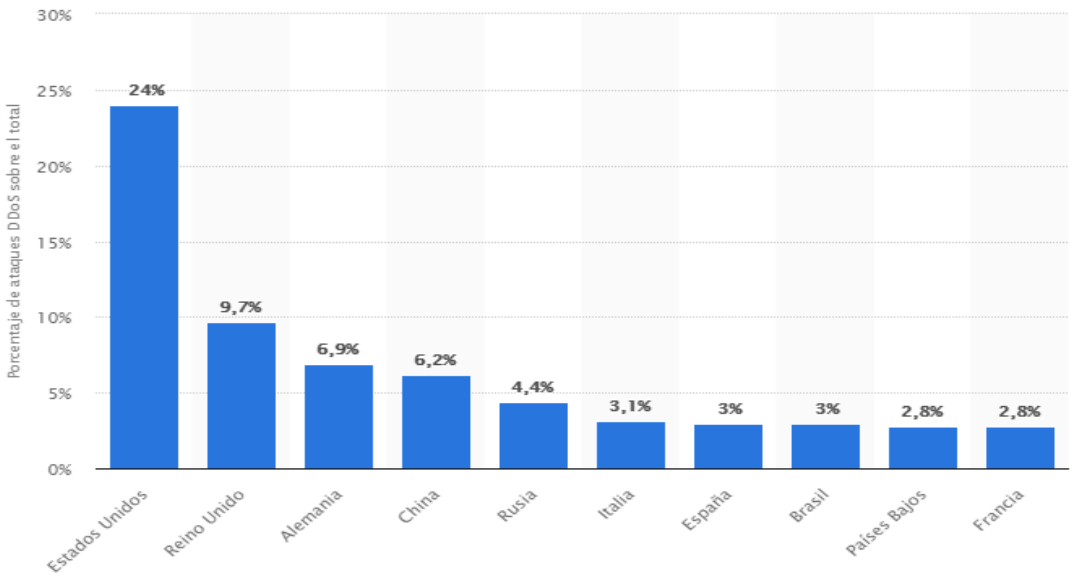
Fuente: (BBC, 2016) Obtenido de http://www.bbc.com/mundo/noticias-37286420

Como se puede observar en la tabla número 1, según las estadísticas de la BBC en el año 2016, los *ciber-ataques* en América Latina sumaron un total de 20 ataques por segundo, el país que más arremetidas presenta es Brasil con un 49.9% de intentos de invasiones por usuarios conectaos, Colombia ocupa un sexto puesto con un porcentaje de 39.3% y el país que presenta ofensivas en una menor medida es Argentina con un 29.5%.

En referencia a Estados Unidos, se puede ver que pesar de ser líder en programas se seguridad es uno de los que más *ciber ataques* sufre, como se observa en la gráfica 1, según el sitio de estadísticas mundiales *Statistas*, en el primer trimestre del año 2016 EEUU sufrió un 24% de los ataques a nivel mundial, esto lo pone muy por encima de los demás países con economías fuertes como lo es Reino Unido con un 9.7 % y Francia con un 2.8%. A esto corresponde el interés del país norteamericano por la incorporación a un programa de seguridad como BASC, para la protección de su economía empresarial y su seguridad nacional, ya que estos ataques no solo se dan a plataformas financieras, sino también pueden llegar a afectar servicios como la salud y organismos estatales como las fuerzas militares.

El país norteamericano no es solo uno de los que más crímenes recibe sino también el que mayor cantidad de ataques realiza; no es sorpresa que uno de los países que más inventos en materia tecnología no sea participe de este tipo de actuaciones en la red, ya que cientos de escándalos han salido a la luz pública, han puesto al descubierto como el gobierno americano y los países desarrollados filtran y espían a otros países para conocer sus procesos internos, como se demostró con el caso de los de *Wikileaks*, entre los delitos que desarrollo por este medio fue el espionaje a conversaciones por parte de mandatarios europeos; es claro que *Wikileaks* para mostrar toda esta información se valió de igual forma de una *hackeo* a la información clasificada de EEUU (CNN , 2016), lo que deja claro que los ataques no solo provienen de otros países sino que pueden ser fundados desde el mismo Estado, es más, se puede tener un hacker cerca y no conocer tal hecho.

