uc3m | Universidad Carlos III de Madrid

Máster Universitario en Ciencias Actuariales y Financieras
2016-2017

Trabajo Fin de Máster

"Modelo de Gestión Integral del Ciber riesgo"

Daniel Arturo Hoyos Nieto

Tutor/es

JOSÉ MIGUEL RODRÍGUEZ-PARDO DEL CASTILLO

JESÚS RAMÓN SIMÓN DEL POTRO

Madrid, 13 de Junio de 2017

Daniel Hoyos

Resumen

Este trabajo pretende aportar una metodología que permita a las organizaciones identificar, analizar y evaluar el ciber riesgo como herramienta para establecer diferentes medidas, procesos y sistemas de acción para gestionarlo. El trabajo se encuentra dividido en cuatro capítulos. El primer capítulo define el Ciberespacio, el segundo aporta un concepto para el Ciber riesgo identificando la importancia de este y la posibilidad de que pudiese representar una catástrofe para la humanidad. El tercer capítulo presenta un sistema de gerencia y gestión del Ciber riesgo y el cuarto y último capítulo aporta una serie de herramientas para cuantificar el Ciber riesgo de forma actuarial.

Palabras Clave

Ciber riesgo, Ciberespacio, ciberseguridad, gestión del riesgo, ISO 31000:2009, ISO 27005:2011.

Abstract

The objective of this work is to provide a methodology that allows organizations to identify, analyze and evaluate risk as a tool to establish different measures, processes and management action systems.

The work has four chapters. The first chapter defines Cyberspace, the second one provides a concept for cyber risk, identifying the importance of cyberspace and the possibility that it could represent a catastrophe for humanity. The third chapter presents a cyber risk management and management system and the fourth and last chapter provides a series of tools to quantify cyber risk in actuarial form.

Key Words

Cyber risk, Cyberspace, cybersecurity, risk management, ISO 31000: 2009, ISO 27005: 2011.

Contenido

1. Introducción.

Mientras se desarrollaba este trabajo el mundo ha sido testigo del que quizá es el mayor ciberataque lanzado hasta la fecha, un ciberataque de ransomware que afectó los sistemas informáticos de un sinnúmero de países y organizaciones, la prestación de los servicios se ha visto comprometida con consecuencias que van desde lo económico hasta la seguridad de la vida humana (Oliveira & Jiménez Cano, 2017).

El Ciberespacio se presenta muchas veces como algo difuso y lejano, sin embargo, es una nueva realidad en la sociedad que da lugar a una nueva dimensión donde los seres humanos pueden interactuar y generar beneficios, aún así, las organizaciones recién están despertando a los innumerables riesgos que involucra esta nueva realidad.

Aunque no se perciba, la existencia dentro de una organización de sistemas conectados al ciberespacio genera que el ciber riesgo se encuentre por todas partes; las organizaciones no saben cómo gestionar este tipo de riesgo y peor aún, no sospechan cuanto podría costarles un incidente cibernético del cual –en la mayoría de los casos– presumen lejano a su actuar.

El objetivo de este trabajo es aportar una metodología que permita a las organizaciones identificar, analizar y evaluar el ciber riesgo como herramienta para establecer diferentes medidas, procesos y sistemas de acción que faciliten su gestión.

Para tal propósito el trabajo cuenta con cuatro capítulos. El primero de ellos aporta una definición del Ciberespacio tratando de acotar las consecuencias y límites que puede traer esta nueva dimensión para la sociedad, por otro lado se introduce el concepto de ciberseguridad y la relación que puede establecer con otros niveles de seguridad. El segundo es un capítulo que –partiendo de la definición de Riesgo–

trata de aportar un concepto para el Ciber riesgo identificando la importancia de este y la posibilidad de que pudiese representar una catástrofe para la humanidad.

El tercer capítulo presenta un sistema de gerencia y gestión del Ciber riesgo utilizando como guía la norma ISO 31000:2009 que señala una familia de normas sobre la gestión del riesgo, complementadas por otra serie de normas ISO relacionadas con la gestión de la ciberseguridad como la norma ISO 27005:2011. El propósito de este capítulo es claramente el proporcionar una serie de principios y directrices que permitan implementar y gestionar el Ciber riesgo a nivel estratégico y operativo.

El cuarto y último capítulo contiene el análisis actuarial de la frecuencia y la severidad de una información que contiene registros de datos comprometidos en la violación a sistemas de compañías desde el año 2005. En el último apartado de este capítulo se introduce la utilización de las redes neuronales para el análisis actuarial.

Con este trabajo se pretende aportar una herramienta para los gerentes de riesgo de las diferentes compañías que sirva como punto de partida para la implementación de sistemas de gestión integral del ciber riesgo.

2. El Ciberespacio y la Ciberseguridad.

2.1 El Ciberespacio, una nueva dimensión en la sociedad.

Ciber proviene del inglés Cyber (Real Academia de la Lengua Española, 2014), prefijo que significa el involucramiento, el uso o la relación que se establece con los ordenadores y especialmente con Internet (Cambridge University Press, 2017).

La palabra Ciberespacio, aparece por primera vez en la novela de ciencia ficción Neuromante de William Gibson y la adopción de esta palabra por parte de los aficionados y profesionales en informática se da a comienzos de los años noventa (Strate, 2009). En Neuromante, Gibson explora las posibilidades de las tecnologías de la información mucho antes de que se popularizara el uso de Internet, el escritor describe el ciberespacio como parte de un escenario del futuro cercano donde existen conexiones neuronales entre los seres humanos y los ordenadores, todos vinculados a una vasta computadora llamada Matrix (Dodge & Kitchin, 2001).

Desde que apareció la palabra se ha recurrido a muchas definiciones, comenzando por Gibson que la presenta como una fantasía, pasando a otros autores que la consideran como algo real y presente y unos más que la equiparan a la realidad virtual. El término se ha aplicado a una variedad de fenómenos relacionados con la informática y la comunicación entre computadoras. De esta manera una temprana aproximación a Ciberespacio correspondió a las diversas experiencias de espacio asociado con la informática y sus tecnologías relacionadas. (Strate, 2009)

A comienzos del segundo milenio, los autores comienzan a entender que el ciberespacio no sólo establecía relaciones entre redes informáticas, sino también estaba alterando las relaciones entre los seres humanos y la sociedad. Además, la extensión y uso del ciberespacio crecía rápidamente, con más de mil millones páginas web accesibles al público en el año 2000 y el número de otros medios como correo electrónico, salas de chat y mundos virtuales también había crecido

significativamente, el ciberespacio se había convertido en un entidad confusa difícil de supervisar y navegar (Dodge & Kitchin, 2001)

De esta manera encontramos que el ciberespacio se convirtió en un lugar virtual, un espacio al que se puede acceder a través de redes informáticas interconectadas y en el que se realizan interacciones entre agentes (Ploug, 2009). Esta definición aporta tres componentes que merecen la pena analizarse individualmente: la virtualidad, la relación establecida en red y la interacción.

La virtualidad. Hace referencia a la independencia espacio temporal. En otras palabras, el ciberespacio no requiere necesariamente que las partes que interactúen estén en el mismo lugar o en un momento determinado. Al ser un lugar virtual o un espacio para la interacción, el ciberespacio es claramente un cuasi lugar, no es un lugar en el sentido estricto de la palabra, dado que tendría que ocupar un lugar particular en el espacio tiempo (Ploug, 2009).

Relación establecida en red. El ejemplo más destacado de un Ciberespacio es Internet, pero sólo es un ejemplo de lo que realmente es (Refsdal, Solhaug, & Stølen, 2015), por lo tanto, Ciberespacio no es un mero sinónimo de Red, pero sí depende de la existencia de la misma, si la red o la conexión deja de existir también dejará de existir el Ciberespacio (Ploug, 2009).

Interacción. Entendida como la relación entre dos o más sujetos, el ciberespacio ha permitido dicha interacción entre individuos, organizaciones y ordenadores. Esto ha permitido que muchas interacciones que se establecían en el mundo físico, se trasladaran al ciberespacio. Existen innumerables ejemplos de interacciones en el ciberespacio, uno de ellos corresponde a la banca por Internet, la cual permite que los clientes mediante un ordenador y un programa específico puedan acceder a sus cuentas bancarias con el fin de realizar pagos o transferir dinero a otras cuentas evitando el desplazamiento a sucursales físicas de los bancos. Otro ejemplo corresponde a las compras en línea, la mayoría de las compañías ofrecen sus

productos y servicios en el ciberespacio, permitiendo a los compradores pagar por ellos en Internet y recibir el producto más tarde o en el instante de acuerdo al producto o servicio contratado (Ploug, 2009).

La norma ISO/IEC 27032 de 2012 describe el Ciberespacio como un entorno virtual, el cual no existe en ninguna forma física, un espacio resultante de la aparición de la Internet y la interacción con las personas, software, servicios de Internet y las organizaciones, respaldado por todo tipo de dispositivos tecnológicos y de comunicación distribuidos a nivel mundial y redes conectadas, por lo que se ha convertido en un entorno complejo.

La definición anterior dada por la norma ISO/IEC 27032 parece definir el Ciberespacio como un entorno dentro de Internet, limitando el alcance del mismo, sin considerar aquellos sistemas que hacen uso del Ciberespacio y además lo limita a actividades puramente virtuales y no tangibles. Es necesario entonces para entender el riesgo en relación con el Ciberespacio, comprender las relaciones que establece este con los Cibersistemas. Para ello se utilizarán las definiciones y relaciones establecidas por Refsdal, Solhaug y Stølen.

Los Cibersistemas son aquellos sistemas que hacen uso o forman parte del ciberespacio. Estos son los que establecen la relación entre la información, las personas y las organizaciones, todos ellos participan en los procesos y comportamientos en el ciberespacio. A su vez esta clase de sistemas forman parte de la estructura organizativa de la mayoría de las empresas y se han vuelto más omnipresentes en la sociedad, los ciudadanos, las empresas y los gobiernos, estos agentes son quienes los utilizan para la prestación y el consumo de servicios. Dichos servicios van desde bienestar, salud, banca, hasta entretenimiento, redes, comercio, energía, transporte, entre otros muchos. Todo esto ha llevado a que las llamadas infraestructuras críticas también se conviertan en sistemas cibernéticos; como ejemplos de Infraestructuras críticas encontramos las telecomunicaciones, el

transporte, las finanzas, el suministro de energía, el suministro de agua y los servicios de emergencia (Refsdal, Solhaug, & Stølen, 2015).

También deben distinguirse los sistemas ciberfísicos, que son casos especiales de los cibersistemas y corresponden a sistemas cibernéticos que interactúan con su entorno físico, es decir aquel sistema que es capaz de controlar y responder a entidades físicas mediante activadores y sensores. Estos sistemas son cada vez más utilizados en la vida cotidiana para controlar los llamados hogares inteligentes, coches autónomos, líneas de producción y otro tipo de entidades físicas (Refsdal, Solhaug, & Stølen, 2015).

Los sistemas ciberfísicos se encuentran contenidos dentro del concepto de cibersistema, la diferencia de este con un sistema tradicional viene dada por la relación que establece el cibersistema con el ciberespacio; si el cibersistema se desconecta del ciberespacio pasaría a ser un sistema, siendo importante acotar que los cibersistemas se encuentran incluidos dentro del concepto general de sistema.

2.2 La Ciberseguridad y sus relaciones.

Por la naturaleza misma del Ciberespacio, donde la conexión entre diferentes sistemas es intrínseca, cualquier sistema que dependa de una u otra manera del ciberespacio se encuentra conectado y como consecuencia de dicha conexión se encuentra expuesto a ser vulnerado (Refsdal, Solhaug, & Stølen, 2015).

Dado lo anterior, la mayoría de las empresas y organizaciones se ocupan de la protección de sus propios sistemas contra las amenazas cibernéticas. Por lo tanto la ciberseguridad es la protección de los cibersistemas contra las amenazas cibernéticas. Las amenazas cibernéticas son aquellas que surgen a través del ciberespacio y por tanto son una amenaza para cualquier cibersistema (Refsdal, Solhaug, & Stølen, 2015). El concepto de ciberseguridad ha tomado tal relevancia que algunos autores hablan de ciberseguridad como una ciencia (Dykstra, 2016).

La Agencia Nacional de Seguridad (NSA) de los Estados Unidos define la ciberseguridad como medidas que protegen y defienden los sistemas de información, garantizando su disponibilidad, integridad, autenticación y confidencialidad. Estas medidas incorporan protección, detección y reacción (Fischer, 2009).

Para un delincuente podría ser de interés, por ejemplo, el hecho que muchos entornos del Ciberespacio utilicen una moneda virtual y que exista un valor asociado en el mundo real a dicha moneda. De esta manera, existen lugares en el ciberespacio donde se negocian de manera frecuente cambios de divisa real a divisa virtual. A menudo estos canales de monetización hacen que estos mundos virtuales sean un objetivo de ataque, usualmente mediante técnicas que permiten el robo de la cuenta (ISO/IEC 27032, 2012), por ello en el contexto de los servicios financieros, la ciberseguridad se ha definido como aquellas políticas, directrices, procesos y acciones que son necesarias para permitir las transacciones electrónicas con el mínimo riesgo de violación, intrusión o robo (Fischer, 2009).

2.2.1 Norma ISO/IEC 27032:2012

Esta norma Internacional ha sido desarrollada en conjunto por la ISO (Organización Internacional de Normalización) y la CEI (Comisión Electrotécnica Internacional), proporcionando una orientación para mejorar el estado de la ciberseguridad, aunque es importante anotar que limita la realización del Ciberespacio a Internet, sin abordar otras representaciones del mismo que se han visto anteriormente, sin embargo es relevante considerarla como un punto de partida para el análisis del Ciber Riesgo.

La norma destaca aspectos relevantes de la ciberseguridad tales como: Seguridad de la información, seguridad de la red, seguridad en Internet y protección de infraestructura de la información crítica; además establece una visión general de la

ciberseguridad, la relación establecida entre la ciberseguridad y otros tipos de seguridad, definición de las partes interesadas y una descripción de las funciones que desempeñan en la ciberseguridad, una orientación para abordar cuestiones comunes y un marco de referencia para solucionar los problemas relacionados con este tipo de seguridad (ISO/IEC 27032, 2012). La norma ISO/IEC 27032:2012 se utilizará en este trabajo como un marco de referencia para la estructuración de un sistema gerencial integral del Ciber Riesgo.

