RIESGOS CIBERNÉTICOS ASOCIADOS A LA CADENA DE SUMINISTRO

Díaz Bermúdez Sandra Milena
ing.diazsandra@gmail.com
Universidad Piloto de Colombia

***Resumen*—** En los últimos años se han presentado numerosos ciberataques sofisticados a gran escala y a nivel mundial, que han afectado la continuidad del negocio y reputación de organizaciones de diferentes sectores y tamaños, en consideración a estos incidentes, las organizaciones están invirtiendo grandes cantidades de recursos en la protección de sus redes, software, activos de información críticos y métodos de concientización sobre ciberseguridad a sus empleados para que no sean víctimas de la ingeniería social. Todo esto, con el fin de garantizar que sus redes y sistemas de información no sean infiltradas por los ciberdelincuentes. Sin embargo, los ciberdelincuentes son creativos, incluso innovadores que aprovechan cualquier brecha de seguridad para infiltrarse en el objetivo sin ser detectados.

Una nueva tendencia de infiltración y ataques informáticos a las organizaciones, sucede a través de la explotación de vulnerabilidades de sus terceros (proveedores, socios o clientes), por lo que se considera un ciberataque a la cadena de suministro, en este sentido, los ciberdelincuentes pueden acceder a una organización no atacándola directamente, sino vulnerando a sus proveedores (que participan en la cadena de suministro para que puedan desarrollar sus productos y/o negocios), consiguiendo infiltrarse en sus redes y posteriormente buscando alguna forma de llegar a su objetivo principal, comprometiendo considerablemente la confidencialidad, integridad y disponibilidad de la información y operaciones.

***Abstract*—** In recent years there have been numerous sophisticated cyber attacks on a large scale and worldwide, that have affected the business continuity and reputation of organizations of different sectors and sizes, in consideration of these incidents, organizations are investing large amounts of resources in the protection of their networks, software, critical information assets and cybersecurity awareness methods to its employees, so that they are not victims of social engineering. All this in order to ensure that their networks and information systems are not infiltrated by cybercriminals. However, cybercriminals are creative, even innovative, who take advantage of any security breach to infiltrate the target undetected.

A new tendency of infiltration and computer attacks to the organizations, is through the exploitation of vulnerabilities of third parties (their suppliers, partners or clients), for what is considered a cyberattack to the supply chain, in this sense, the cybercriminals they can access an organization by not attacking it directly, but by violating its suppliers (who participate in the supply chain so that they can develop their products and / or businesses), getting infiltrated in their networks and then looking for some way to reach their main objective , significantly compromising the confidentiality, integrity and availability of information and operations.

***Índice de Términos*—** Amenazas cibernéticas, cadena de suministro, ciberataques, ciberseguridad, riesgos, vulnerabilidades y proveedores.

I. INTRODUCCIÓN

De acuerdo con las estadísticas e informes revelados por las principales compañías de seguridad informatica, el año 2017 fue el periodo de los ciberataques más potentes y sofisticados de los últimos tiempos, dejando grandes desastres económicos, financieros, políticos y sociales a nivel global. Así lo expuso una de las compañías más importantes en ciberseguridad "Sonicwall" en su informe "Amenazas cibernéticas" publicado recientemente [1], donde indica que se registraron más de 9.320 millones de ataques de malware a nivel global en el año 2017, con un incremento del 18,4% anual de ciberataques en todo el mundo en el mismo año y se evidenciaron 12.500 nuevas vulnerabilidades y exposiciones comunes en el CVE (Common Vulnerabilities and Exposures - según la NIST es una lista de vulnerabilidades de ciberseguridad a nivel mundial, públicamente conocidas, cada vulnerabilidad tiene un número de identificación, una descripción y al menos una referencia pública. La lista CVE se utiliza en numerosos productos y servicios de seguridad cibernética de todo el mundo, incluida la base de datos nacional de vulnerabilidades de Estados Unidos).

Así mismo, la compañía Sonicwall afirma que los ataques cibernéticos se están convirtiendo en el riesgo empresarial número uno [1].

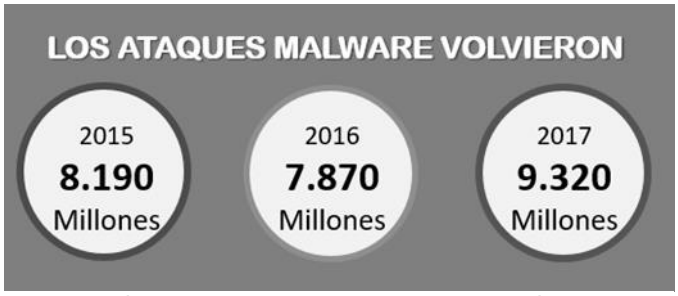

Fig. 1. Estadística de los ataques de malware registrados los últimos tres años, según [1].

Sin embargo, este es un panorama que muestra los ciberataques que tuvieron éxito, infiltrándose o comprometiendo a las organizaciones. Es importante enfatizar

en las numerosas amenazas que se generan día a día por los ciberdelincuentes y que son detectadas a tiempo por los diferentes programas y compañías de ciberseguridad, como por ejemplo la empresa de seguridad e investigación de amenazas y desarrollo de técnicas de ciberdefensa "Panda Security", que en su informe anual 2017 indicó que se registraron 285.000 nuevos ejemplares de malware al día, que el 62% de las brechas de seguridad se han explotado por técnicas de hacking, donde el 51% de los atacantes han utilizado malware y el resto se han valido de otras herramientas de las que la mayoría de organizaciones no están protegidas [2].

El crecimiento de las ciberamenazas sigue siendo explosivo, y el costo de proteger a las empresas y a los consumidores continúa en aumento. Mientras tanto hay grandes organizaciones que están avanzando e implementando nuevas estrategias, herramientas y recursos fundamentales para la protección de sus redes, sistemas informáticos y recursos humanos que mitiguen estos riesgos, dando paso a un nuevo concepto de 'ciber-resiliencia', que consiste en la administración de las amenazas virtuales de modo tal que sea posible para las empresas gestionar de manera efectiva los ataques cibernéticos [3]. Esto se refleja en los últimos estudios de Gartner, que indican una creciente inversión a nivel mundial en productos y servicios en seguridad informática y un aumento considerable de la concientización entre los empresarios sobre el impacto comercial y devastador de los incidentes de ciberseguridad [4].

Por otro lado, en Colombia las cifras y estadísticas son desfavorables, ya que según el diario 'Portafolio' el 59% de las empresas en Colombia recortarían el presupuesto en las actividades y productos para la seguridad informática, o lo mantendrían congelado [5]. Sin embargo, el gobierno colombiano sigue trabajando en la inclusión de nuevas políticas, lineamientos y estándares sobre la seguridad digital, tales como el Conpes 3854 (Consejo Nacional de Política Económica y Social), que es la máxima autoridad nacional de planeación, que se desempeña como organismo asesor del gobierno en todos los aspectos relacionados con el desarrollo económico y social del país y el Modelo Nacional de Gestión de Riesgos de Seguridad Digital, el cual se analizará dentro de este artículo.

Ahora bien, aunque las grandes organizaciones tengan más conciencia del impacto que contribuye la ciberseguridad y estén realizando nuevas estrategias, como la de mitigar uno de los riesgos más latentes que es la ingeniería social, los expertos han manifestado que no se pueden dejar de lado las pequeñas y medianas organizaciones, que son parte del suministro ya sea de software, hardware, servicios TI u otro tipo de productos de estas grandes organizaciones y que actualmente no tienen la misma conciencia, ni recursos para implementar medidas de protección a sus sistemas de información y operaciones.

Por consiguiente, en este artículo se presenta en primera instancia, la definición de algunos términos asociados a la ciberseguridad y la cadena de suministro, con el fin de aclarar algunas imprecisiones que se generan alrededor de estos temas. Así mismo, se expone una perspectiva global sobre diferentes aspectos de los riesgos cibernéticos adheridos a los proveedores o servicios de terceros, los cuales son considerados como los actores principales dentro de la cadena de suministro. Lo anterior basado en la referenciación y análisis de algunos casos reales de ataques cibernéticos a gran escala que se han presentado a nivel mundial.

En última instancia, se plantea la importancia y los beneficios de la inclusión de la cadena de suministro en la gestión del riesgo, por medio de la implementación de estrategias, herramientas, políticas y estándares internacionales en seguridad de la información.