Gráfica 1: Porcentaje ataque a nivel mundial



Fuente: (Statista, 2016) Obtenido de https://es.statista.com/estadisticas/487448/listado-mundial-de-paises-afectados-de-ataques-ddos-en-segundo-semestre/

Esto demuestra que la amenaza del ciber crimen no solo se da en los países más industrializados, sino que todos pueden llegar a ser víctima de estos. Partiendo de la realidad de los países Latinoamericanos, se deben tomar los correctivos necesarios para evitar que esta problemática llegue a afectar el funcionamiento normal tanto de su sector macroeconómico como microeconómico.

Ahora bien, las compañías son también víctimas de estos daños, especialmente en su cadena logística. "Solo 2017 se registraron más de 134.000 ataques de ransomware; siendo el de denegación de servicios el más utilizado" (It Digital Security, 2018). Existe una gran variedad de ataques a la cadena logística, por lo que se hará mención a los más destacados:

- Ataque denegación de servicios: "consiste en un ataque a un sistema de ordenadores o red que causa que sea inaccesible el servicio a los usuarios" (Web security.es, 2016); es decir, que por medio de saturar un

servicio web, se haga imposible el ingreso de un usuario legítimo a está, presentando que el servicio no se encuentre disponible.

- Conexiones no autorizadas a equipos o servidores: "violación de la seguridad de ingreso a información de un equipo o servidor por medio de programas que periten una conexión remota, suplantación, ingresos ilegítimos, "puertas traseras*"* para ingresar a una información, violando todos los controles de acceso" (Vieites, 2014).
- *DNS Spoofing*: c*onsiste en la redirección de la búsqueda de un usuario hacia una IP modificada con el fin de obtener información personal del usuario,* por ejemplo el robo de datos para la creación de perfiles falsos. (Vieites, 2014).
- Virus informáticos (Malware): Se trata de un programa que tiene la capacidad de copiarse automáticamente por medios informáticos o internet y su función es alterar el funcionamiento de un equipo y acceder o eliminar datos. Existen distintos tipos de virus informáticas entre los que se encuentran: "Virus, virus encriptados, virus polimórficos, gusanos / worm, troyanos, virus falsos, bombas lógicas, bug-ware, de MIRC" (Prieto, 2007).

Entre los virus más destacados se encuentran: CIH en 1998 que trajo pérdidas de 80 millones de dólares, fue altamente dañino ya que su función era la eliminación de datos y se multiplicaba rápidamente. También se destaca el virus I LOVE YOU en 2000, el cual dejo pérdidas de más de 10 billones de dólares era un gusano (worm), este se camuflaba como un correo inocente, pero al ser abierto por los usuarios infectaba el equipo y automáticamente se enviaba a los demás contactos de la víctima (Prieto, 2007).

- Phishing: Este término es principalmente usado cuando se trata de ataques a sistemas financieros, donde se trata de obtener datos bancarios. Por medio de páginas web fraudulentas de los bancos, roban estos datos; es una actividad que ha entrado en furor los últimos años (Vieites, 2014).
- SMTP Spoofing: Donde por medio del *envío de mensajes bajo en nombre de un usuario de confianza, esto con la finalidad de afectar la buena imagen de este usuario* ya que el contenido de estos mensajes no es

adecuado; este es un proceso relativamente sencillo de realizar ya que no hay un buen filtro de autenticación de usuarios (Vieites, 2014).

- Modificación del tráfico y enrutamiento: Por medio de este ataque se logra que "los mensajes que son enviados de un usuario a un destinatario llegue primero a la persona que está *hackeando* el mensaje antes de que llegue al destinatario original" (Vieites, 2014); es una de las medidas más usadas en el robo de la información por medio de los correos electrónicos o redes de mensajería instantánea como lo son las redes sociales.
- Ataques a sistemas criptográficos: "por medio del hackeo a los algoritmos criptográficos, se pueden desbloquear y hacer visibles las contraseñas puestas a equipos o documentos" (Vieites, 2014). Ya sea por medio del uso de malware que permiten conocer la clave o con el intento de distintas claves hasta obtener la correcta; son distintas medidas utilizadas con el fin del conocimiento de la contraseña.
- Controles psicología social: En relación a estos, no se dan 100% por medio tecnológicos, ya que dentro de una compañía u organización puede encontrarse una persona trabajadora que tenga la intención de robar la información, por lo que puede extraerla por medio magnéticos como CD, memorias; robando directamente la información física en los archivos, o analizando la basura en busca de información que sea de validez. Para este caso es importante la concientización y capacitación del personal y ejercer y control del acceso a la información.