Para la norma, la ciberseguridad se refiere a las acciones que las partes interesadas –tanto personas como organizaciones– deben tomar para establecer y mantener la seguridad en el ciberespacio, previniendo y respondiendo de manera eficaz al uso indebido y ataques criminales. La Ciberseguridad se relaciona con otros entornos de seguridad que se convierten en bloques de construcción fundamentales, tales como:

- **Seguridad de la información:** Corresponde a la protección de la confidencialidad, la integridad y la disponibilidad de la información de los usuarios.

- **Seguridad de las aplicaciones:** Proceso por el cual se establecen controles y mediciones a los aplicativos de una organización para gestionar el riesgo de utilizarlos. Dichos controles y mediciones se pueden implementar al propio aplicativo (Procesos, componentes, software y resultados), a sus datos (datos de configuración, datos de usuario, datos de organización) y a todas las tecnologías, procesos y actores involucrados en su ciclo de vida.

- **Seguridad de la red**: Corresponde al diseño, la implementación y el funcionamiento de las redes para lograr los propósitos de la seguridad de la información en las redes que se establecen dentro de las organizaciones, las redes entre organizaciones y las redes entre las organizaciones y los usuarios.

- **Seguridad en Internet:** Se ocupa de la protección de los servicios relacionados con Internet y los sistemas y redes de las tecnologías de la información y la comunicación (TIC), garantizando la fiabilidad y disponibilidad de los servicios de Internet.

- **Protección de la Información de la Infraestructura Crítica**: Se refiere a la protección de los sistemas que operan infraestructura crítica, tales como departamentos de energía, telecomunicaciones y agua, asegurando que estos sistemas y redes estén protegidos contra los riesgos de seguridad de la información, los riesgos de seguridad de la red, los riesgos de seguridad de Internet, así como los riesgos de seguridad cibernética.

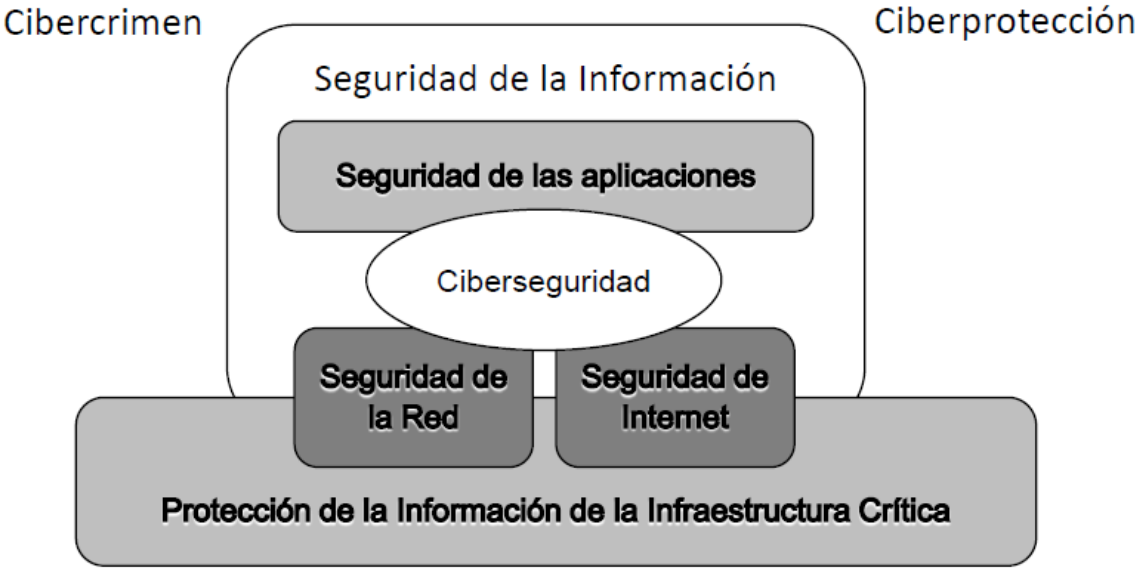


Figura 1. Relación de la Ciberseguridad con otros dominios de la seguridad.

Fuente: ISO/IEC 27032:2012

La relación establecida entre la Ciberseguridad y otros dominios de la seguridad es compleja tal como se observa en la Figura 1, por ejemplo, algunos de los servicios de infraestructura críticos, como el agua y el transporte, no afectan la Ciberseguridad directa o significativamente. Sin embargo, la falta Ciberseguridad puede tener un impacto negativo en la disponibilidad de sistemas de información de

la infraestructura crítica. Por otro lado, la disponibilidad y el funcionamiento del Ciberespacio depende en gran medida de servicios de infraestructura crítica, tal como la infraestructura de la red de telecomunicaciones. Como gran conclusión de este análisis la ciberseguridad requiere una comunicación y una coordinación entre diferentes organismos, entidades públicas y privadas que puede llegar a involucrar diferentes países y organizaciones (ISO/IEC 27032, 2012).

3. El Ciber Riesgo.

3.1 La definición de Riesgo.

La palabra Riesgo proviene del antiguo vocablo ‘riesco’, el cual significa risco, que corresponde a un peñasco alto y escarpado, difícil y peligroso para andar por él y la palabra es definida como la contingencia o proximidad de un daño (Real Academia de la Lengua Española, 2014). Traduciendo la palabra al idioma Inglés está sería ‘Risk’ cuya definición –según el Diccionario de Cambridge– es la posibilidad de que algo vaya mal y que por tanto, cause algún tipo de daño o pérdida (Cambridge University Press, 2017). El Riesgo es abordado por diferentes áreas de investigación y por diferentes disciplinas científicas (Luhmann, 1993).

Retomando la etimología de la palabra, el escalar un risco puede tener consecuencias negativas pero también puede convertirse en una oportunidad para alcanzar una cima que simbólicamente representaría un objetivo. Por lo tanto un concepto más amplio para la palabra Riesgo correspondería a los efectos de la incertidumbre sobre los objetivos esperados, dichos efectos pueden ser positivos o negativos, según lo que se esté esperando (Guía ISO/CEI 73, 2009)

Por tanto desde un punto de vista más general, el Riesgo puede definirse como el resultado incierto de la exposición a un hecho futuro sobre un objeto o bien de

interés (Holton, 2004). Los antropólogos, los científicos y políticos señalan que la evaluación del riesgo y la disposición a aceptar el riesgo no son sólo problemas psicológicos, sino sobre todo problemas sociales y al parecer sólo cuantificamos los riesgos cuando los desastres tocan cierto umbral, el cual se entiende como desastre (Luhmann, 1993),

La ciencia económica se ha sumado al análisis y tratamiento estadístico del riesgo, de esta manera Frank Knight explica la rentabilidad empresarial en función de la absorción de la incertidumbre, además de escribir sobre los fundamentos de la probabilidad (Luhmann, 1993), otros grandes economistas trataron de asociar el riesgo a su campo de estudio, tales como John Maynard Keynes, Richard von Mises y Andrey Kolmogorov, centrando su diálogo en la el carácter objetivo o subjetivo de las probabilidades, según la interpretación objetiva las probabilidades son reales, siendo obtenidas a través de estadísticas y desde el punto de vista subjetivo las probabilidades son sólo creencias cuyo valor depende de la percepción del sujeto. (Holton, 2004)

La Actuarial Standard Board en su manual de prácticas sobre la Gerencia de Riesgos en las compañías, define el Riesgo como el potencial de futuras pérdidas o déficit de expectativas debido a la desviación de los resultados reales sobre los resultados esperados (Actuarial Standards Board, 2012)

Retomando la definición de la guía ISO sobre la Gestión de riesgos (Guía ISO/CEI 73, 2009) el Riesgo puede entenderse como la probabilidad de ocurrencia de un suceso y de sus consecuencias. A continuación se explican los tres conceptos a los que se refiere esta definición y que son también desarrollados en la guía:

Probabilidad: Es un número entre 0 y 1 otorgado a un evento aleatorio. Al describir el riesgo puede utilizarse la palabra “frecuencia” en lugar de “probabilidad”.

Suceso: Es la ocurrencia de una serie de circunstancias particulares que pueden ser ciertas o inciertas.

Consecuencias: Corresponde al impacto o resultado del suceso y que puede variar de positivo a negativo, aunque el término es siempre negativo en aspectos relacionados al campo de la seguridad.

3.2 El Concepto de Ciber Riesgo.

Con los conceptos introducidos hasta el momento podría decirse que el Ciber Riesgo es la probabilidad de ocurrencia de una amenaza proveniente del Ciberespacio y las consecuencias que estas tienen sobre los cibersistemas.

El Ciber riesgo no significa que corresponda a cualquier riesgo al que esté expuesto un cibersistema, por ejemplo, si un servidor en el que se encuentra alojado un cibersistema se daña por una inundación de agua no es un ciber riesgo a menos que una amenaza cibernética haya sido un factor de contribución a la situación. De otro lado, las violaciones de confidencialidad ocasionadas por una ataque de un virus a través del ciberespacio y la pérdida de disponibilidad debida a ataques puede considerarse un ejemplo de Ciber riesgo (Refsdal, Solhaug, & Stølen, 2015).

Retomando la definición general del riesgo, donde el resultado del hecho incierto se produce sobre un objeto o bien de interés, tendría que hablarse entonces de los valores que son de interés en el Ciberespacio para que se presenten dichas amenazas en esta dimensión. Al respecto de este bien u objeto de interés la norma

ISO/IEC 2012 da claridad y define estos objetos de interés en el ciberespacio como ciber activos, siendo aquellos activos o valores que tienen un valor para un individuo o una organización y los clasifica de esta manera.

Ciber activos personales: Las claves personales se convierten en el principal activo de los individuos en el ciberespacio, ya que representa la identidad y datos relevantes personales como por ejemplo la información financiera en línea.

Otro activo personal en el Ciberespacio puede considerarse los avatares virtuales que representan o identifican a una persona para actuar en su nombre, en esta categoría también entran las monedas virtuales que se utilizan para transacciones en línea. Tanto avatares como monedas se consideran un ciberactivo perteneciente a un consumidor individual.

Una tercera categoría de ciberactivos personales corresponde al hardware, software y dispositivos digitales o puntos finales que permiten al individuo conectarse y comunicarse en el ciberespacio.

Ciber activos empresariales: Cada vez cobra mayor relevancia el valor de los activos virtuales de las compañías, de esta manera la marca en línea y otras representaciones de una compañía identifican de manera única a la organización en el ciberespacio y son tan importantes como los activos físicos o tangibles. Como ejemplos de ciberactivos de una empresa pueden encontrarse su URL y la información que albergan en sus sitios web corporativos.

Otros activos de las organizaciones que están expuestos a través de vulnerabilidades en el Ciberespacio están relacionados con la propiedad intelectual

tales como fórmulas, procesos, patentes y resultados de investigación. Los planes y estrategias empresariales como tácticas de lanzamiento y comercialización de productos, información financiera y datos de informes.

Dentro de esta categoría también deben considerarse los Gobiernos y las entidades gubernamentales, quienes poseen información sobre asuntos de seguridad nacional, y otros muchos elementos relacionados con el gobierno y el Estado con una amplia gama de información sobre individuos, organizaciones y la sociedad en su conjunto.

Continuando con la norma ISO/IEC 2012 las amenazas cibernéticas, mejor conocidas como ciber amenazas son aquellas que se presentan sobre los ciber activos y también se clasifican en aquellas que están relacionadas con los ciber activos personales y los ciber activos empresariales.

Ciber amenazas a los ciber activos personales: Estas amenazas giran en torno a la fuga o robo de la identidad y la información personal en el ciberespacio, y la persona puede ser privada del acceso a servicios y aplicaciones. Como consecuencias más serias se pueden presentar incidentes financieros que abren la posibilidad a robos de dinero o fraude electrónico.

Otra ciber amenaza para los ciber activos personales es que los dispositivos personales o puntos finales terminen siendo zombies, los cuales serían controlados por un pirata informático después de haber sido infectados por un virus, pasando a formar parte de una botnet, siendo utilizadas para realizar acciones delictivas (Instituto Nacional de Ciberseguridad, 2017).

Otros ciber activos personales expuestos corresponderían a los detalles del avatar y monedas virtuales, sujetos a ataques y explotación, el robo virtual y asalto virtual son términos que son cada vez más comunes para este tipo de ciber amenazas.

Ciber amenazas a los ciber activos empresariales: Las grandes organizaciones con negocios en línea son frecuentemente objetivo de los ciber delincuentes quienes a menudo amenazan con derrumbar o degradar a través de acciones los sitios web corporativos ocasionando pérdida de la reputación de las empresas.

En un ataque informático exitoso la información personal de empleados, clientes, socios, proveedores podría ser extraída acarreando sanciones contra las organizaciones si se evidencia una falta de gestión que contribuye a la pérdida.

Los gobiernos deben proteger su infraestructura e información contra el acceso indebido y la explotación, los sitios gubernamentales que se encuentran en el ciberespacio se convierten en un canal para lanzar ataques y acceder a información privilegiada, con un alto riesgo para una nación, su gobierno y la sociedad.

Otras categorías que deben considerarse dentro de las ciber amenazas a los ciberactivos empresariales están relacionadas con la infraestructura que soporta el Ciberespacio y las formas criminales que afloran en internet gracias al alto alcance otorgado por la red mundial.

La ciber amenazas pueden ser de carácter malicioso o no malicioso, en el primer grupo se encuentran aquellas que tienen motivos o intenciones. Para ilustrar esta clasificación se pone como ejemplo un incidente ocurrido por el acceso no autorizado a datos sensibles, este evento pudo ser ocasionado por un pirata

informático convirtiéndose en una amenaza maliciosa, mientras que si hubiese sido causada por la publicación accidental de los datos en un sitio web abierto correspondería a una amenaza no intencionada (Refsdal, Solhaug, & Stølen, 2015).

Podría presentarse el caso de que una amenaza fuese de carácter combinado, es decir, que se pudiese clasificar entre maliciosa y no maliciosa; como ejemplo puede considerarse la intrusión mientras los sistemas de detección y prevención de intrusos está inactiva debido a fallos accidentales (Refsdal, Solhaug, & Stølen, 2015).

Las ciber amenazas pueden venir de un individuo o grupo de individuos que desempeñan algún papel en las mismas. Es importante tener en cuenta tres factores: motivos, capacidades e intenciones. Los motivos pueden ser de tipo religioso, político o económico; las capacidades que tienen que ver con conocimientos o financiación; y por último, las intenciones, que pueden ir desde diversión, pasando por la delincuencia y el espionaje.