II. CONCEPTOS ASOCIADOS

A. Cadena de suministro

El concepto de cadena de suministro día a día ha adquirido mayor importancia entre los diferentes sectores de la industria, sin embargo, para este artículo es un buen referente la definición de la Norma Técnica Colombiana NTC-ISO 28000 sobre especificaciones de sistemas de gestión de la seguridad para la cadena de suministro, la cual define como el conjunto relacionado de recursos y procesos que comienzan con el suministro de materias primas y se extiende hasta la entrega de productos o servicios al usuario final, incluidos los medios de transporte. La norma adiciona una nota en la definición que indica que la cadena de suministro puede incluir vendedores, instalaciones de manufactura, proveedores, centro de distribución interna, distribuidores, mayoristas y otras entidades que conducen al usuario final" [6].

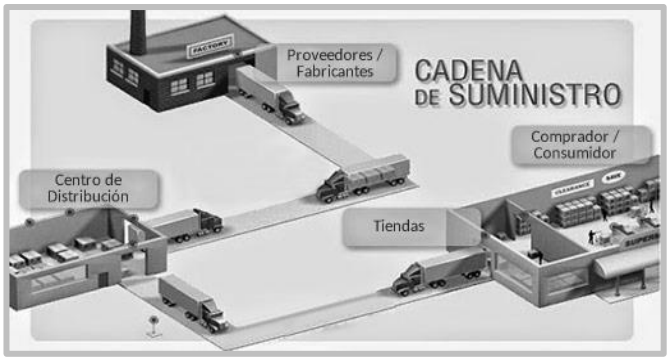

Fig. 2. Ejemplo del concepto cadena de suministro [6].

La norma ISO 28000 identifica y define los principales actores de la cadena de suministro así:

1) Proveedor(es): Son los encargados de surtir a las empresas de los insumos o materias primas necesarios para el desarrollo de su actividad. Un proveedor puede ser una persona o una empresa que abastece a otras empresas con insumos o materias primas, los cuales serán transformados para venderlos posteriormente o directamente. Estos insumos o materias primas adquiridas están dirigidas directamente a la actividad o negocio principal de la empresa que compra esos elementos.

2) Fabricante(s): Empresa(s) dedicada(s) a la fabricación de productos para el consumo en la cadena de suministro.

3) Cliente(s): Se refiere a quién accede al producto o servicio en cuestión con asiduidad, existen los clientes ocasionales. Cliente es sinónimo de comprador (la persona que compra el producto), usuario (la persona que usa el servicio) o consumidor (quien consume un producto o servicio).

4) Detallista(s) / Minoristas(s): Venden productos al consumidor final y contribuyen el último eslabón del canal de distribución, son los que están en contacto con el mercado y tienen gran importancia porque pueden alterar frenando o potenciando, las acciones de marketing y merchandising de los fabricantes y mayoristas. Adicionalmente son capaces de influir en las ventas y resultados finales de los artículos que comercializan.
5) Distribuidor(es): Estos ponen a disposición de los consumidores finales el producto o servicio para su consumo directamente a través de una red de tiendas físicas o a distancia (internet, pedido telefónico, venta catálogo) los bienes del fabricante.

B. Conceptos de cibernética.

En el desarrollo de este artículo, es importante precisar en algunos conceptos entorno a la ciberseguridad y la cibernética, dado que en muchas ocasiones se interpretan de forma inadecuada. En consideración a esto, las siguientes definiciones se tomaron del Modelo Nacional de Gestión de Riesgos de Seguridad Digital de Colombia, como guía en español para evitar las malas interpretaciones [7].
1) Amenaza cibernética: Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del estado.
2) Ataque cibernético: Acción organizada y premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio.
3) Cibercrimen o Delito cibernético: Conjunto de actividades ilegales asociadas con el uso de las tecnologías de la información y las comunicaciones, como fin o como medio.
4) Ciberseguridad: Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio.
6) Incidente de seguridad de la información: Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de información de la organización o comprometer sus operaciones.
7) Vulnerabilidad: Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan.
8) Control: Es la medida que modifica al riesgo o medios para gestionar el riesgo y que incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

C. Tipos de ataques cibernéticos

Conforme a la anterior definición sobre un ataque cibernético o ciberataque, se debe precisar en que estos ataques permiten a los ciberdelincuentes, acceder a sistemas y computadores de manera no permitida y descontrolada y su objetivo generalmente es acceder, cambiar o destruir información sensible, extorsionar con dinero a los usuarios o interrumpir los procesos empresariales normales. La compañía de Symantec en sus informes de ciberseguridad define los tipos de ciberataques [8].
1) Virus informático: Es un programa informático malicioso que puede copiarse e infectar un computador, el término "virus" también se usa comúnmente pero erróneamente para referirse a otros tipos de malware, incluidos, entre otros, los programas de adware y spyware que no tienen capacidad reproductiva.
Por otra parte, un virus verdadero puede propagarse de una computadora a otra (con algún tipo de programa) cuando su host se lleva a la computadora de destino. Por ejemplo, porque un usuario lo envió a través de una red o lo llevó en un medio extraíble, como una unidad usb.
2) Malware: Es un término usado para describir software malicioso, incluyendo spyware, ransomware, virus y gusanos. El malware infringe una red a través de una vulnerabilidad, generalmente cuando un usuario hace clic en un enlace peligroso o un archivo adjunto de correo electrónico que luego instala un software arriesgado. Una vez dentro del sistema, el malware puede bloquear el acceso a los componentes clave de la red (ransomware), instalar malware o software dañino adicional, obtener secretamente información mediante la transmisión de datos desde el disco duro (spyware) e interrumpir ciertos componentes y dejar el sistema inoperable.
3) Gusano informático: Es un programa informático de malware auto-replicable. Utiliza una red informática para enviar copias de sí mismo a otros nodos (computadoras en la red) y puede hacerlo sin intervención del usuario. Esto se debe a deficiencias de seguridad en la computadora de destino y diferencia de un virus, no es necesario que se una a un programa existente. Los gusanos casi siempre causan al menos algún daño a la red, al consumir ancho de banda, mientras que los virus casi siempre corrompen o modifican archivos en una computadora específica.
4) Adware: Software respaldado por publicidad, es cualquier paquete de software que reproduce, muestra o descarga publicidad en una computadora automáticamente después de instalar el software o mientras se usa la aplicación. Las funciones de publicidad se integran o se incluyen con el software, que a menudo está diseñado para identificar los sitios de internet qué visita el usuario y presentar la publicidad pertinente a los tipos de productos o servicios que allí aparecen.
5) Spyware: Software espía, es un tipo de malware que se instala en las computadoras y recopila pequeñas porciones de información sobre los usuarios sin su conocimiento. La presencia de spyware generalmente está oculta para el usuario y puede ser difícil de detectar. Normalmente el spyware se instala secretamente en el computador personal del usuario y algunas veces los spyware como Keyloggers son instalados por el propietario de un computador compartido a propósito, para monitorizar en secreto a otros usuarios.
6) Troyano / (Caballo de Troya): Es un malware no auto-replicante que parece realizar una función deseable para el usuario pero que en cambio facilita el acceso no autorizado al sistema informático del usuario.

7) Root kit: Es un tipo de software que está diseñado para obtener el control de nivel de administrador, sobre un sistema informático sin ser detectado. Generalmente en todos los casos, el propósito y el motivo es realizar operaciones maliciosas en un sistema informático sin el conocimiento de los administradores o usuarios de ese sistema.

8) Ransomware: Según la compañía de ciberseguridad "Kaspersky", un ransomware es un software malicioso específicamente un tipo de troyano diseñado para obtener dinero de una víctima, que al infectar una computadora le da al ciberdelincuente la capacidad de cifrar datos almacenados en el disco de la víctima, para que esta no pueda acceder a la información o bloquear el acceso normal al sistema de la víctima. A menudo, el ransomware exige un pago para deshacer los cambios que el virus troyano haya realizado en la computadora de la víctima.

La manera más común en que se instala un ransomware, es camuflándose dentro de otro archivo o programa apetecible para el usuario, que invite a hacer clic a archivos adjuntos en correos electrónicos, vídeos de páginas de dudoso origen o incluso en actualizaciones de sistemas y programas en principio fiables como Windows o Adobe Flash. Una vez que ha penetrado en el ordenador, el malware se activa y provoca el bloqueo de todo el sistema operativo y lanza el mensaje de advertencia con la amenaza y el costo del rescate que se ha de pagar para recuperar toda la información. Para potenciar la incertidumbre y el miedo de la víctima, en ocasiones incluyen en la amenaza la dirección IP, la compañía proveedora de internet y hasta una fotografía captada desde la webcam del computador de la víctima.