  De igual manera puede darse la situación en que a un miembro del personal este siendo víctima de extorciones o amenazas con el fin de conocer información de valor para la empresa, para ello es importante inculcar en los trabajadores la confianza para revelar dichas situaciones por medio de jornadas de capacitación.

Entre los ataques más destacados a la cadena de suministros se encuentran los financieros; hasta el 2016 se presentaron más de 198 millones de *ciber-ataques*. Diariamente se dan 542.465 ataques generando pérdidas hasta por 6.179 millones de dólares. Para el sector empresarial son aproximadamente 83.756 daños

diarios; pese a los controles que ejercer las empresas los *hacker* logran burlarlo e ingresar a su información (El tiempo, 2017).

La importancia de reconocer estos *malware* no solo es necesaria para entender cuál es su capacidad de daño, ya que en una situación en que haya vulneración de información por causa de estos, se proveen las medidas para evitar la pérdida total de la información y cuáles son los programas o antivirus que pueden evitar los ataques o permitir la recuperación de los datos después de uno.

BASC como herramienta para prevenir ciber- ataques en cadena logística

La conectividad de las empresas es un elemento indispensable para dar a conocer sus bienes y servicios y llevar acabo sus operaciones productivas; la *información que esta posee suele ser de gran volumen por lo que se valen de distintos medios tecnológicos para almacenarla, ya sea desde "la nube" cuando es información probada o compartiéndola por medio de sus páginas web cuando es información pública* (MIN-TIC, 2016), pero esta información es vulnerable de ser manipulada por malintencionados hackers.

Frente a las amenazas mencionadas anteriormente, BASC dispone de una serie de recomendaciones para proteger la información de cualquier afección que pueda sufrir. En primer lugar, debe clasificarse la información que se posee de acuerdo a su importancia, pues existen activos de información que son más importantes que otros y que en caso de pérdida o robo puede traer consecuencias a la empresa a nivel operativo y económico, este proceso es conocido también como un inventario de información (Torres, 2014). Entre la información de más importancia de una empresa se puede encontrar: Lista de clientes, proveedores, información empleados y asociados de negocios; es por ello que se da una política de privacidad de datos personales.

De igual manera, se debe establecer un control por medio de contraseñas para el ingreso a esta información crítica y que el conocimiento de estas claves sea para un número limitado de personas (BASC, 2012). "Se debe instalar y mantener actualizado software antivirus y anti-espía en los sistemas de computación, para prevenir la fuga de información o amenaza a los sistemas de información" (Vallejo, 2016).

Si se llega a presentar un *ciber-ataque*, se debe en primer lugar tener una copia de la información, ya que si esta llega a ser robada se cuenta con un soporte para evitar la pérdida total de esta; en caso que sea una falla en controles humanos (Finanzas Personales, 2015). En caso de tratarse de robo a activos financieros, se debe informar a las autoridades competentes.

Para BASC es importante instituir procedimientos documentados para conocer cómo se debe reaccionar ante estas amenazas y desarrollar actividades de capacitación al personal. Se debe implantar responsabilidades; se debe establecer un tiempo objetivo de recuperación (RTO) y un plan de continuidad del negocio (PCN).

Conclusiones:

Se encuentra en un mundo de constante cambio, donde cada día las acciones de las personas se desarrollan detrás de una pantalla, las relaciones son cada vez más impersonales y se tiene todo en la vida conectado con tendencias como “Internet de las cosas. Todos estos logros tecnológicos son vulnerables a distintas amenazas; es realmente necesario conocer de ellas, de cómo podría afectar, especialmente si puede llevar a pérdidas ecónomas e incluso consecuencias en la integridad de las personas.