3.3 Importancia del Ciber riesgo.

En el Informe de Riesgos Globales 2017 publicado por el Foro Económico Mundial en su duodécima edición, el Riesgo Cibernético emerge como uno de los principales riesgos a ser considerados en el entorno global, clasificándose entre los 10 principales riesgos globales, debido al aumento en los últimos años tanto en frecuencia como severidad y como consecuencia de que el Internet de las cosas ha generado un sinnúmero de conexiones entre personas y máquinas, generando una ciber dependencia que aumenta las probabilidades de un ciberataque con alto potencial de efecto dominó a través del Ciberespacio. (World Economic Forum, 2017)

En el mismo informe se aclara que el Internet de las cosas es una realidad que introduce nuevas eficiencias, pero también vulnerabilidades interconectadas. Los avances tecnológicos recientes han beneficiado a la humanidad de muchas maneras pero también han abierto la puerta a una oleada de riesgos que incluyen el espionaje electrónico, el ciber crimen y los ciberataques y estos se trasladan al mundo de los activos físicos ya que la gran mayoría de operaciones de los sistemas involucran tecnología cibernética, desde las redes eléctricas, las represas, las redes de comunicación hasta los sistemas de transporte e instalaciones nucleares.

Existe una preocupación debida a que el Ciberespacio ha abierto una nueva frontera en las guerras del mundo moderno, cada futuro conflicto tendrá un elemento cibernético, y algunos probablemente se combatirán enteramente en esta dimensión y dado que el ataque es más fácil que la defensa en la red, se cambiará la manera como las organizaciones se preparan para recibir al enemigo, la distancia física ya no ofrecerá protección, el alcance, la escala y los ataques cibernéticos crecerán rápidamente debido a la digitalización de la información pública y privada, pasando de lo virtual al mundo físico.

Los Gobiernos vienen reconociendo la amenaza económica que supone el Ciber riesgo, de esta manera en la actualidad más de 30 países, han venido desarrollando estrategias de ciber seguridad. En China por ejemplo, se anunció una nueva política nacional de ciberseguridad, otros países como Singapur han creado una agencia de Seguridad Cibernética, el propósito de estas iniciativas es desarrollar estrategias de defensa contra las ciber amenazas (World Energy Council, 2016)

La materialización del ciber riesgo involucra altos costos, entre los cuales se puede contar los costos por el rescate de la información, el costo por la pérdida de datos y el costo por las demandas judiciales. Los altos funcionarios de una compañía pueden perder sus empleos y las juntas de administración pueden ser demandadas por negligencia. Por lo anterior, el Ciber riesgo ha cobrado especial relevancia

convirtiéndose en una oportunidad para que los actuarios desarrollen modelos exitosos para la valoración y cuantificación de este tipo de Riesgos (Solomon, 2016).

De acuerdo a legisladores estadounidenses con conocimiento en asuntos de inteligencia, al hablarse de ciberespionaje sólo hay dos tipos de empresas: las que saben que han sido vulneradas cibernéticamente y las que no lo saben (Editorial Wall Street Journal, 2013).

Toda clase de negocio puede ser afectado por un ciberataque, sin distinción del tipo de sector: desde el sector financiero, el de infraestructura, hasta el sector público y privado, variando en frecuencia y severidad de acuerdo al tipo de negocio. En el año 2015 los sectores más atacados en frecuencia fueron Servicios de Salud, Financieros, Retail y Educación, sin embargo los sectores que sufrieron mayores pérdidas fueron Restaurantes y hostelería (Maxwell, 2017).

El uso de una industria para clasificar el tipo de riesgos es un buen punto de partida para fijar el valor del riesgo cibernético, debe considerarse también el volumen de datos, el valor de los datos, el número de puntos finales. Las compañías que ofrecen cibercobertura muestran poca diferenciación en los precios, lo que puede deberse a falta de datos históricos, las compañías se ven obligadas a buscar datos externos para mejorar los precios de los riesgos cibernéticos, estas informaciones pueden encontrarse en los centros Centro de Recursos para el Robo de Identidad, el Departamento de Seguridad Nacional, el Centro de Estudios Estratégicos e Internacionales y la Oficina de las Naciones Unidas contra la Droga y el Delito. (Maxwell, 2017)

Para el sector asegurador, el Ciber Riesgo cobra especial relevancia. De acuerdo a estudios del mercado de la firma de servicios profesionales PwC el pago de primas en Ciberseguros es de $ 2.5 Billones de USD a 2015 y se espera un crecimiento substancial al año 2020, con proyección de alcanzar los 7.5 Billones en primas para este tipo de Riesgo (PwC, 2015).

3.4 El Ciber riesgo como riesgo catastrófico.

Se identifica una catástrofe como un evento de muy baja probabilidad de ocurrencia pero que en caso de materializarse produciría un daño tan grande y repentino que no tendría ningún grado de comparación con algún acontecimiento que lo precediera (Posner, 2004).

El huracán Andrew devastó la costa sur de Florida en el año 1992, dejando a su paso una gran cantidad de víctimas mortales y causando más de $USD 25 mil millones en pérdidas materiales. Esta catástrofe puso en evidencia las deficiencias en la forma como el sector asegurador realizaba la cuantificación del potencial costo de una catástrofe. Hoy en día las aseguradoras luchan por entender el alcance económico de una catástrofe producida por una ciber amenaza. Algunas lecciones aprendidas de la catástrofe de 1992 podrían aplicarse al Ciber Riesgo, sin embargo, muchas compañías todavía están luchando por entender la naturaleza de esta clase de amenaza (Orcutt , 2017).

Quienes tratan de demostrar que el Ciber riesgo no es de naturaleza catastrófica afirman que a pesar de los millones de dólares en pérdidas que puede ocasionar y la interrupción en la prestación de servicios esto sólo representa tan sólo el 1% del producto interno bruto de los Estados Unidos, convirtiéndose más en una molestia que en un evento de naturaleza catastrófica, además existe la creencia que con el paso del tiempo el Ciberespacio será cada vez menos vulnerable (Posner, 2004).

Otras de las razones por las cuales no debería considerarse el Ciber riesgo como un riesgo catastrófico, es que existe una diferencia notable entre la modelación de las catástrofes naturales y las catástrofes cibernéticas, debido a que los eventos en el ciberespacio están conducidos por el hombre, mientras las catástrofes naturales responden a leyes físicas y de la naturaleza que hasta ahora el hombre no puede controlar.

Podría afirmarse que el mayor reto en la actualidad es estar en capacidad de cuantificar el riesgo de que una catástrofe cibernética golpee a muchos asegurados a la vez, estimando la pérdida en el peor de los casos, que es lo que las aseguradoras no pudieron realizar –por ejemplo– antes de que el huracán Andrew ocasionara la catástrofe. Es difícil modelar un desastre cibernético comparable en escala con un fenómeno natural de esta magnitud, en buena parte porque todavía no ha ocurrido (Orcutt , 2017).

Al parecer los ataques cibernéticos que podrían ocasionar un carácter verdaderamente catastrófico provienen de los ataques a la infraestructura física tradicional, como el provocado por el virus BlackEnergy que dejó sin servicio de energía eléctrica a más de 1.4 millones de personas durante 6 largas horas el 23 de Diciembre de 2015 en Kiev, Ucrania (Lipovsky & Cherepanov, 2016). Aunque no se han cuantificado las pérdidas ocasionadas por este ataque, en un informe publicado por la firma Lloyd's se estimó un caso hipotético donde un apagón de todo el noreste de Estados Unidos dejara sin suministro eléctrico a 93 millones de personas, llegando a la conclusión que un evento de este tipo podría costarle a las aseguradoras entre $USD 21 mil millones y $USD 71 mil millones (Lloyd's, 2015), cifras que se encuentran dentro de los costos ocasionados por el huracán Andrew.

Algunos autores tratan de establecer semejanzas entre los eventos de naturaleza catastrófica como el huracán Andrew y lo que podría denominarse una catástrofe cibernética. La lógica detrás de este planteamiento es que existen una serie de condiciones que contribuyen a crear lo que se denomina la “tormenta perfecta” que no es más que la combinación de una serie de circunstancias que agravan o intensifican una situación hasta convertirla en catástrofe (Ulsch, 2014). A continuación se exponen los factores que crearían una “tormenta cibernética perfecta” que podría ocasionar una catástrofe.

- Las organizaciones son vulnerables y no están preparadas para enfrentar las ciber amenazas desde lo técnico, organizacional y operacional.

- Las ciber amenazas se están expandiendo e intensificando rápidamente.
- Los marcos regulatorios son inconsistentes con respecto al tratamiento de los ciberataques. Por ejemplo, en los Estados Unidos existen diferencias regulatorias entre los Estados.
- El nivel de conciencia sobre el Ciber riesgo por parte de la alta dirección y las juntas de administración es demasiado bajo.
- Las compañías que operan con márgenes pequeños invierten muy poco o casi nada en ciberseguridad.
- Se considera la amenaza cibernética como un problema tecnológico y no como un riesgo.
- Los dispositivos móviles están creando una arquitectura de información altamente distribuida.
- Las redes sociales están permitiendo un intercambio de datos sin precedentes.
- La ingeniería social para acceder a la información está logrando nuevos niveles y facilidad de ejecución gracias a las redes sociales.
- Muchas compañías no han calculado adecuadamente el potencial impacto de la materialización del ciber riesgo, o la posibilidad de que un ciber ataque esté dirigido específicamente a la organización, así como también el que puedan ser víctimas de un ataque a gran escala.
- Las amenazas internas provenientes de empleados, clientes o proveedores sigue latente en las compañías debido a que no se investigan los antecedentes adecuadamente.
- Muchas empresas niegan su vulnerabilidad cibernética debido a la inconsciencia o el desconocimiento que tienen sobre el Ciber riesgo.

4 Gerencia y Gestión del Ciber Riesgo.

Muchas empresas están viviendo por debajo de la línea de pobreza en cuanto a ciberseguridad. Las soluciones para abordar el Ciber riesgo son limitadas, sumado a la falta de información acerca de cuáles riesgos tienen mayor probabilidad de materializarse; con estas condiciones las organizaciones se ven inclinadas a

comprar seguros cibernéticos en lugar de invertir en costosos esfuerzos para mitigar el ciber riesgo, no obstante una cobertura de este tipo podría dar lugar a una situación de riesgo moral que anime a la empresa a asumir riesgos en lugar de mejorar sus cultura de gestión del Ciber riesgo (Solomon, 2016).

En entrevista a Shawn Henry, ex jefe de de la división de seguridad cibernética del FBI, este informa que el mayor error cometido por las empresas en la gestión del Riesgo Cibernético es ser reactivas en lugar de proactivas, (Henry, 2016). En el estudio de Verizon 2013 sobre violación de datos, el 90% de los ataques cibernéticos pudieron ser evitados con sistemas simples o intermedios de protección (Solomon, 2016).

Por lo tanto, es importante la implementación de sistemas de Gestión del Ciber Riesgo tanto para las empresas aseguradas como para las aseguradoras; estas últimas tienen la necesidad de incluir dentro de sus pólizas con cobertura cibernética, el asesoramiento en la implementación de estos tipos de sistemas de gestión del riesgo o por lo menos exigir que las compañías aseguradas tengan implementado alguno.

Para la gestión del Ciber Riesgo deberían considerarse además de la Norma ISO/IEC 27032:2012 que ya se ha introducido en este trabajo, las norma ISO 31000:2009 y la norma ISO/IEC 27005:2011 (ISO/IEC 27032, 2012).

4.1 La norma ISO 27005:2011. Gestión de riesgos de la seguridad de las tecnologías de la información.

Esta norma proporciona directrices, procesos y requisitos de un sistema general para la gestión del riesgo de la seguridad de la información en una organización. Estas directrices y procesos se consideran suficientes para abordar la gestión de riesgos en el contexto del Ciberespacio (ISO/IEC 27032, 2012).

Esta norma no proporciona ninguna metodología específica para la gestión del Ciber Riesgo (ISO/IEC 27032, 2012). Por ello se necesita de otra norma para complementar el Sistema de Gestión propuesta.

4.2 La norma ISO 31000:2009. Gestión de Riesgos. Principios y directrices.

Es la norma de referencia utilizada para la gestión de cualquier tipo de riesgo, proporcionando unos lineamientos generales para ser aplicados en la construcción de un sistema de gestión integral del Riesgo.

La norma está sustentada en tres pilares, los cuales serán adoptados y acondicionados en el presente trabajo para la gestión del Ciber Riesgo, estos son: Principios de la Gestión del Riesgo, Marco de trabajo (Framework) y el Proceso de Gestión.

4.2.1 Principios de la Gestión del Ciber Riesgo.

Los principios se diseñan para asegurar que una organización actúe de manera coherente y colectiva hacia el logro de sus metas y objetivos estratégicos (Kendrick, 2010).

El estándar ISO 31000:2009 desarrolla un total de once principios para garantizar una gestión efectiva del riesgo, a continuación se exponen el total de principios adaptados a la gestión del Ciber Riesgo.

1. ***Creación y protección de valor.***

Garantiza que la organización, a través de sus socios y de la junta de administración, pueda mantener un control sobre sus estrategias, funciones y estándares de funcionamiento; garantizando el cumplimiento de las metas y objetivos a largo plazo (Kendrick, 2010).

2. ***Integración con todos los procesos de la organización.***

Los procesos de la empresa deben tener un entendimiento integral del alcance, función y limitación de la estrategia a perseguir (Kendrick, 2010).

3. ***Ser parte en la toma de decisiones.***

La implementación de un sistema de gestión del ciber riesgo es responsabilidad de la junta de administración. Son ellos quienes deben establecer el marco de gestión dentro del cual la organización implementa la estrategia y logra los objetivos estratégicos definidos, facilitando la toma de decisiones de manera informada y la prioridad de los planes de acción dentro de la organización.

4. ***Explicitar la incertidumbre.***

Es indispensable que se cree una conciencia dentro de la organización de que el riesgo está presente y no puede ser ignorado.

5. ***Sistemática, estructurada y oportuna.***

Por lo general, las estrategias relacionadas con tecnología dentro de las organizaciones con demasiada frecuencia se desalinean de los objetivos y no proporcionan los rendimientos esperados (Kendrick, 2010). Un enfoque de gestión de riesgos que cumpla con las características de ser sistemático, estructurado y ordenado contribuye a que los procesos sean eficientes y que se consigan los resultados de forma eficaz, minimiza el riesgo inherente a esta clase de proyectos.