9) Puertas traseras: Es una forma de malware qué distorsiona los procedimientos de autenticación estándar para obtener acceso a un sistema. La instalación de una puerta trasera se logra generalmente aprovechando los elementos vulnerables en las aplicaciones web. Un programador inserta un fragmento de código en áreas vulnerables que le permitiría acceder a un sitio web o sistema seguro utilizando una contraseña que solo conocen personas o grupos específicos. Después de la instalación, los archivos se ofuscan, lo que dificulta la detección de una puerta trasera. El malware de puerta trasera también juega un papel esencial en la unión de un grupo de dispositivos infectados para crear una botnet que pueda aprovecharse para el delito cibernético.

10) Inyección SQL: Se denomina ataque de inserción SQL, que ayuda al atacante a ejecutar un código debido a la presencia de vulnerabilidad en la capa de la base de datos de la aplicación. En consecuencia, el código obtendrá datos confidenciales o incluso comprometerá la aplicación.

11) Cross-Site Request (CSRF): Es la falsificación de solicitudes entre sitios, también conocida como ataque con un solo clic o sesión, es un ataque que obliga al usuario final a ejecutar acciones no deseadas en una aplicación web en la que está autenticado actualmente. Estos ataques se dirigen específicamente a las solicitudes que cambian el estado, no al robo de datos, ya que el atacante no tiene forma de ver la respuesta a la solicitud falsificada. Con un poco de ayuda de ingeniería social (como enviar un enlace por correo electrónico o chat), un atacante puede engañar a los usuarios de una aplicación web para que ejecuten las acciones que el atacante elija. El fin de este ataque es explotar la confianza que un sitio web tiene en un usuario particular.

12) Cross Site Scripting (XSS): Se basa en insertar código o script en el sitio web de la víctima, y hacer que el visitante al ingresar al sitio lo ejecute y cumpla el cometido para el que fue escrito, como robo de sesiones o datos vulnerables.

13) Robo de cookies: Es un ataque que se realiza mediante scripts del lado del cliente como JavaScript. Cuando el usuario hace clic en un enlace, el script buscará la cookie almacenada en la memoria de la computadora para todas las cookies activas y las enviará (como los correos electrónicos) al atacante.

14) Phishing: Es el método más utilizado por los ciberdelincuentes y consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude.

Los principales daños provocados por el phishing son el robo de identidad y datos confidenciales de los usuarios (esto puede conllevar a pérdidas económicas para los usuarios o incluso impedirles el acceso a sus propias cuentas), pérdida de productividad y consumo de recursos de las redes corporativas (ancho de banda, saturación del correo, etc.)

15) Ataque de agujero de riego: Es un tipo más complejo de ataque de phishing. En lugar de la forma habitual de enviar correos electrónicos falsificados a los usuarios finales con el fin de engañarlos para que revelen información confidencial, los atacantes usan un enfoque de múltiples etapas para obtener acceso a la información específica. En los primeros pasos, el atacante está perfilando a la víctima potencial, recabando información sobre sus hábitos de internet, historial de sitios web visitados, etc. En el paso siguiente, el atacante usa ese conocimiento para inspeccionar vulnerabilidades de sitios web públicos legítimos específicos, si hay vulnerabilidades, el atacante compromete el sitio web con su propio código malicioso, espera que la víctima objetivo regrese al sitio web comprometido y luego los infecta con vulnerabilidades (a menudo vulnerabilidades de día cero) o malware.

16) Web Defacement: La desfiguración del sitio web, es un ataque a un sitio web que cambia la apariencia visual del sitio. Básicamente los ciberdelincuentes entran en un servidor web y reemplazan el sitio web alojado con uno propio. Lo más probable es que este tipo de ataques se hagan intencionalmente para arruinar la reputación de la compañía que ha alojado este sitio web.

17) Buffer Overflow: Desbordamiento de búffer, es una anomalía en la que un proceso almacena datos en un búffer fuera de la memoria que el programador reservó para ello. Los datos adicionales sobrescriben la memoria adyacente, que puede contener otros datos, incluidas variables de programa y datos de control de flujo del programa. Esto puede provocar errores de acceso a la memoria, resultados incorrectos, finalización del programa o una violación de la seguridad del sistema. Esta vulnerabilidad es completamente un error del programador.

18) Ataque de denegación de servicio (DoS) y ataque distribuido de denegación de servicio (DDoS): Son ataques diseñados para causar una interrupción o suspensión de

servicios de un host o servidor específico, inundándose con grandes cantidades de tráfico inútil o solicitudes de comunicación externa. Cuando el ataque DoS tiene éxito, el servidor ya no puede responder ni siquiera a solicitudes legítimas; esto se puede observar de varias maneras: respuesta lenta del servidor, rendimiento lento de la red, falta de disponibilidad de software o página web, incapacidad para acceder a los datos, sitio web u otros recursos. El ataque de denegación de servicio distribuido (DDoS) ocurre cuando múltiples sistemas comprometidos o infectados inundan un host particular con tráfico simultáneamente.

19) Botnet: Es una red de dispositivos infectados por un ciberdelincuente, que se utiliza para llevar a cabo, por ejemplo, los ataques DDoS y difundir mensajes de correo electrónico con spam. Prácticamente cualquier dispositivo conectado a internet, incluyendo routers residenciales, puede ser infectado e incluso en una botnet sin que su propietario tenga conocimiento.

20) Ataque Man-in-the-middle: Este ataque es una forma de monitoreo activo o escucha de las conexiones de las víctimas y la comunicación entre los hosts de las víctimas. Esta forma de ataque incluye también la interacción entre ambas partes: las víctimas de la comunicación y el atacante, este ataque se materializa cuando el atacante intercepta toda la comunicación, modifica su contenido y la envía de vuelta como respuestas legítimas. Las dos partes que hablaron no son conscientes de la presencia del atacante y creen que las respuestas que reciben son legítimas. Para que este ataque tenga éxito, el ciberdelincuente debe suplantar con éxito al menos uno de los puntos finales; este puede ser el caso si no hay protocolos establecidos que aseguren la autenticación mutua o el cifrado durante el proceso de comunicación [8].

III. RIESGOS OCULTOS DE LA CADENA DE SUMINISTRO

Debido a la creciente demanda de los clientes y la competitividad en los mercados impulsada por el mundo digital, actualmente la mayoría de las organizaciones independientemente de su naturaleza, no son autónomas y por lo general forman parte u operan dentro de una compleja cadena de suministro que cada vez es más amplia, ya que estas organizaciones están en constante búsqueda de nuevos mercados, clientes y proveedores, explotando sus oportunidades presentadas por la globalización, pero que sin duda conllevan a una serie de desafíos administrativos y de seguridad más amplios.

Este aspecto en seguridad tiene grandes retos, ya que cada día se presentan casos donde los ciberdelincuentes intentan vulnerar cierto objetivo por algún periodo de tiempo, pero sin tener éxito. Tal vez esto se debe a que las organizaciones objetivo han implementado redes y software impenetrables y a que los empleados son capacitados para no ser víctimas de la ingeniería social, a pesar de ello, los ciberdelincuentes son persistentes y no se dan por vencidos, entonces buscan organizaciones débiles a nivel de seguridad, que estén vinculadas a su objetivo principal y así mismo ejecutan sencillos ataques informáticos a estas organizaciones

Fig. 3. Aumento de 200% en los ataques a la cadena de suministro, en los tres últimos años [11].

vulnerables, que son proveedoras, clientes o socios de las grandes organizaciones, logrando evadir ciertos controles de prevención y detección, comprometiendo a su primer y principal objetivo.

Es por lo anterior, que algunos expertos consideran y coinciden, en que la cadena de suministro representa la parte más vulnerable de las grandes organizaciones, porque se centran en la seguridad interna y omiten que sus proveedores, clientes o con quienes comparten sus activos de información, poseen ciertas vulnerabilidades que pueden ser explotadas para infiltrarse en estas grandes organizaciones u objetivos específicos.

En uno de los más importantes eventos sobre ciberseguridad que se realiza anualmente, "RSA Conference", el expositor Jon Boyens del NIST (National Institute for Standards and Technology) en su conferencia: "Integrando la ciberseguridad en la gestión del riesgo de la cadena de suministro", mostró estadísticas del aumento de los ciberataques a la cadena de suministro y una parte de las causas de estos ataques, en el que indica que el 80% de todas las vulnerabilidades de la información se originan en la cadena de suministro, el 45% de todos los ataques cibernéticos se atribuyeron a socios anteriores. El 72% de las empresas no tienen visibilidad completa en sus cadenas de suministro y el 59% de las empresas no tienen un proceso para evaluar la ciberseguridad de terceros proveedores con los que comparten datos o redes [9].