Hacker es el nombre que reciben las personas que tienen la capacidad de vulnerar programas tecnológicos y violar cualquier barrera en la red con el fin de desarrollar alguna actividad, sea buena o mala. Si cada vez se conecta más la vida a la red se va llegar al punto en que hackee los hogares, mascotas (con la conexión WiFi) a los collares e incluso vehículos, lo cual ya se ha logrado hacer.

Ahora bien, vale la pena preguntarse ¿si se ha logrado hackear medios tan usados por las personas como las redes sociales o celulares, porque no hackear grandes plataformas como las económicas?, el ciber-crimen es cada vez más frecuente, como una medida de hacer dinero por parte de los criminales. Bandas dedicadas al *ciber-ataque* son desmanteladas cada día.

Los medios tecnológicos con los que cuentan las grandes empresas exportadoras son un objetivo llamativo para los criminales, al igual que el engaño a usuarios de estas plataformas y de las bancarias. Es muy importante que las personas se encuentran informando cada día sobre las nuevas amenazas que pueden existir en las redes, especialmente las empresas, ya que deben encontrar las medidas adecuadas para proteger su información y su economía.

Asimismo, se puede analizar que anteriormente la economía mundial estaba dominada por los Estados, las multinacionales intervenían en menor medida en los sectores productivos y la existencia de éstas no cambiaba las relaciones en el sistema económico internacional, pero a raíz de la globalización se han convertido en un fuerte actor económico rival para el estado, por lo cual es conveniente la protección de información para evitar desequilibrios que afecten el sistema.

Por parte de los profesionales, es necesario que conozcan todo lo concerniente a la *ciber-seguridad* ya que es un plus para poner en práctica en las futuras empresas que lleguen a trabajar. Fácilmente logran engañar a las personas para obtener la información que necesiten y en muchas ocasiones no son conscientes que están siendo víctimas de un ciber-ataque.

Glosario:

- **Seguridad:** La palabra seguridad proviene del latín *securitas*, que a su vez se deriva de *securus*, que significa libre de cualquier peligro o daño (Concepto , 2016).

- **Red:** Conjunto de computadoras o de equipos informáticos conectados entre sí y que pueden compartir información (RAE, 2018).

- **BASC:** (Business Alliance for Secure Commerce) Acuerdo que reafirma el compromiso se las organizaciones para trabajar de manera conjunta en la seguridad de la cadena logística en América y promover un mejor comercio en el mundo (BASC, 2012).

- **Hacker:** Persona experta en el manejo de computadoras, que se ocupa en la seguridad de los sistemas y de desarrollar técnicas de mejora (RAE, 2018).

- **Estándares de SGCS:** Conjunto de requerimientos específicos aplicables, complementarios a la norma BASC y de obligatorio cumplimiento en función al alcance del SGCS, en las empresas que lo implementen (BASC, 2012).

- **Comercio internacional:** Es el movimiento que tienen los bienes y servicios a través de los distintos países y sus mercados. Se desarrolla con el uso de las divisas y está sujeto a las regulaciones adicionales que establecen los gobiernos participantes en el intercambio (Comercio y Aduanas, 2016).

- **Asociado de Negocios:** Tercero vinculado a la cadena de suministro considerado con algún nivel de criticidad de acuerdo al modelo de gestión del riesgo de la organización (BASC, 2012).

- **Seguridad de la información:** Tiene como finalidad la protección de la información y de los sistemas de información del acceso, uso, divulgación e interrupción no autorizada (AEC, 2017).

- **Control:** Seguimiento del desarrollo y etapas de los procesos de la cadena de suministro, para asegurar el resultado esperado u tomar medidas preventivas, correctivas y de mejora, para reducir la posibilidad de materialización de un riesgo (BASC, 2012).

- **Documento:** Información y su medio de soporte o registro, especificación, procedimiento documentado, norma. El medio de soporte puede ser papel, magnético, óptico, electrónico o una combinación de estos (BASC, 2012).