6. ***Basada en la mejor información disponible.***

La recopilación de datos para la medición del riesgo cibernético apenas está emergiendo y mucha información no es de dominio público ya que las empresas afectadas prefieren no divulgarlo (Eling & Wirfs, 2015); por ello la organización debe

informarse de manera adecuada y tener en cuenta las limitaciones en el acceso a los datos históricos y la proyección de los futuros.

7. ***Adaptabilidad.***

En una dimensión como el Ciberespacio, donde los ciber riesgos se pueden manifestar de una manera insospechada y variada, es necesario que la gestión de este tipo de amenazas sea particularmente dinámica y se adapte con rapidez a las necesidades del entorno.

Las nuevas soluciones en tecnología emergen frecuentemente y la organización debe estar en la capacidad de manejar los cambios a medida que ocurren y sobre todo adaptarse a ellos. Cada solución plantea la aparición de nuevos riesgos que deben identificarse y ser gestionados.

8. ***Integrar factores humanos y culturales.***

Las organizaciones con procesos y sistemas que están debidamente controlados y dirigidos bajo un sólido liderazgo apoyado por sus funcionarios, están más en sintonía con la necesidad de alcanzar y mantener estándares aceptables de desempeño derivados del respeto mutuo entre la administración, los socios, la gerencia y el equipo colaborador.

9. ***Transparencia y participación.***

La implementación oportuna y con ello la sensación de control, dirección y liderazgo que pueda transmitir la Junta de administración, respaldando una toma de decisiones transparente, fomenta una cultura de responsabilidad a todos los niveles de la organización.

Un liderazgo y una dirección claros apoyados por decisiones transparentes ayudan a todos los niveles de personal a:

- Entender completamente la estrategia de la organización y los objetivos que se pretenden lograr.
- Entender sus roles y responsabilidades.
- Comprender la necesidad de trabajar en equipo para alcanzar los objetivos de la organización.

La amplia gama de riesgos a los que pueden dar lugar el Ciberespacio requiere un enfoque colectivo y una comprensión firme de los métodos de gestión del Ciber riesgo.

10. Dinámica, iterativa y responde a cambios.

Se deben desarrollar habilidades que permitan sopesar el riesgo contra las oportunidades potenciales. Por ejemplo, desarrollar una tecnología de encriptación para adaptarse a los requerimientos de seguridad puede implicar recursos importantes al invertir en capacitación al personal y la tecnología necesaria para su desarrollo, sin embargo si se gestiona de manera adecuada, atraerá nuevos clientes gracias a la respuesta a las preocupaciones y necesidades de seguridad de los consumidores.

11. Facilitar la mejora continua de la organización.

Además, si las empresas logran la aplicación de los principios se garantiza que la organización, a través de su junta directiva o de sus socios, pueda mantener un control sobre sus estrategias, funciones y estándares de desempeño. Como consecuencia esto conduce a una mayor seguridad de las metas y objetivos puedan ser alcanzados en el largo plazo, logrando una mejora continua en el proceso.

4.2.2 Marco de Trabajo (Framework).

El marco de trabajo tiene como objetivo establecer los lineamientos y actividades para implementar y mejorar continuamente el proceso de gestión del Ciber Riesgo. Este marco de trabajo debe integrarse en el marco de la gestión global de organización.

La empresa debe contar con al menos un miembro dentro del consejo de dirección experto en Riesgos y este a su vez contar con un equipo experto en seguridad informática que colabore en la gestión del ciber riesgo, también podría contar con un asesoramiento externo si la empresa no cuenta con la inversión necesaria para tener dicho equipo en la compañía. El gerente de Riesgos requiere asesoramiento e información por parte de los expertos en cuanto a temas tecnológicos, cumplimiento legal y asuntos operativos.

La norma ISO 31000:2009 estandariza cuatro fases para el marco de trabajo de un sistema de Gestión de Riesgos y la norma ISO 27032:2012 establece un marco de trabajo para compartir información en red, a continuación, se realiza una adaptación de estos dos marcos de trabajo al Ciber riesgo.

1. **Planear.** La fase de planeación de un sistema de gestión del Ciber riesgo debe incluir las siguientes actividades.

a. Clasificar y categorizar los ciber sistemas y los ciberactivos de la organización identificando la información compartida a través de ellos.
b. Identificar la audiencia y usuarios de los cibersistemas, la función que realizan en el proceso y que tipo de información comparten, si es de carácter público, privado o confidencial.
c. Establecer protocolos de coordinación, autenticación y verificación de identidades para las audiencias y usuarios de la información.
d. Seleccionar los controles de seguridad de los ciber sistemas y los

ciberactivos.

2. **Hacer.** La ejecución y puesta en marcha de un proceso de gestión del Ciber riesgo, implica el apoyo de toda la organización, ejecutando las siguientes actividades:

a. Firmar acuerdos de confidencialidad con los usuarios, proveedores y clientes de la información.
b. Establecer un código de buenas prácticas con los ciber activos, los ciber sistemas y la información de la organización.
c. Implementar controles de seguridad.
d. Ejecución de protocolos de seguridad en caso de incidentes.
e. Mantener los controles de seguridad de acceso a los cibersistemas de la organización.
f. Estandarizar la información de la organización.
g. Administración de un sistema de claves criptográficas para garantizar el intercambio de información en caso de un ciberataque.

3. Verificar. El sistema de gestión del ciber riesgo debe estar sometido a una revisión y seguimiento para garantizar la efectividad del mismo.

   a. Se deben proporcionar informes periódicos sobre el estado del ciber riesgo y la ciberseguridad.
   b. Realizar simulaciones de ciberataques a través de sistemas de prueba para asegurar la efectividad y fiabilidad de los sistemas de gestión del Ciberriesgo.
   c. Realizar revisiones periódicas, post-prueba y post-incidente para mejorar la gestión del Ciber riesgo.

4. Actuar. La dinámica del Ciberespacio debe impulsar a la organización a tener una cultura de adaptación y desarrollo de habilidades para afrontar las

nuevas amenazas que vayan surgiendo.

4.2.3 Proceso de Gestión del Ciber riesgo.

El proceso de gestión del Riesgo tradicional viene de la norma AS/NZ 4360 y se divide en tres etapas: Establecimiento del contexto, Evaluación de riesgos y Tratamiento del riesgo (Australian/New Zealand Standard)

Al adaptar el proceso de gestión del riesgo tradicional al ciber riesgo, se presenta una diferencia por la división al momento de identificar los riesgos, caracterizando si estos han sido de carácter malicioso o no, esto es importante para categorizar la naturaleza y fuente de la amenaza.

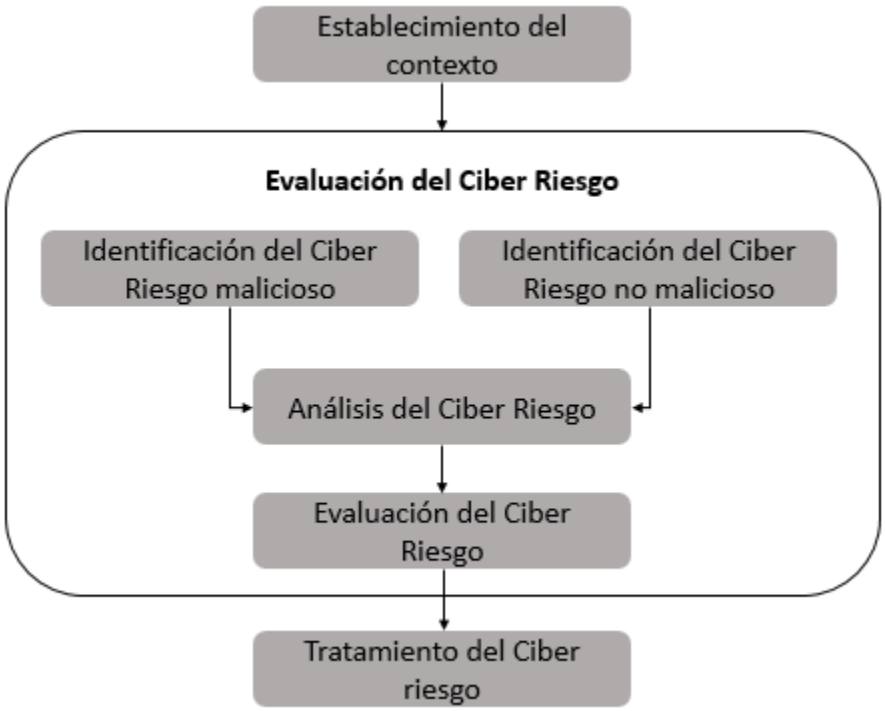


Figura 2. Proceso de Gestión del Ciber riesgo
Fuente: (Refsdal, Solhaug, & Stølen, 2015)

1. **Establecimiento del contexto.**

La organización debe entender y documentar cómo sus ciber sistemas interactúan con el Ciberespacio y el funcionamiento de la interfaz entre ambos. Lo anterior, no es más que una definición de fronteras lógicas (interconexiones) que proporciona un sustento para identificar el lugar y la razón de donde pueden surgir las ciberamenazas, reconociendo cuáles ciberactivos son los más relevantes para concentrarse en ellos.

Debe tenerse en cuenta que no sólo los ciberactivos están comprometidos en un ataque cibernético, una ciberamenaza también puede causar daños a la vida, la salud y el medio ambiente, por ello es importante que la empresa identifique el entorno en el que se desenvuelve.

2. **Evaluación del Ciber riesgo.**

Esta segunda etapa, permite identificar el valor de los ciber activos, así como las ciberamenazas y vulnerabilidades que puedan existir en la organización, analizando y evaluando los controles existentes y el efecto que estos tienen sobre los ciber riesgos identificados. Por último, prioriza y clasifica los ciber riesgos determinando las posibles consecuencias (Lachapelle & Halili, 2015).

a. **Identificación del Ciber riesgo malicioso.**

Una organización posee una serie de ciberactivos que pueden llegar a representar un conjunto de objetivos para un ciberatacante dando lugar a motivos e intenciones para atacar los cibersistemas.

Por lo general las estrategias del atacante suelen estar condicionadas por las fortalezas y debilidades del defensor, por lo que se hace indispensable identificar las vulnerabilidades y la forma como los adversarios podrían aprovecharse de ellas.

En primer lugar se debe identificar y documentar las fuentes de amenazas maliciosas para luego investigar de qué forma y en qué medida puede afectar a los ciberactivos. La identificación del ciber riesgo malicioso incluiría los siguientes pasos:

- Identificación de los ciber activos que podrían representar un objetivo para los ciberatacantes.
- Identificación de las fuentes de amenazas maliciosas.
- Identificación de las amenazas maliciosas.
- Identificación de los controles existentes contra las amenazas maliciosas.
- Identificación de las vulnerabilidades de los cibersistemas de la organización.
- Identificación de los incidentes ocasionados por amenazas maliciosas.
- Identificación de las consecuencias ocasionadas por una amenaza maliciosa.

b. Identificación del Ciber riesgo no malicioso.

Al igual que en la identificación del Ciber riesgo malicioso conviene comenzar por la identificación de los ciber activos de la compañía, pero como detrás de un Ciber riesgo no malicioso no hay intenciones o motivos no es práctico identificar y documentar fuentes de amenazas; la pregunta que debería plantearse en su lugar es de qué manera los ciber activos se pueden ver amenazados directamente por una fuente no intencionada. Los demás pasos de la identificación del riesgo no malicioso serían idénticos a los correspondientes a la identificación del Ciber riesgo malicioso vistos anteriormente.

c. Análisis del Ciber riesgo.

Existen dos aspectos importantes que diferencian el análisis del Ciber riesgo del análisis de Riesgo general. En primer lugar, detrás de las amenazas maliciosas existen intenciones y motivos humanos que pueden dar lugar a que sea difícil

estimar las probabilidades de ocurrencia. En segundo lugar, gracias a la naturaleza de los sistemas informáticos existen una serie de recursos que permiten identificar los usuarios, realizar monitoreos y análisis fácilmente (Refsdal, Solhaug, & Stølen, 2015).

Es importante analizar las causas de los ciber riesgos para tener una mejor comprensión de las ciber amenazas y las vulnerabilidades. En el caso del análisis de las ciber amenazas maliciosas es importante utilizar técnicas para modelar aspectos que permitan entender los requisitos del ataque, las habilidades del atacante, el conocimiento requerido, los recursos necesarios, los motivos, entre otros factores.

Todos estos análisis permiten una mejor comprensión del Ciber riesgo y se convierten en un punto de partida para estimar las probabilidades de ocurrencia de las ciberamenazas y la gravedad de las vulnerabilidades que podrían explotar los ciber delincuentes.

El análisis del Ciber riesgo podría dividirse en las siguientes secciones:

- Metodologías de análisis del Ciber riesgo. Estas metodologías pueden dividirse a su vez en métodos cuantitativos y cualitativos.

- Determinación de las potenciales consecuencias. Esta sección está fuertemente ligada a la valoración de los ciber activos.

- Determinación de las probabilidades de incidencia. Debe tener en cuenta la frecuencia con la que se presentan las ciberamenazas y la facilidad con la que pueden aprovecharse las vulnerabilidades.

- Niveles del Ciber riesgo. Generar una lista con los niveles y valores que la compañía estaría dispuesta a asumir.

d. Evaluación del Ciber riesgo.

Del análisis del Ciber riesgo se obtienen nuevas formas de entender y aproximarse al Ciber riesgo, de esta manera la evaluación de esta clase de riesgo debe considerar cuáles son las prioridades para el tratamiento del riesgo considerando los niveles de riesgo que se han estimado (Lachapelle & Halili, 2015).

A continuación se enuncian las tareas que deben realizarse para la evaluación del ciber riesgo:

- Consolidar los resultados del análisis de Ciber riesgos.
- Evaluar y comparar los niveles de Ciber riesgo de la compañía.
- Agregación de Ciber Riesgos. La evaluación del ciber riesgo se realiza individualmente, sin embargo es importante una evaluación conjunta para determinar los niveles a los que se expone la compañía de manera combinada.
- Agrupación de Ciber riesgos. La agrupación de Ciber riesgos puede dar origen a nuevas formas de este tipo de riesgo que se deben considerar al momento de realizar la evaluación.

3. Tratamiento del Ciber riesgo.

Por la naturaleza altamente técnica del Ciber riesgo, las opciones para el tratamiento de este tipo de riesgo son también de carácter técnico; además, también tiene implicaciones en el tratamiento del ciber riesgo la distinción entre aquellos maliciosos y los no maliciosos.