Por otra parte, durante el año 2017 numerosas compañías e instituciones de análisis e investigación en seguridad informática, predijeron que para el año 2018 se esperan grandes ataques cibernéticos a la cadena de suministro. Así lo expresó el equipo de KasperskyLab, en su boletín de seguridad "Predicciones sobre amenazas para el 2018", donde se esperan ver más ataques a la cadena de suministro, tanto reales (llevados a cabo) como detectados, así como el uso de programas especializados infectados, en donde los ciberdelincuentes realizan estudios de vulnerabilidades de los sitios más visitados por los empleados de las organizaciones objetivo [10].

La compañía de seguridad informática Symantec, también mostró en su informe de amenazas de seguridad de internet 2018, un aumento considerable del 200% en ataques, como implantes de malware en la cadena de suministro, con el fin de infiltrarse en las grandes organizaciones víctimas, así mismo la compañía afirma que las vulnerabilidades son cada

vez más fáciles de identificar y explotar para los ciberdelincuentes.

Las actualizaciones de los software maliciosos como el ransomware, proporcionan a los ciberdelincuentes un punto de entrada para comprometer objetivos bien protegidos o para dirigirse a una región o sector específico, utilizando una variedad de métodos extendiéndose a través de las redes corporativas para desplegar la carga maliciosa de los atacantes. Por lo que Symantec, detectó y expuso los diferentes ataques que se han presentado a la cadena de suministro desde el año 2015, relacionados en las siguientes tablas [11]:

TABLA I
ATAQUES A LA CADENA DE SUMINISTRO
EN EL AÑO 2015 [11].

Mes	Ataque
Abril	EvLog, actualización comprometida con malware
Mayo	Herramienta japonesa de procesador de palabras utilizada para instalar malware.
Junio	XcodeGhost, malware encontrado en el entorno de desarrollo de Apple
Diciembre	Se encontró una puerta trasera en el firewall de red de un Juniper.

TABLA II
ATAQUES A LA CADENA DE SUMINISTRO
EN EL AÑO 2016 [11].

Mes	Ataque
Mayo	Software de seguridad coreano utilizado para instalar malware.
Septiembre	Atacantes secuestran todos los DNS de un banco brasileño.
Noviembre	Ask Toolbar Network utilizado para instalar malware.
Diciembre	Ask Partner Network Updater usado para instalar malware.

TABLA III
ATAQUES A LA CADENA DE SUMINISTRO
EN EL AÑO 2017 [11].

Mes	Ataque
Febrero	Versión troyanizada de yeecall de Android utilizada como RAT.
	Campaña Kingslayer secuestró las actualizaciones de software sysadmin.
Marzo	Instalador de Adobe Reader infectado con malware
Mayo	Herramienta de video HandBrake para instalar malware.
	WilySupply compromete actualizaciones de herramientas de edición.
Junio	Actualizador M.E.Doc se usa para distribuir Petya/NotPetya.
Julio	Software de la Farmacia ePrica instala un troyano de puerta trasera.
Agosto	Herramienta CCleaner infectada con malware.
Septiembre	Puerta trasera encontrada en el software del servidor netSarang mgmt.
	Módulos modificados de Python encontrados en el repositorio oficial.
	Se encontró el malware “ExpensiveWall” en Android SDK.
Octubre	Elmedia Player para Mac OS X infectado con malware.
Noviembre	Bitcoin Gold wallet reemplazado con malware.
Diciembre	Plugins de WordPress utilizados para instalar puertas traseras.

IV. TÉCNICAS Y TIPOS DE ATAQUES A LA CADENA DE SUMINISTRO

Una de las finalidades de este artículo es dar a entender por medio de ejemplos, casos o ataques reales, los riesgos cibernéticos que se asocian a la cadena de suministro y que no son del mundo de la ciencia ficción o con poca ocurrencia. Estos casos o ejemplos son muestra de que los ataques cibernéticos no precisan entre país, tamaño de la organización o tipo de industria. En la siguiente parte se explican las técnicas más usadas por los ciberdelincuentes para atacar la cadena de suministro.

A. Ataques al proveedor de software.

Los ciberataques a los proveedores de software de terceros son el ejemplo más representativo y de mayor frecuencia, en este caso, uno de los grupos de ciber-espionaje conocido como “Dragonfly”, comprometió los sitios web de los proveedores de software de ICS (Sistemas de Control Industriales) y reemplazó los archivos legítimos en sus repositorios con sus propias versiones infectadas con malware. Posteriormente, cuando el software ICS se descargó de los sitios web de los proveedores, instaló malware junto con el software ICS legítimo. El malware incluía funcionalidades de acceso remoto adicionales que podrían utilizarse para controlar los sistemas en los que se instaló. El software comprometido es muy difícil de detectar si ha sido alterado en la fuente, ya que no hay ninguna razón para que la empresa objetivo sospeche que no era legítimo.

Esto confiere gran confianza al proveedor, ya que no es factible inspeccionar cada pieza de hardware o software en la profundidad requerida para descubrir este tipo de ataque. Sin embargo, es posible mitigar estos riesgos, con la inclusión de los proveedores y clientes en el sistema de gestión de riesgos de la organización. En la siguiente gráfica se explica el

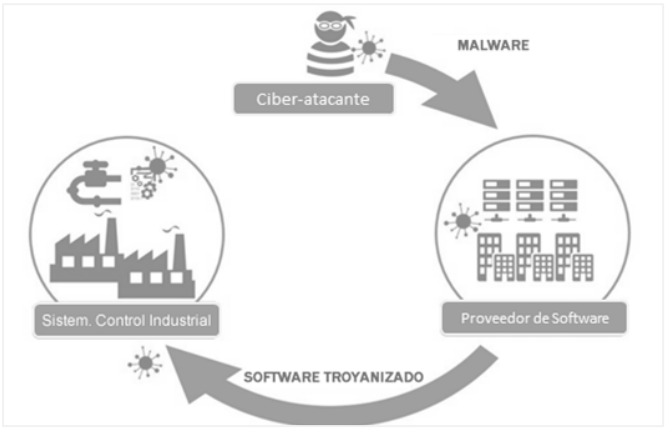

Fig. 4. Ciberataque a la cadena de suministro por medio del proveedor de software [12].

proceso de cómo se ejecuta un ataque a la cadena de suministro por medio de un proveedor de software [12].

B. Ataque a constructores de sitios web.

Los ciberdelincuentes también se dirigen a las cadenas de suministro como un medio para llegar a la audiencia más amplia posible con su malware. Identificar y poner en peligro un elemento estratégicamente importante, es un uso eficiente de los recursos y puede dar lugar a un número significativo de infecciones. Un buen ejemplo de esto es el troyano bancario Shylock, centrado en la banca electrónica en el Reino Unido, Italia y Estados Unidos, la amenaza del grupo detrás de este virus se redujo mediante una operación conjunta entre las agencias encargadas de hacer cumplir la ley y la comunidad de ciberseguridad, en julio de 2014. Los atacantes de Shylock comprometieron sitios web legítimos a través de constructores de sitios web utilizados por agencias creativas y digitales, emplearon un script de redireccionamiento que envió a las víctimas a un dominio malicioso propiedad de los autores de Shylock. A partir de ahí, el malware Shylock se descargó e instaló en los sistemas de aquellos que navegan en sitios web legítimos. Mediante la integración de una multitud de características diferentes adoptadas a partir de otro malware, Shylock fue capaz de realizar ataques personalizables de "hombre en el navegador", evitando la detección y protegiéndose del análisis. En lugar de comprometer individualmente varios sitios legítimos, el ataque se centró en el script principal de una plantilla de sitio web diseñada por una agencia digital creativa de Reino Unido.