Bibliografía

AEC. (2017). *Asociación Española para la Calidad*. Obtenido de https://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

BASC. (2012). *Norma y Estándares BASC versión 04-2012.* Bogotá D.C.: World BASC orgnization.

BBC. (06 de 09 de 2016). *Cuales son los paises de Amércia Latina mas amenazados con Malware*. Obtenido de http://www.bbc.com/mundo/noticias-37286420

CFC. (2018). *Comisión federal del comercio*. Obtenido de Como proteger su información personal: https://www.consumidor.ftc.gov/articulos/s0272-como-proteger-su-informacion-personal

CNN . (04 de 10 de 2016). *Las 10 filtraciones mas importantes de Wikileaks*. Obtenido de http://cnnespanol.cnn.com/2016/10/04/las-10-filtraciones-mas-importantes-de-wikileaks-en-sus-10-anos/#0

Comercio y Aduanas. (2016). *Que es el comercio internacional*. Obtenido de http://www.comercioyaduanas.com.mx/comercioexterior/comercioexterioryaduanas/que-es-comercio-internacional/

Concepto . (2016). *Definición seguridad*. Obtenido de http://conceptodefinicion.de/seguridad/

El Espectador. (03 de 2018). *Avances tecnológicos*. Obtenido de http://www.eltiempo.com/noticias/avances-tecnologicos

El tiempo. (27 de 09 de 2017). *A diario se registran 542.465 ataques informáticos en Colombia*. Obtenido de http://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370

Finanzas Personales. (2015). *Que hacer si usted o su negocio son víctimas de ataque cibernético*. Obtenido de http://www.finanzaspersonales.co/consumo-inteligente/articulo/ciberseguridad-que-hacer-si-soy-victima-de-un-ciberataque/71919

ICEMD. (2017). *Definición de ciber seguridad y riesgo*. Obtenido de Instituto de economía digital: https://www.icemd.com/digital-knowledge/articulos/definicion-ciberseguridad-riesgo/

It Digital Security. (30 de 01 de 2018). *Cifras de ataques a empresas en 2017*. Obtenido de http://www.itdigitalsecurity.es/actualidad/2018/01/la-cifra-de-ciberataques-a-empresas-en-2017-podria-superar-los-350000

MIN-TIC. (2016). *Ministerio de las tecnologías de la infomación y comunicaciones*. Obtenido de Industri: http://www.mintic.gov.co/portal/604/w3-propertyvalue-1056.html

PFS . (2011). *La importancia de la seguridad de información*. Obtenido de http://www.pfsgrupo.com/la-importancia-de-la-seguridad-de-la-informacion/

RAE. (2018). *Diccionario Real Academia de la Lengua Española*. Obtenido de http://dle.rae.es/?id=DgIqVCc

Statista. (2016). *Raking mundial de los países que mas ciber ataques sufrieron en el primer trimestre del 2016*. Obtenido de https://es.statista.com/estadisticas/487448/listado-mundial-de-paises-afectados-de-ataques-ddos-en-segundo-semestre/

Torres, S. A. (10 de 2014). *Importancia de implementar un SGSI en una empresa certificada BASC.* Obtenido de http://repository.unimilitar.edu.co/bitstream/10654/12262/1/IMPORTANCIA%20DE%20IMPLEMENTAR%20EL%20SGSI%20EN%20UNA%20EMPRESA%20CERTIFICADA%20BASC.pdf

Vallejo, H. A. (2016). *Manual del sistema de gesntión en control de seguridad BASC.* Obtenido de http://www.lameseta.com.co/wp-content/uploads/Manual-Seguridad-BASC-La-Meseta.pdf

Vícto Manuel Prieto Álvares, R. A. (2007). *Virus Informáticos .* Obtenido de Master en Informática: http://sabia.tic.udc.es/docencia/ssi/old/2006-2007/docs/trabajos/08%20-%20Virus%20Informaticos.pdf

Vieites, Á. G. (08 de 2014). *Tipos de ataques e intrusos en las redes informáticas .* Obtenido de http://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf

Web security.es. (2016). *Que es un ataque de denegación de servicios*. Obtenido de http://www.websecurity.es/que-es-un-ataque-denegaci-n-servicio