A continuación se exponen aquellos aspectos más relevantes en cuanto a las opciones del tratamiento del ciber riesgo.

a. Reducción del Ciber riesgo.

El Ciber riesgo puede reducirse a través de la implementación o cambio de controles de ciber seguridad que permitan reducir las vulnerabilidades y proteger de mejor manera los ciber activos. Cuando se realice este proceso la organización debe asegurarse que las soluciones cumplen suficientemente los requerimientos de ciber seguridad que se necesitan.

Dichos controles pueden implementarse a través de la corrección, eliminación, prevención, disuasión, detección, recuperación, vigilancia y sensibilización; buscando las formas más eficaces y eficientes para la compañía. Se suelen utilizar modelos de ciber riesgo que aporten información sobre las ciber amenazas más probables y las vulnerabilidades más graves (Refsdal, Solhaug, & Stølen, 2015).

Para reducir la probabilidad de amenazas y la gravedad de las vulnerabilidades, se consideran las diversas partes y aspectos de los ciber-sistemas de la organización y cómo estos interactúan con el ciberespacio. Esto incluye aplicaciones, servidores, clientes y redes. Para las amenazas no maliciosas, puede ser posible, por ejemplo, eliminar fuentes de amenaza mediante la implementación de barreras técnicas, como un control de acceso más estricto para reducir la posibilidad de fugas accidentales de datos sensibles. Los tratamientos de carácter más socio técnico incluyen una mayor sensibilización y formación en materia de seguridad, políticas de seguridad mejoradas y procesos y rutinas mejorados.

Deben tenerse en cuenta los tiempos y el costo de la implementación de los controles, así como también aspectos técnicos, del entorno y culturales de la organización (ISO/IEC 27005:2011, 2011). Las limitaciones que pueden presentarse al momento de reducir el ciber riesgo están relacionadas con el tiempo, el dinero a invertir y las técnicas utilizadas para hacerlo.

b. Retención del Ciber riesgo.

La retención del Ciber riesgo está determinada por los resultados obtenidos de la evaluación, si estos muestran que los niveles de vulnerabilidad y protección que tiene la compañía son aceptables, no es necesario implementar controles adicionales.

c. Evitación del Ciber riesgo.

La evitación natural del Ciber riesgo corresponde a la desconexión de los ciber sistemas del Ciberespacio, esto implicaría una pérdida de competitividad para las organizaciones debido a la relevancia del Internet de las cosas para los negocios.

No obstante, en muchas ocasiones es relevante buscar alternativas cuando la exposición al ciber riesgo pueda ser demasiado alta para una organización y esta no cuente con los recursos suficientes para reducir el riesgo. A modo de ejemplo puede considerarse el hecho de finalizar el uso de servicios en la nube o aplicaciones web y reemplazarlos por soluciones internas (Refsdal, Solhaug, & Stølen, 2015).

d. Transferencia del Ciber riesgo.

Esta opción de tratamiento del ciber riesgo implica a otras partes, tales como compañías de seguros, o subcontratistas que supervisan los sistemas de información contra ciber amenazas. Debe tenerse en cuenta, que esto no significa que la responsabilidad sea compartida, ya que la responsabilidad de las consecuencias sigue siendo de la organización (Lachapelle & Halili, 2015).

El Ciber seguro es una clase de seguro que ha comenzado a surgir con el propósito de cubrir una amplia gama de riesgos relacionados con el ciberespacio (European Network and Information Security Agency, 2012). Estos productos del sector

asegurador todavía son inmaduros, pero las compañías están ofreciendo cada vez más este tipo de pólizas, puede verse por ejemplo como Mapfre ofrece en la actualidad un ciber seguro con coberturas de responsabilidad civil y daños propios para las empresas (Mapfre, 2017).

4. Modelos avanzados de valoración actuarial del Ciber riesgo.

Las soluciones cuantitativas para abordar el análisis y evaluación de la gerencia del ciber riesgo son limitadas, una de estas limitaciones es la falta de información acerca de qué riesgos tienen mayor probabilidad de materializarse; los ciber riesgos se presentan aparentemente como fenómenos de baja frecuencia y alta severidad (Solomon, 2016). Se pretende entonces, proporcionar herramientas cuantitativas para el análisis del ciber riesgo.

La información que se ha logrado recopilar es gracias a las leyes que se han venido promulgando en los Estados Unidos y que obligan a las empresas o agencias gubernamentales a notificar a las personas cuando una violación de seguridad comprometa su información personal.

Dentro de la información personal se catalogan: El nombre de una persona, número de Seguro Social, licencia de conducir, números de cuentas bancarias, información médica, seguro de salud o información recolectada a través de un sistema propio de las compañías; ID de usuarios y contraseñas u otras formas de validación que permiten el acceso a cuentas en línea.

La notificación tiene unas características que la ley determina y deben enviarse copias a la Fiscalía General del Estado correspondiente.

Las instituciones financieras y las instituciones con información médica están sujetas –en Estados Unidos– a leyes federales que las obliga a adoptar procedimientos que protejan los datos y notifiquen cuando han ocurrido accesos no

autorizados a los datos de sus clientes y usuarios y estos datos hayan sido mal utilizados.

Estas leyes no sólo aplican para las empresas que prestan el servicio directamente, sino también para los proveedores informáticos y todos aquellos que están relacionados con la manipulación de la información.

4.1 Descripción de la muestra.

Para el presente trabajo los datos fueron tomados del Centro de Información sobre los derechos de privacidad, PRC por sus siglas en inglés, una organización sin fines de lucro que se dedica a la educación y defensa de los consumidores en todo lo relacionado con la protección de su privacidad, esta compañía se encuentra ubicada en San Diego, California (Privacy Right Clearinghouse, 2017) .

La información se extrajo del reporte sobre violación de datos y corresponde a todos aquellos incidentes en los que un dato sensible, protegido o confidencial, es copiado, transmitido, visto, robado o usado por un individuo no autorizado para hacerlo.

La información se ha publicado cronológicamente desde el año 2005 hasta el momento de realizar el estudio, correspondiente al 7 de Marzo del año 2017. Como se informa en la página web de la Institución no es una base datos exhaustiva ya que no se es capaz de enumerar cada incumplimiento, además, muchas de las organizaciones no son conscientes de que han sido violadas o no están obligados a reportar. Los datos correspondientes a China –por ejemplo– se limitan a violaciones reportadas dentro de los Estados Unidos; si una violación afecta a un individuo fuera de Estados Unidos solo aparece registrada si también se encuentran afectados otros individuos dentro de Estados Unidos (Privacy Right Clearinghouse, 2017).

La base de datos contiene 5.354 registros con las siguientes variables:

a. **Compañía:** La base de datos cuenta con los nombres de las compañías que fueron objetivo del ciberataque.

b. **Ubicación:** Como ubicación se registra la sede principal de las compañías que fueron atacadas.

c. **Tipo de ataque:** Las violaciones de datos fueron clasificadas en 8 tipos.

- **Payment Card Fraud (CARD)** Es el fraude de tarjetas débito o crédito, corresponde a todos los fraudes realizados a este tipo de tarjetas que no se logra mediante piratería, sino por ejemplo a través de escaneo con dispositivos en terminales de puntos de servicio.

- **Hacking or Malware (HACK).** Corresponde a ataques maliciosos que provenientes del exterior o infectados por Malware; son causados por ciber delincuentes

- **Insider (INSD).** Información privilegiada, alguien con acceso legítimo infringe intencionalmente información, ya sea un empleado, un proveedor o un cliente.

- **Physical Loss (PHYS).** Incluye documentos en papel físico no electrónico que se pierden, descartan o son robados.

- **Portable Device (PORT).** Ordenadores portátiles, asistentes digitales, teléfonos inteligentes, memorias de almacenamiento, CDS, discos duros, cintas de datos y otros dispositivos que almacenan información vital del negocio y que se pierden o son robados.

- **Stationary Device (STAT).** Dispositivos fijos como ordenadores o servidores, que se pierden o son robados.

- **Unintended Disclosure (DISC).** Divulgación no intencionada que no implica piratería informática, incumplimiento intencional o pérdida física - por ejemplo: información confidencial publicada masivamente, maltratada o enviada a la parte equivocada mediante publicación en línea, envío de un correo electrónico, envío por correo o envío por fax.

d. **Tipo de Organización:** El tipo de organización que ha sido objeto del ataque, también es incluido dentro de la base de datos en las siguientes categorías.

- **Businesses-Financial and Insurance Services (BSF).** Empresas de servicios financieros y de seguros.

- **Businesses-Retail/Merchant - Including Online Retail (BSR).** Negocios de comercio, ventas directas, incluyendo ventas en línea.

- **Educational Institutions (EDU).** Instituciones Educativas.

- **Government & Military (GOV).** Instituciones Gubernamentales y Militares.

- **Healthcare, Medical Providers & Medical Insurance Services (MED).** Salud, proveedores médicos

- **Nonprofits NGO.** Organizaciones sin fines de lucro.

- **Businesses – Other (BSO).** Otros negocios que no se clasificaron en las categorías anteriores.

e. **Severidad:** La base de datos aporta la cantidad de datos comprometida en

cada violación a los sistemas informáticos, esta variable será considerada como la severidad dentro del estudio.

4.2 Análisis descriptivo univariante.

A continuación se realiza el análisis de cada una de las variables que forman parte de la base de datos.

a. Tipo de Ataque.

TipoAtaque

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	CARD	66	1,2	1,2	1,2
	DISC	977	18,2	18,2	19,5
	HACK	1580	29,5	29,5	49,0
	INSD	569	10,6	10,6	59,6
	PHYS	585	10,9	10,9	70,5
	PORT	1177	22,0	22,0	92,5
	STAT	249	4,7	4,7	97,2
	UNKN	151	2,8	2,8	100,0
	Total	5354	100,0	100,0	

Tabla 1. Tabla de frecuencia variable tipo de ataque

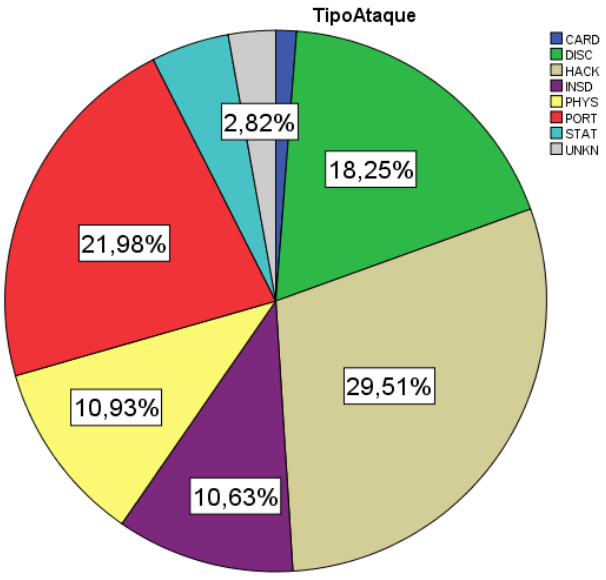


Gráfico 1. Frecuencia de la variable Tipo de Ataque

El 29,51% de las amenazas cibernéticas proviene de Hacking o Malware, es decir proviene de amenazas maliciosas, seguido por un 21,98% de dispositivos portátiles, en tercer lugar el 18,25% de las ciberamenazas corresponden a divulgación no intencionada de información, es decir amenazas no maliciosas.

b. **Tipo de Organización.**

TipoOrg

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	BSF	671	12,5	12,5	12,5
	BSO	883	16,5	16,5	29,0
	BSR	553	10,3	10,3	39,4
	EDU	788	14,7	14,7	54,1
	GOV	747	14,0	14,0	68,0
	MED	1602	29,9	29,9	97,9
	NGO	110	2,1	2,1	100,0
	Total	5354	100,0	100,0	

Tabla 2. Frecuencia de la variable tipo de Organización

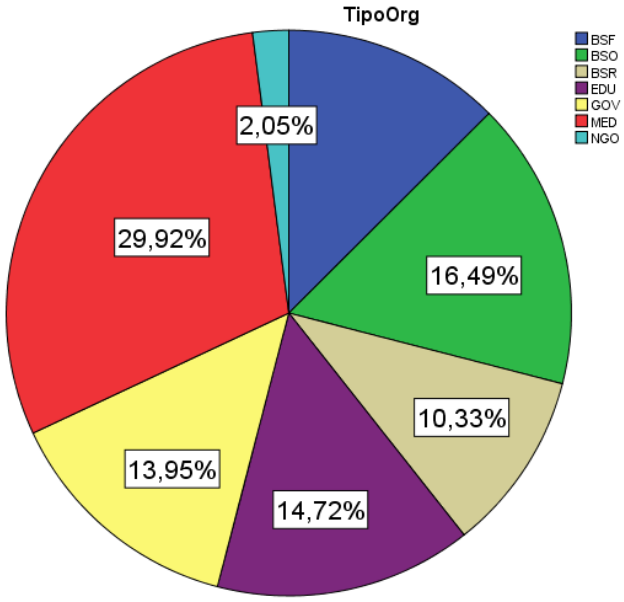


Gráfico 2. Frecuencia de la variable tipo de Organización

Las organizaciones que presentación mayor cantidad de ciber ataques son aquellas correspondientes al sector salud y proveedores médicos con un 30% aproximadamente, seguido por organizaciones que no fueron clasificadas con un 16,5% de participación, en tercer lugar aparecen las empresas del sector educativo con una participación del 14,7%.

4.3 Análisis de la frecuencia y de la severidad.

a. Frecuencia.

Se organizaron los datos en una serie histórica diaria, generando una tabla de frecuencia para identificar el número de ataques presentado por día. La tabla de frecuencias se muestra a continuación.

Categoría	*Frec. Absoluta*	*Frec. Relativa*
0	*1875.00*	*0.4222*
1	*1159.00*	*0.2610*
2	*679.00*	*0.1529*
3	*394.00*	*0.0887*
4	*174.00*	*0.0392*
5	*90.00*	*0.0203*
6	*32.00*	*0.0072*
7	*17.00*	*0.0038*
8	*8.00*	*0.0018*
9	*4.00*	*0.0009*
10	*6.00*	*0.0014*
11	*1.00*	*0.0002*
12	*1.00*	*0.0002*
13		*0.0000*
14		*0.0000*
15	*1.00*	*0.0002*

Tabla 3. Frecuencia de la variable No. Sinietros

Con estos datos se ha construido el gráfico de la frecuencia para tratar de ajustarlo a una función de distribución.