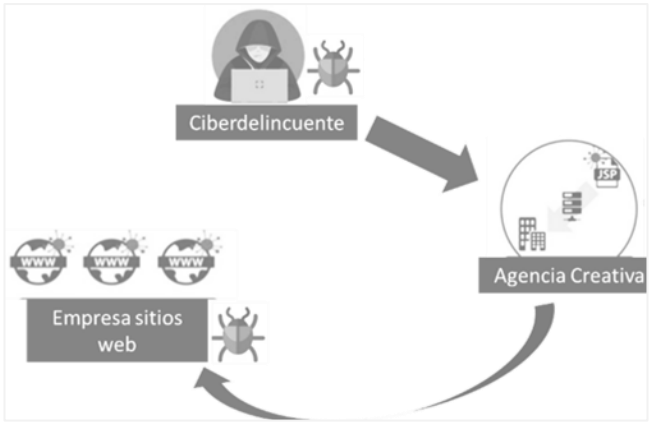

Fig. 5. Ejemplo de ciberataque a constructores de sitios web [12].

C. Ataques a tiendas de datos de terceros.

Muchas empresas modernas subcontratan sus datos a empresas de terceros que registran, almacenan, procesan y negocian la información, estos serían proveedores de datos que muchas veces no tiene relación con los clientes, como por ejemplo un proveedor de datos de terceros podría pagar a los editores o medios de comunicación online para recopilar información acerca de sus visitantes y lo utilizan para reconstruir los perfiles detallados sobre los gustos y comportamientos de los usuarios para posteriormente vender esta información a los anunciantes, con el fin de ayudarles a dirigir sus compras de anuncios enfocados a los clientes potenciales, dichos datos confidenciales no son necesariamente sólo acerca de los clientes, sino que también podrían abarcar la estructura del negocio, el estado financiero, la estrategia y la exposición al riesgo [12] [13].

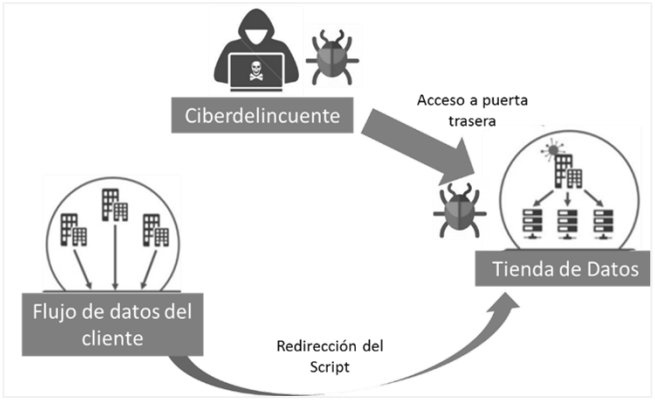

Fig. 6. Ejemplo de ciberataque a la cadena de suministro por medio de las tiendas de datos de terceros [6].

En septiembre de 2013, se presentó un ejemplo para este caso, en el cual se informó que varias redes pertenecientes a grandes recopiladores de datos estaban en peligro, los ciberdelincuentes lograron implantar un pequeño botnet (bot o robot que es capaz de expandirse en una red e implantar malware para controlar remotamente los equipos infectados), este extraía información de los sistemas internos de numerosos almacenes de datos, a través de un canal encriptado a un controlador de botnet en internet. La víctima de más alto perfil fue un recopilador de datos que otorga licencias de información sobre empresas y corporaciones para su uso en decisiones de crédito, marketing de empresa a empresa y gestión de la cadena de suministro. Si bien es posible que los atacantes buscaran datos de consumidores y empresas, los expertos en fraude sugirieron que la información sobre hábitos y prácticas de consumidores y empresas era la más valiosa. La víctima era una agencia de informes crediticios para numerosas empresas, que proporcionaba "autenticación basada en el conocimiento" para solicitudes de transacciones financieras. Este compromiso de la cadena de suministro permitió a los atacantes acceder a información valiosa almacenada a través de un tercero y posteriormente cometer fraude a gran escala [12].

D. Ciberataques a la cadena de suministro

En la siguiente parte se explican sólo algunos, de tantos ciberataques que se han presentado a nivel mundial.

1) CCleaner: En agosto de 2017, una popular herramienta de limpieza de sistemas llamada “CCleaner” fue atacada por los ciberdelincuentes desde la cadena de suministro. Un grupo desconocido de atacantes obtuvo acceso al entorno de desarrollo de la empresa, lo que les permitió crear y distribuir una versión maliciosa de la herramienta a través del proceso de actualización. El éxito de la campaña se vio favorecido por el hecho de que los ciberdelincuentes pudieron firmar la actualización infectada con la firma digital oficial del fabricante. Entre el 15 de agosto y el 12 de septiembre, la versión comprometida, CCleaner v5.33.6162, y la versión en la nube se distribuyeron a los clientes. Según las cifras de Avast, la versión modificada se descargó 2,27 millones de veces [14].

2) NotPetya: Fue un ataque global cibernético a gran escala que afectó organizaciones en Ucrania, Australia, España, Estados Unidos entre otros. En el que los expertos en seguridad informática inicialmente pensaron que era un tipo de ramsonware como Petya (un virus que secuestra los datos o sistemas, el cual bloquea el acceso a los datos del equipo y exige dinero para su devolución), pero pronto se hizo evidente que no era un Petya, por lo tanto lo denominaron NotPetya, porque aunque se disfrazó como un ransomware, su verdadero propósito era propagarse rápidamente y causar daños a las redes de las TIC en lugar de recaudar dinero. Casi el 70% de los ataques NotPetya fueron a empresas, agencias gubernamentales e individuos de Ucrania.

Los expertos indican que NotPetya genera para cada computadora afectada, una identificación aleatoria, que se usa para guardar información sobre cada víctima infectada y la clave de descifrado. Dado que el virus genera datos aleatorios para esa ID en particular, el proceso de descifrado se vuelve imposible, lo que significa que las víctimas no recuperan sus datos. El vector de infección original parece ser a través de una puerta trasera plantada en una nueva actualización de Medoc, (un programa de contabilidad que es utilizado por casi todas las empresas de Ucrania), el cual habiendo infectado computadoras de los servidores de Medoc, NotPetya usó una variedad de técnicas para propagarse a otras computadoras, incluyendo EternalBlue y EternalRomance y dos exploits desarrollados por la NSA de los Estados Unidos para aprovechar un error en la implementación de Windows del protocolo SMB.

Este malware interrumpió el funcionamiento de los servicios de los bancos, electricidad, aeropuertos y metro en Ucrania, para luego extenderse globalmente, afectando a las empresas internacionales en cientos de millones de dólares. En junio del 2017 el gobierno de los Estados Unidos emitió en un comunicado de prensa, acusando a las fuerzas armadas rusas de iniciar el ataque cibernético más destructivo y costoso en la historia, utilizando el virus NotPetya. Así mismo el gobierno de Australia manifestó que se ha unido a los Estados Unidos y el Reino Unido para condenar a Rusia por el uso del malware 'NotPetya' para atacar infraestructura crítica y negocios [15]. El Ministro de Infraestructura de Ucrania, “Volodymyr Omelyan”, dijo a Associated Press que su departamento enfrenta "millones" en costos relacionados y agregó que cientos de estaciones de trabajo de su agencia estaban deshabilitadas y que dos de sus seis servidores están en peligro [16].

Por otra parte, FedEx (una compañía aérea y logística de origen estadounidense, que tiene cobertura a nivel internacional), admitió recientemente que algunos de sus sistemas se han visto afectados de manera significativa y permanente por el malware.

3) Equifax: Fue el ataque que ha sido catalogado como la fuga más grave de datos de la historia y quien se llevó, la primera posición del ranking de la revista Forbes, sin lugar a dudas, la empresa global de soluciones de información Equifax, quien fue víctima de una fuga de datos, catalogada como la más grave de la historia, la cual supuso de la exposición de información sensible de más de 143 millones de personas, incluyendo números de la seguridad social, direcciones, información bancaria, etc. Esta información se estima que vale alrededor de 30 dólares por archivo en el mercado negro, lo que otorga un potencial valor de hasta 4.200 millones de dólares al robo. El ataque consistió en el aprovechamiento de una vulnerabilidad pública del servidor web “Apache” en el que residía el sitio web de Equifax. El CEO de la empresa anunció, posteriormente al incidente, 5 paquetes de servicios para sus clientes “libres de cargos” (pagados por Equifax) y acto seguido renunció a su cargo [17].