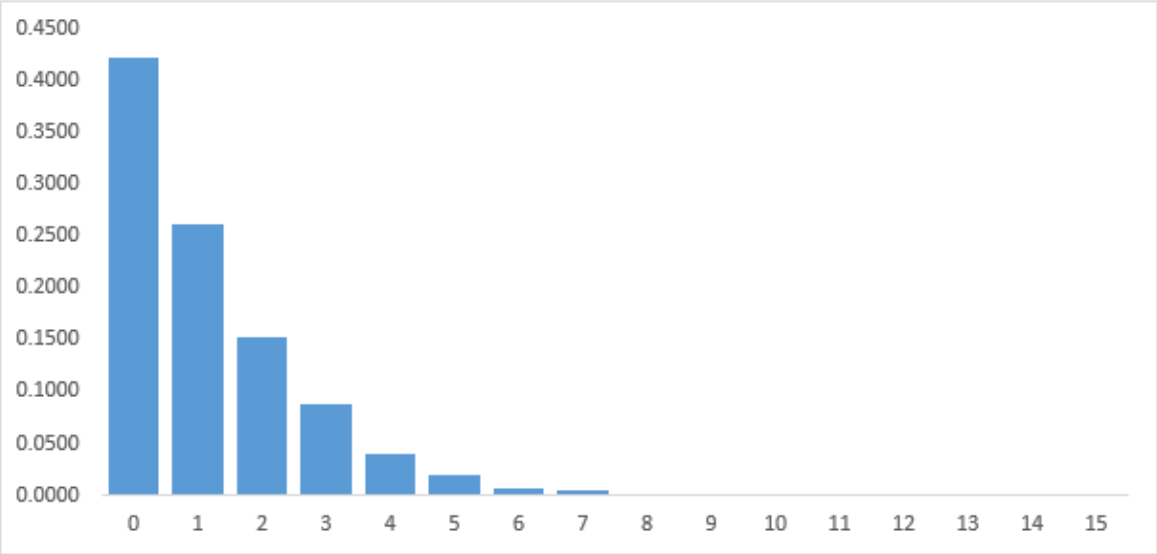


Gráfico 3. Frecuencia de la variable No. Siniestros

Se realizó la prueba de bondad de ajuste con el test Chi cuadrado en Matlab para determinar a qué distribución de probabilidad se ajusta la frecuencia. Se probó con una distribución Poisson y una Binomial Negativa, a continuación los resultados.

- **Distribución Poisson.**

Los parámetros de la distribución con los intervalos de confianza fueron obtenidos con el comando fitdist.

```
Poisson distribution
  lambda = 1.20586    [1.17356, 1.23816]
```

Se utilizó el comando chi2gof de Matlab para realizar la prueba de bondad de ajuste.

```
h =

     1


p =

  7.5062e-117


std =

    chi2stat: 534.7734
          df: 2
       edges: [4.9407e-324 1.5000 3.0000 4.5000 15.0000]
           O: [3033 1073 174 160]
           E: [2.9327e+03 1.3551e+03 117.1269 35.0725]
```

El resultado de h representa 0 o 1, en este caso el resultado 1 significa que se rechaza la hipótesis nula, lo cual significa que los datos no se ajustan a la distribución Poisson.

El valor p representa el valor de significancia de la prueba de hipótesis, que en este caso es muy cercano a 0, razón para rechazar la hipótesis nula.

- **Distribución Binomial Negativa.**

Se utilizan los mismos comandos de matlab obteniendo en este caso los parámetros de la distribución binomial negativa con los intervalos de confianza.

```
Negative Binomial distribution
  R =  1.40985   [1.25936, 1.56034]
  P = 0.538994   [0.510965, 0.567024]
```

```
h =

     0


p =

    0.1827


std =

    chi2stat: 4.8554
          df: 3
       edges: [4.9407e-324 1.5000 3.0000 4.5000 6.0000 7.5000 15.0000]
           O: [3033 1073 174 122 17 21]
           E: [3.0650e+03 1.0221e+03 178.6049 132.9622 21.4109 19.9671]
```

El resultado de h= 0, significa que se acepta la hipótesis nula, lo cual significa que los datos de la frecuencia se pueden ajustar a una distribución binomial negativa con parámetros r = 1.40985 y p = 0.538994

El valor p de significancia en este caso es igual a 0.1827 mayor a 0.05 por lo que se acepta la hipótesis nula.

La siguiente gráfica muestra los datos de la frecuencia y las funciones de densidad de la distribución Poisson y la Binomial Negativa que se utilizaron para la realización de los test de bondad de ajuste.

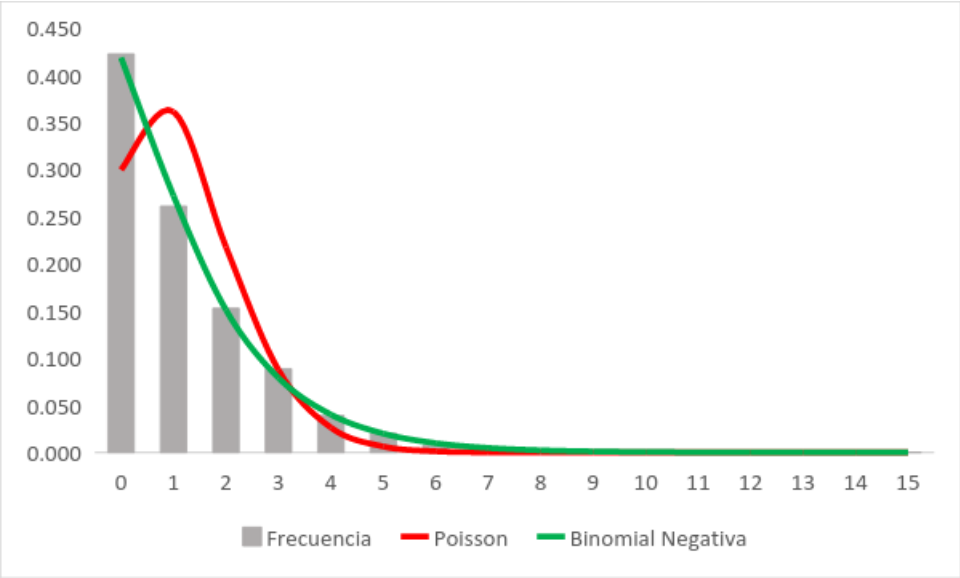


Gráfico 4. Ajuste de la distribución de la variable No. Siniestros

b. Severidad

Del análisis de la muestra se observa que el número de datos promedio comprometidos en cada ataque corresponde 387.632,40, con una muy elevada desviación típica de 4.580.022,191 lo que indicaría un alto nivel de dispersión en los datos. De hecho, si se calcula el Coeficiente de Variación (11.81) se observa que éste es por mucho mayor de 0,5 por lo que se puede concluir que el valor medio no es representativo de los valores de la muestra.

Tanto el hecho de que la media sea superior a la mediana (387.632,40 vs 2.500) y que el coeficiente de asimetría sea positivo (19,942) nos indican que la distribución es asimétrica por la derecha o asimétrica positiva.

A continuación la tabla obtenida del programa SPSS muestra los estadísticos descriptivos de la variable severidad:

Estadísticos

Severidad

N	Válido	2343
	Perdidos	3011
Media		387632,4046
Error estándar de la media		94619,67193
Mediana		2500,0000
Moda		100,00
Desviación estándar		4580022,191
Varianza		2,098E+13
Asimetría		19,942
Error estándar de asimetría		,051
Curtosis		454,558
Error estándar de curtosis		,101
Rango		129999998,0
Mínimo		2,00
Máximo		130000000,0
Suma		908222724,0
Percentiles	10	60,0000
	20	200,0000
	25	327,0000
	30	550,0000
	40	1200,0000
	50	2500,0000
	60	5423,6000
	70	13000,0000
	75	19776,0000
	80	35000,0000
	90	111518,0000

Tabla 4. Estadísticos descriptivos de la variable Severidad

Con el análisis gráfico mediante la elaboración de un histograma, se confirma asimetría por la derecha, no ajustándose por tanto a una distribución normal. Se observan también la posible existencia de outliers en la cola derecha de la distribución.

Se genera el diagrama de cajas confirmando la presencia de valores muy extremos.

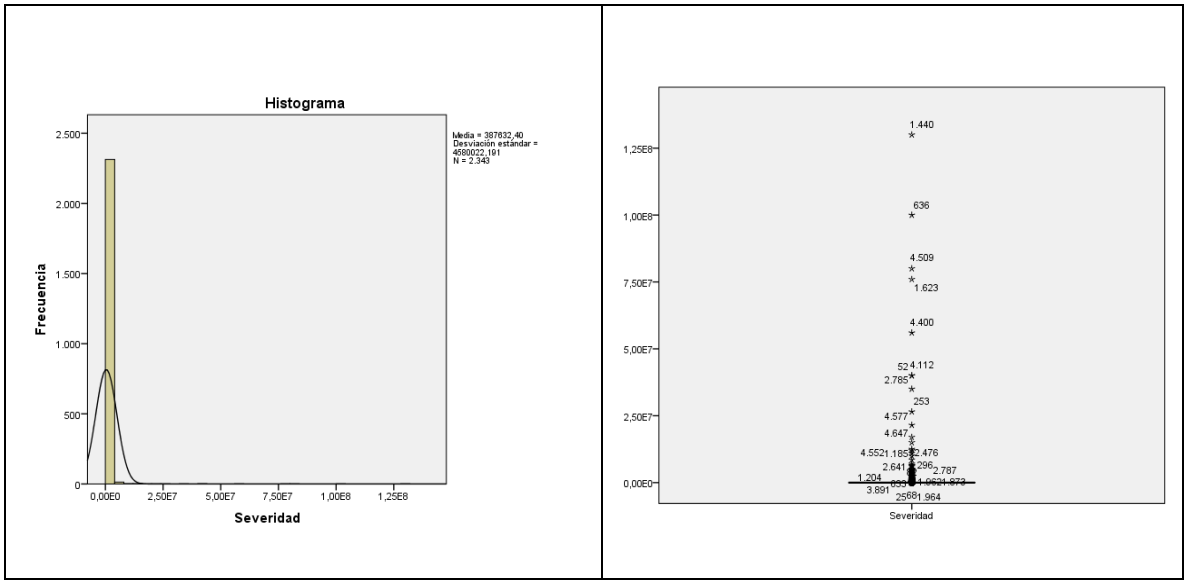


Gráfico 5. Histograma y diagrama de cajas de la variable Severidad

Con la información analizada se puede concluir que para realizar un mejor análisis debe realizarse una transformación de la misma, pasando a un modelo basado en logaritmo neperiano, obteniendo la variable Ln_Transf. Con dicha transformación se consigue expandir los datos y corregir la asimetría. Posteriormente, se realiza una prueba paramétrica para determinar si se puede aceptar la hipótesis de que sigue una distribución normal:

Prueba de Kolmogorov-Smirnov para una muestra

		Ln_Transf
N		2343
Parámetros normales[a,b]	Media	7,9466
	Desviación estándar	2,92046
Máximas diferencias extremas	Absoluta	,025
	Positivo	,025
	Negativo	-,021
Estadístico de prueba		,025
Sig. asintótica (bilateral)		,002[c]

a. La distribución de prueba es normal.

b. Se calcula a partir de datos.

c. Corrección de significación de Lilliefors.

Tabla 5. Prueba de Normalidad de Kolmogorov Smirnov

Por tener más de cincuenta datos utilizamos la prueba de Kolmogorov Smirnov y el nivel de significación para esta prueba es de 0.002 <0.05, por lo que aceptamos la hipótesis alternativa y decimos que la distribución de la variable es diferente a la distribución normal.

Se procede a realizar el estudio estadístico de la nueva variable:

Estadísticos

Ln_Transf

N	Válido	2343
	Perdidos	3011
Media		7,9466
Error estándar de la media		,06033
Mediana		7,8240
Moda		4,61
Desviación estándar		2,92046
Varianza		8,529
Asimetría		,308
Error estándar de asimetría		,051
Curtosis		-,042
Error estándar de curtosis		,101
Rango		17,99
Mínimo		,69
Máximo		18,68
Suma		18618,81
Percentiles	10	4,0943
	20	5,2983
	25	5,7900
	30	6,3099
	40	7,0901
	50	7,8240
	60	8,5985
	70	9,4727
	75	9,8922
	80	10,4631
	90	11,6219

Tabla 6. Estadísticos descriptivos de la variable transformada Severidad

Tras la transformación, se obtiene una media de 7,9466 y una desviación típica de 2,92046 con un coeficiente de variación (0,3675) inferior a 0,5 de esta manera se puede afirmar, que la media ahora sí es representativa de la distribución.

Se genera el histograma para la nueva variable y, aunque ajusta mejor a una distribución normal aún se observa cierta asimetría por la derecha. Todavía contamos con la presencia de puntos extremos. Para confirmarlo se elaboró el diagrama de caja.

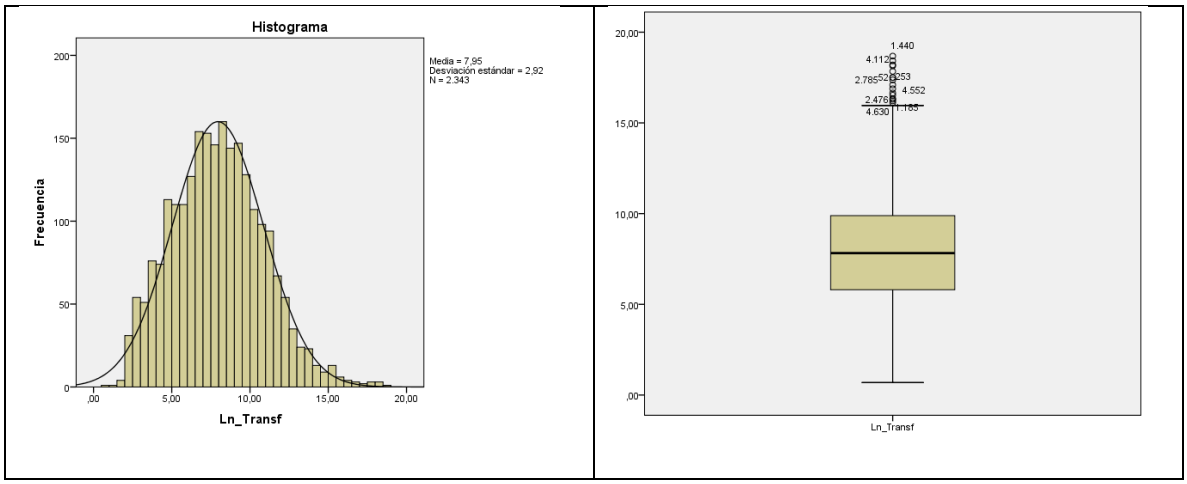


Gráfico 6. Histograma y diagrama de cajas de la variable transformada de la Severidad.

Se realizó la prueba chi cuadrado de bondad de ajuste para ajustar la Severidad a una función de distribución conocida. A continuación se muestran las distribuciones para las cuales se realizó la prueba Chi cuadrado y el p valor obtenido en cada una.

Distribución	*p- Valor*
Burr Type XII	*0.1655*
Weibull	*0.0057*
Normal	*8.5556E-08*
Gamma Distribution	*7.4192E-14*
LogNormal	*1.4732E-48*
Exponential	*0*

Tabla 7. p valor prueba bondad de ajuste chi cuadrado

Como puede observarse se realizó la prueba con las distribuciones más conocidas, sin embargo con un nivel de significancia del 0.05 se rechazó la hipótesis nula, siendo la distribución Weibull la más cercana con un p valor de 0.0057, se probó con distribuciones menos conocidas y se encontró que la distribución Burr Type XII se ajusta a los datos presentados para la severidad de los Ciber ataques.

- **Distribución Burr Type XII**

A continuación se muestran los parámetros de la distribución Burr Tipo XII obtenidos de Matlab con su respectiva prueba chi cuadrado de bondad de ajuste.

```
  BurrDistribution

  Burr distribution
    alpha = 17.6986   [13.6818, 22.8947]
        c = 3.15018   [2.99368, 3.31487]
        k = 9.42121   [4.82536, 18.3943]

>> [h, p, std]= chi2gof(observaciones, 'cdf', ans)

h =

     0


p =

    0.1655


std =

    chi2stat: 9.1474
          df: 6
       edges: [1x11 double]
           O: [37 217 381 547 526 374 170 59 23 9]
           E: [1x10 double]
```

Esta distribución pertenece a una familia de distribuciones descrita por Burr en 1942, esta produce una amplia gama de valores de asimetría y/o curtosis (Rodriguez, 1977), en su primera versión fue presentada como una distribución de la familia de dos parámetros, sin embargo en 1980 Tadikamalla introduce un parámetro de escala adicional, por lo tanto pertenece a la familia de las distribuciones con tres parámetros en la recta real positiva, permitiendo expresar una amplia gama de formas para la distribución, algunas distribuciones compuestas dan como resultado este tipo de distribución.

Una de las principales ventajas de la distribución de Burr Tipo XII es que se ajustan muy bien a datos empíricos, dado que cubren un amplio espectro de asimetría y curtosis (MathWorks, 2017). La función de probabilidad viene dada por la siguiente ecuación.

$$f(x|\alpha, c, k) = \frac{\frac{kc}{\alpha}\left(\frac{x}{\alpha}\right)^{c-1}}{\left(1+\left(\frac{x}{\alpha}\right)^{c}\right)^{k+1}}, \quad x > 0,\ \alpha > 0,\ c > 0,\ k > 0\,.$$

Ecuación 1. Función de probabilidad de la distribución Burr Tipo XII
Fuente: (MathWorks, 2017)

4.4 Cuantificación del Ciber riesgo.

Con la distribución de la frecuencia y la severidad y asumiendo que ambas variables son independientes, puede calcularse la media de la distribución agregada utilizando la ecuación:

$$E(y) = E(N)E(S)$$

Ecuación 2. Media de la distribución agregada de la frecuencia y la severidad

La media de N corresponderá a la media de la distribución binomial negativa y la media de S será el momento de orden uno de la distribución Burr Tipo XII.

- **Media de la Frecuencia $E(N)$**

Reemplazando en la ecuación de la media de la Binomial Negativa los parámetros calculados en el numeral 4.3 obtenemos:

$$E(N) = \frac{r(1-p)}{p} = 1.2058563$$

Ecuación 3. Media de la distribución Binomial Negativa

- **Media de la Severidad $E(S)$**

Para calcular la media de la Severidad utilizamos el momento de orden uno de la distribución Burr Type XII

$$E(S) = k\beta\left(k - \frac{1}{c}, 1 + \frac{1}{c}\right) = 4.7$$

Ecuación 4. Media de la función de distribución Burr Tipo XII

Donde β corresponde a la función beta. Como se ha realizado el ajuste sobre la variable transformada, se transforma este valor a su escala de origen utilizando la función exponencial, de esta manera.

$$E(S) = 111.119$$

La media de la distribución agregada será entonces.

$$E(y) = E(N)E(S) = 134$$

Este valor indica que de la información analizada, las compañías en un día tienen en media una exposición al ciber riesgo de 134 registros.

Todavía no se ha llegado a un consenso de cuanto es el valor de un registro o un ciberactivo, un estudio de NetDiligence sobre reclamaciones al sector asegurador por concepto de Ciber riesgo indica que el costo por registro en una reclamación por un incidente cibernético va desde un mínimo de $ 0.03 USD hasta un máximo de $ 1.6 Millones USD por un solo registro, con una media de $ 17.000 USD, siendo el costo con mayor frecuencia presentado $ 39.82 USD (Net Diligence, 2016).

Al momento de calcular el valor del Ciber riesgo no sólo debe tenerse en cuenta el costo de los datos o la información comprometida, sino también otros costos asociados a las consecuencias de los ciber ataques, siguiendo el mismo estudio de NetDiligence estos costos en promedio para la industria aseguradora representan en promedio 665.000 USD de los cuales el 75% se utilizó en reestablecer los servicios o en cubrir los costos generados por una crisis en la prestación del servicio, el 3% en cubrir los servicios de defensa legal, 10% en el pago de multas e indemnizaciones gubernamentales y 8% en defensa regulatoria. (Net Diligence, 2016) .

4.5 Análisis Bivariante.

4.5.1 Medidas de asociación.

Para establecer la relación entre dos variables cualitativas primero se analiza si existe relación entre ellas (es decir si son dependientes) y, en caso afirmativo, se determina el tipo de asociación que presenta.

Para estudiar la existencia de relación entre estas variables, se utiliza el contraste de independencia chi cuadrado. Posteriormente, para determinar el grado de dependencia en caso de que exista se utilizarán diferentes medidas de asociación.

Como sólo podemos establecer las medidas de asociación mediante variables cualitativas, se recodifica la variable cuantitativa transformada de la severidad en una nueva variable categórica, utilizando el criterio del percentil, de esta manera se establecen 5 grupos de severidad de la siguiente manera:

Pecentil	Desde	Hasta	Categoría
20%	0	5.3	1
40%	5.3	7.1	2
60%	7.1	8.6	3
80%	8.6	10.5	4
100%	10.5	Máx	5

Tabla 8. Categorización de la variable transformada de la Severidad a través del método del percentil.

A continuación se realizó la prueba de significación asintótica de la prueba chi cuadrado entre cada una de las variables cualitativas con la variable Categoría Severidad, tratando de identificar la dependencia entre ellas. Se realiza contraste estadístico con los valores correspondientes a la prueba exacta de Fisher y se verifica la hipótesis nula Ho = Las variables no son dependientes, hipótesis que se rechaza cuando el nivel de significancia es <0,05

a. Tipo de Ataque v.s Categoría Severidad.

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	279,011[a]	28	,000
Razón de verosimilitud	276,220	28	,000
N de casos válidos	2343		

a. 0 casillas (0,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es 5,79.

Tabla 9. Prueba chi-cuadrado asociación variables Tipo Ataque v.s Categoría Severidad.

Rechazo Ho por lo que puede intuirse que existe asociación entre el tipo de ataque y la severidad.

Medidas direccionales

			Valor	Error estándar asintótico[a]	Aprox. S[b]	Aprox. Sig.
Ordinal por ordinal	d de Somers	Simétrico	,039	,016	2,441	,015
		TipoAtaque dependiente	,039	,016	2,441	,015
		GrupoSev dependiente	,038	,016	2,441	,015

a. No se supone la hipótesis nula.

b. Utilización del error estándar asintótico que asume la hipótesis nula.

Medidas simétricas

		Valor	Error estándar asintótico[a]	Aprox. S[b]	Aprox. Sig.
Ordinal por ordinal	Tau-b de Kendall	,039	,016	2,441	,015
	Tau-c de Kendall	,039	,016	2,441	,015
N de casos válidos		2343			

a. No se supone la hipótesis nula.

b. Utilización del error estándar asintótico que asume la hipótesis nula.

Tabla 10. Medidas de asociación entre el Tipo de Ataque y la categoría de la Severidad.

Utilizando las medidas de asociación identificamos que el grado de asociación presentada entre este par de variables es muy baja 0,039, un grado de asociación se considera bajo o débil si es menor a 0.2

b. Tipo de Organización v.s Categoría Severidad.

Tabla cruzada

Recuento

		GrupoSev					Total
		1,00	2,00	3,00	4,00	5,00	
TipoOrg	BSF	81	60	46	49	68	304
	BSO	46	52	41	49	60	248
	BSR	76	37	30	16	40	199
	EDU	90	106	130	136	82	544
	GOV	86	83	98	92	90	449
	MED	93	110	113	129	106	551
	NGO	14	9	5	14	6	48
Total		486	457	463	485	452	2343

Tabla 11. Tabla cruzada de las variables Tipo Organización v.s Categoría Severidad.

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	99,148[a]	24	,000
Razón de verosimilitud	98,673	24	,000
N de casos válidos	2343		

a. 0 casillas (0,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es 9,26.

Tabla 12. Prueba chi-cuadrado asociación tipo de organización y categoría Severidad.

Se rechaza Ho por lo que puede intuirse que existe un grado de asociación entre el tipo de organización y la severidad.

Medidas direccionales

			Valor	Error estándar asintótico[a]	Aprox. S[b]	Aprox. Sig.
Ordinal por ordinal	d de Somers	Simétrico	,035	,017	2,094	,036
		TipoOrg dependiente	,036	,017	2,094	,036
		GrupoSev dependiente	,035	,017	2,094	,036

a. No se supone la hipótesis nula.

b. Utilización del error estándar asintótico que asume la hipótesis nula.

Medidas simétricas

		Valor	Error estándar asintótico [a]	Aprox. S [b]	Aprox. Sig.
Ordinal por ordinal	Tau-b de Kendall	,035	,017	2,094	,036
	Tau-c de Kendall	,036	,017	2,094	,036
N de casos válidos		2343			

a. No se supone la hipótesis nula.

b. Utilización del error estándar asintótico que asume la hipótesis nula.

Tabla 13. Medidas de asociación entre el Tipo de Organización y la categoría de la Severidad.

Utilizando las medidas de asociación se identifica que el grado de asociación presentada entre este par de variables es muy baja 0,035, un grado de asociación se considera bajo o débil si es menor a 0.2.

c. Tipo Org. v.s Tipo de ataque.

Tabla cruzada

Recuento

		TipoAtaque								Total
		CARD	DISC	HACK	INSD	PHYS	PORT	STAT	UNKN	
TipoOrg	BSF	24	112	156	97	58	160	27	37	671
	BSO	5	96	487	62	57	136	22	18	883
	BSR	35	50	260	71	37	66	16	18	553
	EDU	1	227	276	25	56	138	48	17	788
	GOV	0	214	133	79	103	170	24	24	747
	MED	1	267	233	226	264	470	107	34	1602
	NGO	0	11	35	9	10	37	5	3	110
Total		66	977	1580	569	585	1177	249	151	5354

Tabla 14. Tabla cruzada de las variables Tipo Org v.s Tipo Ataque

Pruebas de chi-cuadrado

	Valor	gl	Sig. asintótica (2 caras)
Chi-cuadrado de Pearson	1093,380[a]	42	,000
Razón de verosimilitud	1051,786	42	,000
N de casos válidos	5354		

a. 2 casillas (3,6%) han esperado un recuento menor que 5. El recuento mínimo esperado es 1,36.

Tabla 15. Prueba chi-cuadrado asociación tipo de organización y Tipo Ataque

Medidas direccionales

			Valor	Error estándar asintótico[a]	Aprox. S[b]	Aprox. Sig.
Ordinal por ordinal	d de Somers	Simétrico	,099	,011	9,224	,000
		TipoOrg dependiente	,100	,011	9,224	,000
		TipoAtaque dependiente	,098	,011	9,224	,000

a. No se supone la hipótesis nula.

b. Utilización del error estándar asintótico que asume la hipótesis nula.

Medidas simétricas

		Valor	Error estándar asintótico[a]	Aprox. S[b]	Aprox. Sig.
Ordinal por ordinal	Tau-b de Kendall	,099	,011	9,224	,000
	Tau-c de Kendall	,093	,010	9,224	,000
N de casos válidos		5354			

a. No se supone la hipótesis nula.

b. Utilización del error estándar asintótico que asume la hipótesis nula.

Tabla 16. Medidas de asociación entre el Tipo de Organización y el tipo de ataque.

Utilizando las medidas de asociación se identifica que el grado de asociación presentada entre este par de variables es muy baja 0,099, un grado de asociación se considera bajo o débil si es menor a 0.2.

4.5.2 Análisis de la Varianza Anova.

En el apartado anterior se concluyó que podía existir dependencia entre la variable cuantitativa Severidad y algunas variables cualitativas, en este apartado se realizará el análisis ANOVA para explicar de qué forma las variables cualitativas (factor) influyen en la variables cuantitativa (Variable dependiente), para ello se determinará qué niveles dentro de cada factor optimizan la variable respuesta.

Se seleccionarán como variables dependiente: Ln_Severidad frente a tipo de ataque y tipo de organización.

El análisis de este apartado incluirá la prueba de homogeneidad de varianzas, el ANOVA, la tabla de comparaciones múltiples y gráficos (diagrama de cajas) y evolución de media por factor.

a. Tipo de Ataque v.s Ln_Severidad.

Prueba de homogeneidad de varianzas

Ln_Transf

Estadístico de Levene	df1	df2	Sig.
4,855	7	2335	,000

Tabla 17. Prueba de homogeneidad de varianzas Tipo Ataque v.s Severidad transformada.

Al analizar el resultado de la prueba de homogeneidad de varianzas, se deduce que no puede aceptarse que las categorías de la variable cualitativa tengan homogeneidad de varianzas dado que el valor de significación es 0,0<0,05.

ANOVA

Ln_Transf

	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Entre grupos	1850,070	7	264,296	34,049	,000
Dentro de grupos	18125,028	2335	7,762		
Total	19975,098	2342			

Tabla 18. Análisis ANOVA Tipo Ataque v.s Severidad transformada.