4) Cronbot: Es el primer troyano de banca móvil, en mayo de 2017 fueron arrestados un grupo de ciberdelincuentes que utilizaron un troyano bancario llamado "Cronbot" para robar más de $ 900,000 mil dólares de cuentas bancarias luego de infectar a más de un millón de móviles Android, los ciberdelincuentes escondieron el troyano dentro de una serie de aplicaciones falsas, algunas diseñadas para parecerse a las auténticas aplicaciones de banca en línea y otras diseñadas para parecerse a aplicaciones de pornografía. Estos atacantes conocían su objetivo principal, pues más de un millón de usuarios desprevenidos descargaron e instalaron el aplicativo de Google Play, infectando sus dispositivos móviles Android. Las aplicaciones se agregaron al auto arranque y el malware oculto que estaba dentro, les otorgó a los ciberdelincuentes la capacidad de falsificar las credenciales bancarias de las víctimas e interceptar mensajes SMS que contenían códigos de confirmación enviados por el banco para así verificar las transacciones. Recientemente, el equipo de Avast “Threat Labs” ha descubierto y analizado una nueva versión del malware, denominado Catelites Bot, el cual comparte similitudes con el malware utilizado para Cronbot. Si bien no se tienen pruebas contundentes de que el actor de Catelites esté vinculado a Cronbot, es probable que los miembros de Cronbot hayan utilizado el malware de Catalites en sus campañas. En los últimos meses, se ha visto una o dos aplicaciones falsas por semana atacando dispositivos Android para que las víctimas desprevenidas descarguen el malware, una vez descargados, los ciberdelincuentes utilizan trucos de ingeniería social muy sofisticados para obtener información de la tarjeta de crédito y para posiblemente ingresar a la cuenta bancaria de la víctima [18].

Este último ataque es importante analizarlo para entender la estrategia que los ciberdelincuentes utilizan para llevar a cabo

el engaño, no obstante, la compañía de Avast revela que cuando el usuario hace clic en el icono de la aplicación (aplicación de sistema) maliciosa, le pedirá derechos de administrador. Si se otorgan esos permisos, el malware comienza a funcionar el ícono de la aplicación (falsa) que el usuario descargó desaparece y luego tres íconos de la aplicación de confianza que parecen familiares se colocan en la pantalla de inicio, uno para Gmail, uno para Google Play y uno para Chrome. El autor del malware utiliza sofisticadas técnicas de "ingeniería social" para alentar al usuario a que abra una de estas tres aplicaciones con el fin de mostrar una superposición falsa que lo invite a ingresar información confidencial como su tarjeta de crédito. Los ciberdelincuentes cuentan con el hecho de que el usuario ingresa fácilmente información de tarjetas de crédito para compañías respetables a las que probablemente compra regularmente.

Claramente con el ejemplo anterior se aprecia cómo los ciberdelincuentes utilizan el nombre de empresas reconocidas para valerse de la confianza que generan dichas compañías y en dos sencillos pasos lograr un posible robo masivo a usuarios confiados o desprevenidos, como la creación de iconos duplicados de tres aplicaciones conocidas (Gmail, Google Play y Chrome) y crear una notificación que no se puede eliminar y que lo vincula a un "inicio de sesión" falso en su cuenta Al colocar estas aplicaciones en la pantalla de inicio, es más probable que el usuario las abra y active el malware para que el delincuente pueda robar información confidencial [18].

Ahora bien, por último y para reflejar todos los niveles de riesgos de los ataques a la cadena de suministros, evidenciando no solo que ocurren en las grandes organizaciones o solo en países europeos lejanos de la realidad, se expone el ataque la compañía de Pizza Hut.

5) Ciberataque a Pizza Hut: El 14 de octubre de 2017, Pizza Hut notificó a aproximadamente 60,000 clientes, por correo electrónico, que los ciberdelincuentes pusieron en peligro su información personal. La filtración ocurrió el 1 y 2 de octubre, pero la compañía esperó dos semanas para informar a los clientes y el ataque duró aproximadamente 28 horas, por lo que cualquier persona que ordenó a Pizza Hut a través de la aplicación móvil durante ese tiempo puedo haberse visto afectada.

Los ciberdelincuentes robaron nombres, direcciones de entrega, códigos postales de facturación, números de tarjetas de crédito, números de CVN y direcciones de correo electrónico. A pesar de que Pizza Hut emitió un comunicado diciendo que detectó rápidamente la filtración y solucionó de inmediato la situación, varios clientes tuitearon comentarios sobre cuánto tiempo tomó revelar los detalles del acceso de datos. A varias víctimas se les agotaron los fondos en sus cuentas bancarias [19].

V. BUENAS PRÁCTICAS PARA GESTIONAR LOS RIESGOS DE LA CADENA DE SUMINISTRO

La seguridad de la cadena de suministro, incluye una gran parte de las operaciones e información de las organizaciones, como ya se ha explicado, por lo tanto los riesgos y amenazas son significativos y letales para una organización, es por esto la gran importancia de reconocer los principales riesgos a que están expuestas las organizaciones con la cadena de suministro. Por lo tanto, un informe que en mi opinión es muy preciso y concreto es el informe de la NIST (National Institute of Standards and Technology), “Best Practices in Cyber Supply Chain Risk Management” el cual indica dónde y cuáles son los principales riesgos de la cadena de suministro, denominados “riesgos clave de la cadena de suministro” [20].

Los proveedores de servicios externos, desde servicios de mensajería hasta la producción o abastecimiento de software, cuentan algunos con acceso físico o virtual a los sistemas de información, código de software o a la IP, prácticas de seguridad de la información en algunos casos son deficientes por los proveedores de niveles inferiores, software o hardware comprometido que se ha comprado a proveedores, vulnerabilidades de seguridad del software en la administración de la cadena de suministro o sistemas de información de los proveedores, hardware falsificado o hardware con malware infiltrado, almacenamiento de datos de terceros o recopiladores de datos, entre otros.

Con base en lo anterior, es fundamental tener en cuenta que, para gestionar los riesgos de la cadena de suministros, lo primero que deben hacer las organizaciones es detectar y reconocer esas vulnerabilidades y amenazas a las que están expuestas por parte de terceros.

Así mismo, se deben saber y conocer quiénes son sus proveedores o terceros con quien comparte información o están ligados a ellos, esta tarea se puede realizar a través de la administración y gestión de proveedores o terceros, estableciendo requisitos de cumplimiento y seguridad a los servicios prestados, es probable que los requisitos más explícitos sean comunes en la mayoría de las principales políticas de cumplimiento. Por lo tanto, las organizaciones deben estar al tanto de todos los requisitos y estándares y hacer las revisiones necesarias en las políticas o procedimientos para acomodar esos cambios. La siguiente grafica representa a grandes rasgos como realizar un programa de administración y gestión de seguridad para la cadena de suministro [21].

Fig. 7. Programa para la administración de proveedores [21].

De la misma manera, INCIBE (Instituto Nacional de Ciberseguridad de España), expone algunos puntos clave para gestionar los riesgos asociados a la cadena de suministro

como, revisiones previas de los proveedores, utilización de almacenes y transportes seguros, empleabilidad de análisis independientes de los productos y servicios (según se recoge en el requerimiento SA-12 de la NIST SP 800-53), procedimientos para evaluar las amenazas de los proveedores potenciales de componentes críticos de los sistemas (maximizar la visibilidad), procesos para detectar la ocurrencia, reducción de la probabilidad y mitigación de las consecuencias de productos falsificados o con componentes maliciosas, mejoras en las pruebas de detección de vulnerabilidades, incluyendo soluciones automatizadas, selección de lenguajes de programación y herramientas que contrarresten las debilidades, reducción de los riesgos durante las actualizaciones de software y gestión de parches.

A. Ciberseguridad en la cadena de suministro.

Es fundamental comprender que la seguridad de la cadena de suministro es un programa en el que se centra en los riesgos y vulnerabilidades potenciales asociados con los proveedores de bienes y servicios de una organización, muchos de los cuales pueden tener acceso privilegiado a recursos e información dentro del entorno de la organización o entorno a los clientes de la organización, los cuales pueden ser sensibles y privados. Podría haber muchas formas de ocurrir una violación a la cadena de suministro.

Por ejemplo, un fabricante de software podría ser comprometido a través de malware que modifica el código fuente que luego se distribuye en las empresas que usan el software. Otro vector de compromiso común podría ser el robo de las credenciales de un proveedor que otorga acceso remoto a una empresa con la que trabaja el proveedor, lo que lleva a la infiltración de la red de la organización desde una fuente confiable que sería la red de su proveedor [22].

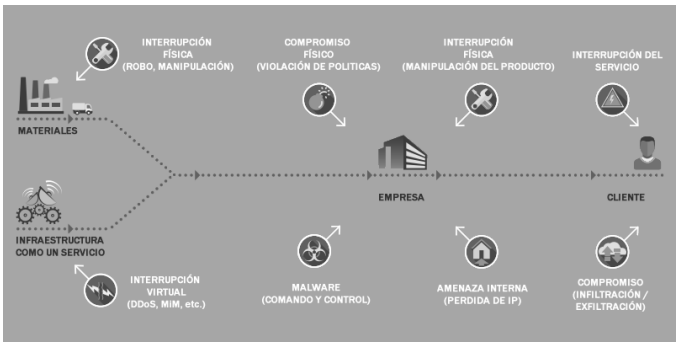

Fig. 8. Ejemplo de una filtración típica a la cadena de suministro, según [22].

B. Políticas y estándares de aplicación.

Una vez que se tienen reconocidos los riesgos de seguridad en la cadena de suministro, es primordial conocer y aplicar todos los lineamientos, políticas y estándares tanto nacionales como internacionales, disponibles por las diferentes instituciones de normalización, los cuales se convierten en un buen referente para que las organizaciones opten por implementar y poder mitigar estos riesgos.

Uno de los principales estándares a tener en cuenta para aplicar no solo en los riesgos de la cadena de suministro, sino al interior de cada organización, es el estándar ISO/IEC 27032, ya que los ciberataques son la modalidad de robo que está de moda y aunque esta norma fue publicada desde el año 2012, la mayoría de organizaciones no la aplica o ni siquiera saben que existe. Siendo esta norma un marco de referencia para la toma de decisiones y para la resolución de temas en cuanto a la ciberseguridad.

1) ISO/IEC 27032:2012 "Tecnología de la información - Técnicas de seguridad - Directrices para la ciberseguridad": Esta norma, es una guía de implementación de buenas prácticas para el mejoramiento de la "Ciberseguridad" o "Seguridad en el Ciberespacio", esta norma no es certificable como la ISO 27001, pero las organizaciones si la pueden alinear a sus análisis y buenas prácticas en la seguridad informática. El alcance y la aplicación de la norma ISO 27032, abarca la protección de la información, protección de las redes, protección de internet y protección de la infraestructura de información crítica.

Los objetivos o fines de esta norma comprenden, la visión general de ciberseguridad, interrelación, ciberseguridad y otros tipos de seguridad, definición de cuáles son las partes interesadas/involucradas, métodos para tratar asuntos comunes de ciberseguridad y marco de referencia para partes involucradas. Así mismo, señala las partes interesadas del ciberespacio y las clasifica en grupos como, el consumidor que son los individuos, las organizaciones ya sean públicas o privadas y los proveedores incluyendo los proveedores de servicio de internet y aplicaciones. [23].

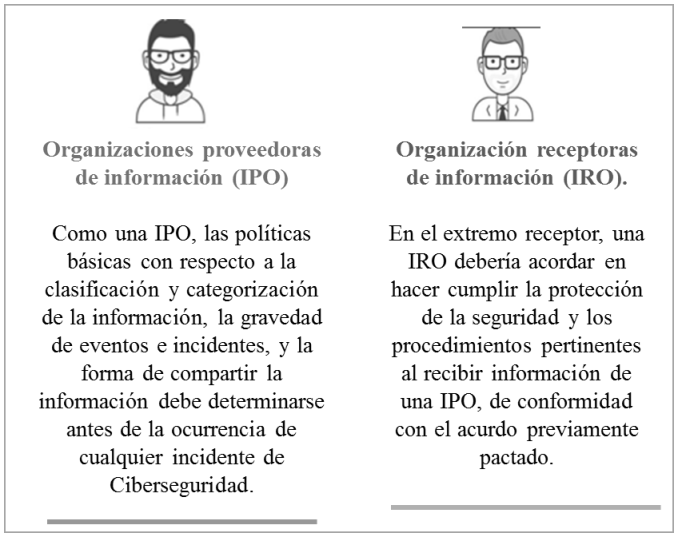

Fig. 9. Partes interesadas de la ciberseguridad, según la ISO/IEC 27032 [23]

La cláusula 11, se enfoca en las directrices para las partes interesadas, las cuales deben tener una guía de protección para los consumidores, requisitos de protección que los proveedores deben especificar, para que los consumidores lo implementen, entre otros. Así mismo indica que las recomendaciones se deben estructurar primero con una introducción a la evaluación y tratamiento del riesgo, directriz para los consumidores y directriz para las organizaciones. Una vez que los riesgos de ciberseguridad se identifican la norma brinda lineamientos apropiados y propone 4 tipos de controles para la ciberprotección, controles a nivel de aplicación, protección del servidor, controles para los usuarios finales y controles contra los ataques de ingeniería social. Estos

controles son desglosados por ítems, los cuales son recomendables analizar y aplicar en cada organización, así como detallar el estándar ISO/IEC 27032:2012 "Tecnología de la información - Técnicas de seguridad - Directrices para la Ciberseguridad".

2) Norma Técnica Colombiana NTC-ISO 28000: Sistema de Gestión de Seguridad de la Cadena de Suministro. Aunque esta norma describe los requisitos de un sistema de gestión de seguridad en un ámbito físico, es relevante para este artículo ya que incluye aspectos críticos para el aseguramiento de la cadena de suministro, esta norma indica que la seguridad está relacionada con muchos otros aspectos de la gestión empresarial, que abarca todas las actividades controladas en todo su ciclo de vida y que impacta en la seguridad de la cadena de suministro.

Esta norma es aplicable para todas las organizaciones de todos los tamaños y sectores sin importar su naturaleza y en cualquier etapa de la producción o la cadena de suministro que se desee [24].

El objetivo y propósito principal de esta norma es establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad, asegurar la conformidad con la política de gestión de la seguridad establecida, demostrar dicha conformidad ante otros, buscar la certificación o registro del sistema de gestión de la seguridad por un organismo de certificación de tercera parte, acreditado y realizar una autodeterminación y auto-declaración de la conformidad con esta norma. Por último, las anteriores precisiones se tomaron explícitamente de la norma técnica colombiana NTC-ISO 28000 para no alterar sus requisitos.

TABLA IV.
REVISIÓN POR LA DIRECCIÓN Y MEJORA CONTINUA [24]

Verificación y acción correctiva	Medición y seguimiento.
	Evaluación del sistema.
	No conformidad y acción correctiva y preventiva
	Registros.
	Auditorias.

TABLA V.
POLÍTICA DE GESTIÓN DE LA SEGURIDAD [24]

Planificación de seguridad	Evaluación del riesgo.
	Requisitos de reglamentación.
	Objetivos y metas de seguridad.
	Programas de gestión de la seguridad.
Implementación y operación	Responsabilidades y competencia.
	Comunicación.
	Documentación.
	Control operacional.
	Preparación para emergencias.

3) ISO / IEC 27036: Tecnología de la información - Técnicas de seguridad - Seguridad de la información para las relaciones con los proveedores. Esta norma es un estándar de varias partes que ofrece orientación sobre la evaluación y el tratamiento de los riesgos de información involucrados en la adquisición de bienes y servicios por parte de los proveedores. El contexto implícito son las relaciones entre empresas, en lugar de la venta minorista, y los productos relacionados con la información, esta norma brinda un marco operacional para ayudar a las organizaciones a garantizar el proceso de gestión de la seguridad de su información y sus sistemas de información en su relación con los proveedores.

El alcance y propósito siendo un estándar de seguridad de la información, son los servicios de externalización de TI y computación en la nube y otros servicios profesionales, por ejemplo guardias de seguridad, limpiadores, servicios de entrega (correos), mantenimiento o servicio de equipos, servicios de consultoría y asesoramiento especializado, gestión del conocimiento, investigación y desarrollo, fabricación, logística, custodia de código fuente y atención médica; suministro de hardware, software y servicios de TIC, incluidos servicios de telecomunicaciones e internet; productos y servicios a medida en los que el adquirente especifica los requisitos y, a menudo, desempeña un papel activo en el diseño del producto (a diferencia de los productos básicos y los productos estándares disponibles en el mercado). utilidades tales como energía eléctrica y agua [25]. En la siguiente tabla se relacionan y las partes que componen este estándar. La primera parte de la norma define el problema y corrige los conceptos clave, sin tener en cuenta la relación de tipos de relaciones con los proveedores de servicios.

TABLA VI.
PARTES DE LA NORMA ISO / IEC 27036 [25]

ISO / IEC 27036-1	Parte 1	Visión general y conceptos
ISO / IEC 27036-2	Parte 2	Requisitos
ISO / IEC 27036-3	Parte 3	Directrices para la seguridad de la cadena de suministro de tecnología de información y comunicación
ISO / IEC 27036-4	Parte 4	Directrices para la seguridad de los servicios en la nube

La siguiente gráfica explica la cadena de suministro de TIC donde los compradores y proveedores a lo largo heredan los riesgos asociados con los sub-proveedores de productos y servicios, reconociendo la complejidad de encontrar quién controle el proceso debido a la poca visibilidad a medida que avanza por la cadena.

Por último, es importante resaltar los planteamientos del Instituto Nacional de Ciberseguridad INCBE, quien afirma que para poder llegar a un cumplimiento y estructuración de

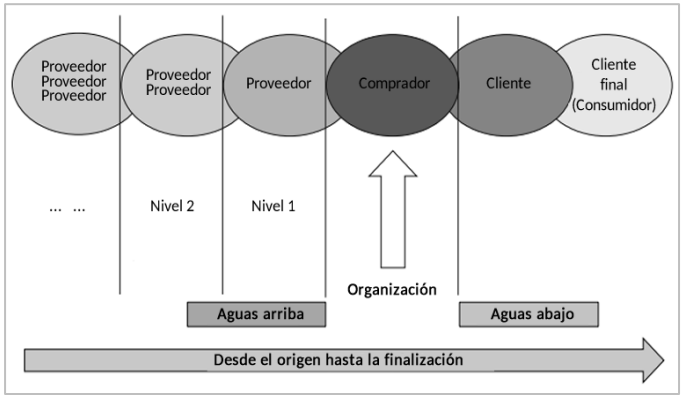

Fig. 10. Relaciones de la cadena de suministro [25]

un buen plan de control del riesgo en la cadena de suministro y todas las actividades correspondientes, se debe implicar la necesidad de recursos suficientes para las actividades de gestión de riesgos en la cadena de suministros TIC, un gobierno adecuado de estos aspectos, procesos y procedimientos para mejorar la confianza y reducir el riesgo, métodos contractuales y legales para evitar utilizar proveedores con demasiado riesgo y revisar las políticas para considerar la gestión de este riesgo.

VI. CONCLUSIONES

Conforme a los riesgos cibernéticos asociados a la cadena de suministro y las estadísticas expuestas en este artículo, gran parte de las organizaciones no están preparadas para mitigar ni gestionar estos riesgos, ya que no conocen las vulnerabilidades de sus proveedores, socios y clientes que están vinculados a ellas o simplemente no saben quiénes son. Es importante que se dé a conocer a la alta gerencia y su equipo de seguridad informática, la cadena de suministro de la organización, sus falencias y vulnerabilidades asociadas y así mismo tomar medidas correctivas para la protección contra estos ciberataques, como por ejemplo, aplicando la normalización, estándares y políticas relacionadas a estos riesgos, que pueden guiar a pequeñas, medianas y grandes organizaciones a mitigar estos riesgos del ciberespacio.

Por último, aunque en Colombia la inversión hacia la seguridad informática disminuyó considerablemente, es importante dar a conocer la norma nacional donde guía a las organizaciones a gestionar y mitigar los riesgos expuestos en la cadena de suministro.

REFERENCIAS

[1] Conner, "Threat Intelligence, Industry Analysis and Cybersecurity Guidance for the Global Cyber Arms Race", SonicWall Inc., Milpitas, California, Cyber threat report, 2018.

[2] L. Corrons, "Informe anual PandaLabs 2017", Panda Security, Bilbao España, Informe annual, Nov 2017. [Online] Available: https://www.pandasecurity.com/spain/mediacenter/pandalabs/informe-anual-y-predicciones-2018.

[3] Colombia Digital, "Ciber-resiliencia: una estrategia de seguridad para las empresas", Corporación Colombia Digital, Colombia, febrero 2015 in [Online] https://colombiadigital.net/actualidad/noticias/item/8144-ciber-resiliencia-una-estrategia-de-seguridad-para-las-empresas.html.

[4] S. Moore, "Gartner Says Worldwide Information Security Spending Will Grow 7 Percent to Reach $86.4 Billion in 2017", Gartner, Australia, in [Online]https://www.gartner.com/newsroom/id/3784965.

[5] J. Cano, Diario el Portafolio, "El 59% de las empresas locales recortaría gastos en ciberseguridad", Colombia, enero 2017, in [Online] http://www.portafolio.co/negocios/empresas/empresas-locales-recortaria-gastos-en-ciberseguridad-502771.

[6] Norma técnica colombiana: sistemas de gestión de la seguridad para la cadena de suministro, NTC-ISO 28000, 2008.

[7] Modelo nacional de gestión de riesgos de seguridad digital, para ser aprobado por MINTIC Colombia 2017.

[8] Sebastian Z, Symantec, "Part 3 - Various types of network attacks" Symantec Corporation, USA, Diciembre 2018 in [Online] https://www.symantec.com/connect/articles/security-11-part-3-various-types-network-attacks.

[9] J. Boyens, "Integrating Cybersecurity into Supply Chain Risk Management" in RSA Conference 2016, San Francisco, 2016.

[10] K. Baumgartner,, "Boletín de seguridad kaspersky: predicciones sobre amenazas para el 2018", Kaspersky, Noviembre 2017.

[11] Symantec, "Executive Summary 2018 Internet Security Threat Report", Symantec Corporation, USA, March 2018.

[12] NCSC, "Guidance Example supply chain attacks", The National Cyber Security Centre, Londres, enero 2018 in [Online] https://www.ncsc.gov.uk/guidance/example-supply-chain-attacks.

[13] Oniup, "Definición de Third Party Data" Agencia de marketing digital, Oniup.com in [Online] https://oniup.com/que-es/third-party-data.

[14] ISTR Symantec, "Executive Summary 2018 Internet Security Threat Report", Symantec Corporation, USA, March 2018. Vol 123 04/18

[15] ENISA, European Union Agency for Network and Information Security., "Supply chain attacks", Colombia, August 2017, in [Online] https://www.enisa.europa.eu/publications/info-notes/supply-chain-attacks.

[16] ID AGENT, "NotPetya – a Threat to Supply Chains", USA, August 2017, in [Online] https://www.idagent.com/2017/08/03/notpetya-threat-supply-chains-across-ukraine/

[17] Forbes Media LLC, "A Brief History Of Equifax Security Fails", USA, Sep 2017, in [Online] https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#62552cdd677c.

[18] N. Chrysaidos, "New malware targets accounts at over 2,200 financial institutions", Avast Inc., USA, Diciembre 2017, in [Online] https://blog.avast.com/new-version-of-mobile-malware-catelites-possibly-linked-to-cron-cyber-gang

[19] Forbes Media LLC, "Los 10 ciberataques más duros de 2017", USA, Sep 2017, in [Online] http://forbes.es/life/37293/los-10-ciberataques-mas-duros-2017/3/

[20] Departament of Comerce, "Best Practices in Cyber Supply Chain Risk Management", NIST - (National Institute of Standards and Technology), USA, 2017.

[21] Modelo nacional de gestión de riesgos de seguridad digital, para ser aprobado por MINTIC Colombia 2017.

[22] D. Shackleford, "Combatting Cyber Risks in the Supply Chain", SANS Institute InfoSec, Sept 2015.

[23] A. Ramos García, "Gestión de riesgos en la cadena de suministro TIC", Instituto Nacional de Ciberseguridad., España, May 2012, in [Online] https://www.incibe.es/protege-tu-empresa/blog/post-riesgos-suministro.

[24] C. Birarda, "Ciberseguridad ISO/IEC 27032" in Conference cybersecurity governance space, centro de certificación y capacitación 360, Feb 2018.

[25] Norma técnica colombiana: Sistemas de gestión de la seguridad para la cadena de suministro, NTC-ISO 28000, 2008.

[26] Modelo nacional de gestión de riesgos de seguridad digital, para ser aprobado por MINTIC Colombia 2017.

[27] International standard: Information technology — Security techniques Information security for supplier relationships —ISO/IEC 27036, 2014.

Autor

Díaz Bermúdez Sandra, (1987) Bogotá, Colombia. Ingeniera de Sistemas de la Universidad de Cundinamarca, estudiante de especialización en Seguridad Informática de la Universidad Piloto de Colombia. Conocimientos y experiencia en el desarrollo y administración de proyectos TI, records management, análisis y levantamiento de información. Asesora en planeación e implementación de proyectos en sistemas de gestión de documento electrónico de archivo, basados en políticas y estándares archivísticos a nivel tecnológico del Archivo General de la Nación.