Al revisar el resultado del análisis ANOVA, se llega a la conclusión que no se tienen medias iguales, 0<0,05 rechazando la hipótesis nula.

Como se tienen medias diferentes y varianzas diferentes, se realiza el análisis de comparaciones múltiples.

Comparaciones múltiples

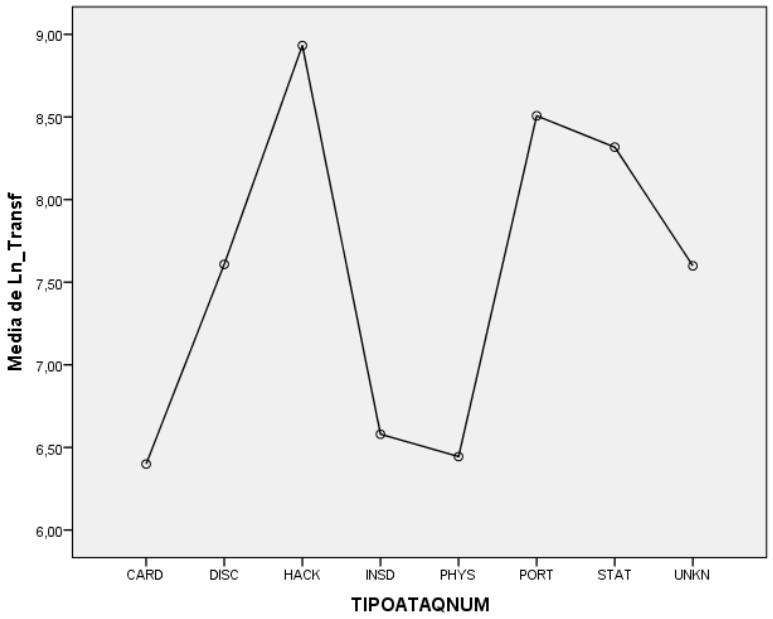
Variable dependiente: Ln_Transf

HSD Tukey

(I) TIPOATAQNUM	(J) TIPOATAQNUM	Diferencia de medias (I-J)	Error estándar	Sig.	95% de intervalo de confianza	
					Límite inferior	Límite superior
CARD	DISC	-1,20872	,52462	,292	-2,8002	,3828
	HACK	-2,53285*	,52308	,000	-4,1197	-,9460
	INSD	-,18049	,53451	1,000	-1,8020	1,4410
	PHYS	-,04485	,54531	1,000	-1,6991	1,6094
	PORT	-2,10738*	,52051	,001	-3,6864	-,5283
	STAT	-1,91757*	,56235	,015	-3,6236	-,2116
	UNKN	-1,19955	,62475	,537	-3,0948	,6957
DISC	CARD	1,20872	,52462	,292	-,3828	2,8002
	HACK	-1,32413*	,17706	,000	-1,8613	-,7870
	INSD	1,02824*	,20841	,000	,3960	1,6605
	PHYS	1,16387*	,23473	,000	,4518	1,8760
	PORT	-,89866*	,16931	,000	-1,4123	-,3850
	STAT	-,70885	,27199	,154	-1,5340	,1163
	UNKN	,00917	,38477	1,000	-1,1581	1,1764
HACK	CARD	2,53285*	,52308	,000	,9460	4,1197
	DISC	1,32413*	,17706	,000	,7870	1,8613
	INSD	2,35237*	,20451	,000	1,7320	2,9728
	PHYS	2,48800*	,23128	,000	1,7864	3,1896
	PORT	,42547	,16449	,161	-,0735	,9245
	STAT	,61528	,26901	,301	-,2008	1,4314
	UNKN	1,33330*	,38267	,012	,1724	2,4942
INSD	CARD	,18049	,53451	1,000	-1,4410	1,8020
	DISC	-1,02824*	,20841	,000	-1,6605	-,3960
	HACK	-2,35237*	,20451	,000	-2,9728	-1,7320
	PHYS	,13563	,25607	1,000	-,6412	,9125
	PORT	-1,92690*	,19783	,000	-2,5271	-1,3267
	STAT	-1,73709*	,29060	,000	-2,6187	-,8555
	UNKN	-1,01906	,39814	,171	-2,2269	,1888
PHYS	CARD	,04485	,54531	1,000	-1,6094	1,6991
	DISC	-1,16387*	,23473	,000	-1,8760	-,4518
	HACK	-2,48800*	,23128	,000	-3,1896	-1,7864
	INSD	-,13563	,25607	1,000	-,9125	,6412
	PORT	-2,06253*	,22540	,000	-2,7463	-1,3788
	STAT	-1,87272*	,31003	,000	-2,8132	-,9322
	UNKN	-1,15469	,41253	,096	-2,4062	,0968
PORT	CARD	2,10738*	,52051	,001	,5283	3,6864
	DISC	,89866*	,16931	,000	,3850	1,4123
	HACK	-,42547	,16449	,161	-,9245	,0735
	INSD	1,92690*	,19783	,000	1,3267	2,5271
	PHYS	2,06253*	,22540	,000	1,3788	2,7463
	STAT	,18981	,26398	,996	-,6110	,9906
	UNKN	,90784	,37914	,244	-,2424	2,0580
STAT	CARD	1,91757*	,56235	,015	,2116	3,6236
	DISC	,70885	,27199	,154	-,1163	1,5340
	HACK	-,61528	,26901	,301	-1,4314	,2008
	INSD	1,73709*	,29060	,000	,8555	2,6187
	PHYS	1,87272*	,31003	,000	,9322	2,8132
	PORT	-,18981	,26398	,996	-,9906	,6110
	UNKN	,71803	,43481	,719	-,6010	2,0371
UNKN	CARD	1,19955	,62475	,537	-,6957	3,0948
	DISC	-,00917	,38477	1,000	-1,1764	1,1581
	HACK	-1,33330*	,38267	,012	-2,4942	-,1724
	INSD	1,01906	,39814	,171	-,1888	2,2269
	PHYS	1,15469	,41253	,096	-,0968	2,4062
	PORT	-,90784	,37914	,244	-2,0580	,2424
	STAT	-,71803	,43481	,719	-2,0371	,6010

*. La diferencia de medias es significativa en el nivel 0.05.

Tabla 19. Prueba de comparaciones múltiples Tipo Ataque v.s Severidad transformada



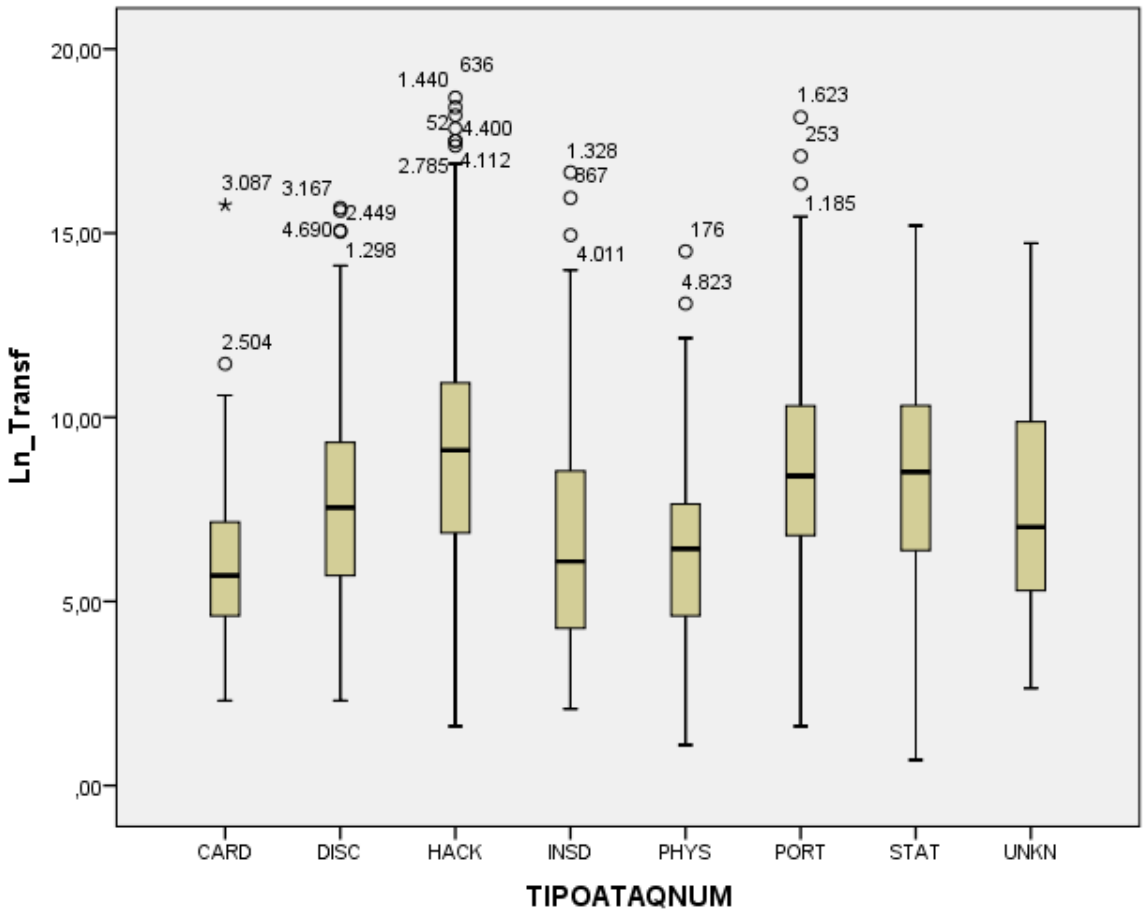


Gráfico 7. Comparación medias Tipo Ataque vs Severidad Transformada

Con el análisis de comparaciones múltiples podemos establecer dos grupos para los tipos de ataques, un grupo lo denominaríamos tipo de ataque más severo donde agruparíamos las categorías Hack, Port, Stat, Unkn (En esta categoría como puede observarse estarían ciber riesgos de carácter malicioso) y un grupo donde agruparíamos los tipos de ataques menos severos Card, Insd, Phys, Disc, esta información es de gran relevancia para la gestión del ciber riesgo, permitiendo identificar los controles adecuados.

b. Tipo de Organización v.s Ln_Severidad

Prueba de homogeneidad de varianzas

Ln_Transf

Estadístico de Levene	df1	df2	Sig.
13,922	6	2336	,000

Tabla 20. Prueba de homogeneidad de varianzas Tipo Organización v.s Severidad

Al analizar el resultado de la prueba de homogeneidad de varianzas, se deduce que no puede aceptarse que las categorías de la variable cualitativa tengan homogeneidad de varianzas dado que el valor de significación es 0,0<0,05.

ANOVA

Ln_Transf

	Suma de cuadrados	gl	Media cuadrática	F	Sig.
Entre grupos	148,002	6	24,667	2,906	,008
Dentro de grupos	19827,097	2336	8,488		
Total	19975,098	2342			

Tabla 21, Análisis ANOVA Tipo Organización v.s Severidad transformada

Al revisar el resultado del análisis ANOVA, se llega a la conclusión que no se tienen medias iguales, 0,008<0,05 rechazando la hipótesis nula.

Como se tienen medias diferentes y varianzas diferentes, se realiza el análisis de comparaciones múltiples.

Comparaciones múltiples

Variable dependiente: Ln_Transf

HSD Tukey

(I) TIPOORGNUM	(J) TIPOORGNUM	Diferencia de medias (I-J)	Error estándar	Sig.	95% de intervalo de confianza	
					Límite inferior	Límite superior
BSF	BSO	-,21874	,24929	,976	-,9544	,5169
	BSR	,72774	,26565	,089	-,0562	1,5117
	EDU	,09757	,20862	,999	-,5180	,7132
	GOV	-,15411	,21639	,992	-,7926	,4844
	MED	-,10352	,20814	,999	-,7177	,5107
	NGO	,44826	,45249	,956	-,8870	1,7835
BSO	BSF	,21874	,24929	,976	-,5169	,9544
	BSR	,94648*	,27726	,012	,1283	1,7647
	EDU	,31630	,22322	,793	-,3424	,9750
	GOV	,06463	,23049	1,000	-,6155	,7448
	MED	,11522	,22277	,999	-,5422	,7726
	NGO	,66700	,45940	,773	-,6886	2,0226
BSR	BSF	-,72774	,26565	,089	-1,5117	,0562
	BSO	-,94648*	,27726	,012	-1,7647	-,1283
	EDU	-,63017	,24136	,123	-1,3424	,0820
	GOV	-,88185*	,24810	,007	-1,6140	-,1497
	MED	-,83126*	,24095	,010	-1,5423	-,1202
	NGO	-,27948	,46848	,997	-1,6619	1,1030
EDU	BSF	-,09757	,20862	,999	-,7132	,5180
	BSO	-,31630	,22322	,793	-,9750	,3424
	BSR	,63017	,24136	,123	-,0820	1,3424
	GOV	-,25167	,18576	,826	-,7998	,2965
	MED	-,20108	,17609	,915	-,7207	,3185
	NGO	,35070	,43867	,985	-,9438	1,6452
GOV	BSF	,15411	,21639	,992	-,4844	,7926
	BSO	-,06463	,23049	1,000	-,7448	,6155
	BSR	,88185*	,24810	,007	,1497	1,6140
	EDU	,25167	,18576	,826	-,2965	,7998
	MED	,05059	,18522	1,000	-,4960	,5972
	NGO	,60237	,44241	,822	-,7031	1,9079
MED	BSF	,10352	,20814	,999	-,5107	,7177
	BSO	-,11522	,22277	,999	-,7726	,5422
	BSR	,83126*	,24095	,010	,1202	1,5423
	EDU	,20108	,17609	,915	-,3185	,7207
	GOV	-,05059	,18522	1,000	-,5972	,4960
	NGO	,55178	,43844	,871	-,7420	1,8456
NGO	BSF	-,44826	,45249	,956	-1,7835	,8870
	BSO	-,66700	,45940	,773	-2,0226	,6886
	BSR	,27948	,46848	,997	-1,1030	1,6619
	EDU	-,35070	,43867	,985	-1,6452	,9438
	GOV	-,60237	,44241	,822	-1,9079	,7031
	MED	-,55178	,43844	,871	-1,8456	,7420

*. La diferencia de medias es significativa en el nivel 0.05.

Tabla 22. Prueba de comparaciones múltiples Tipo Organización v.s Severidad transformada

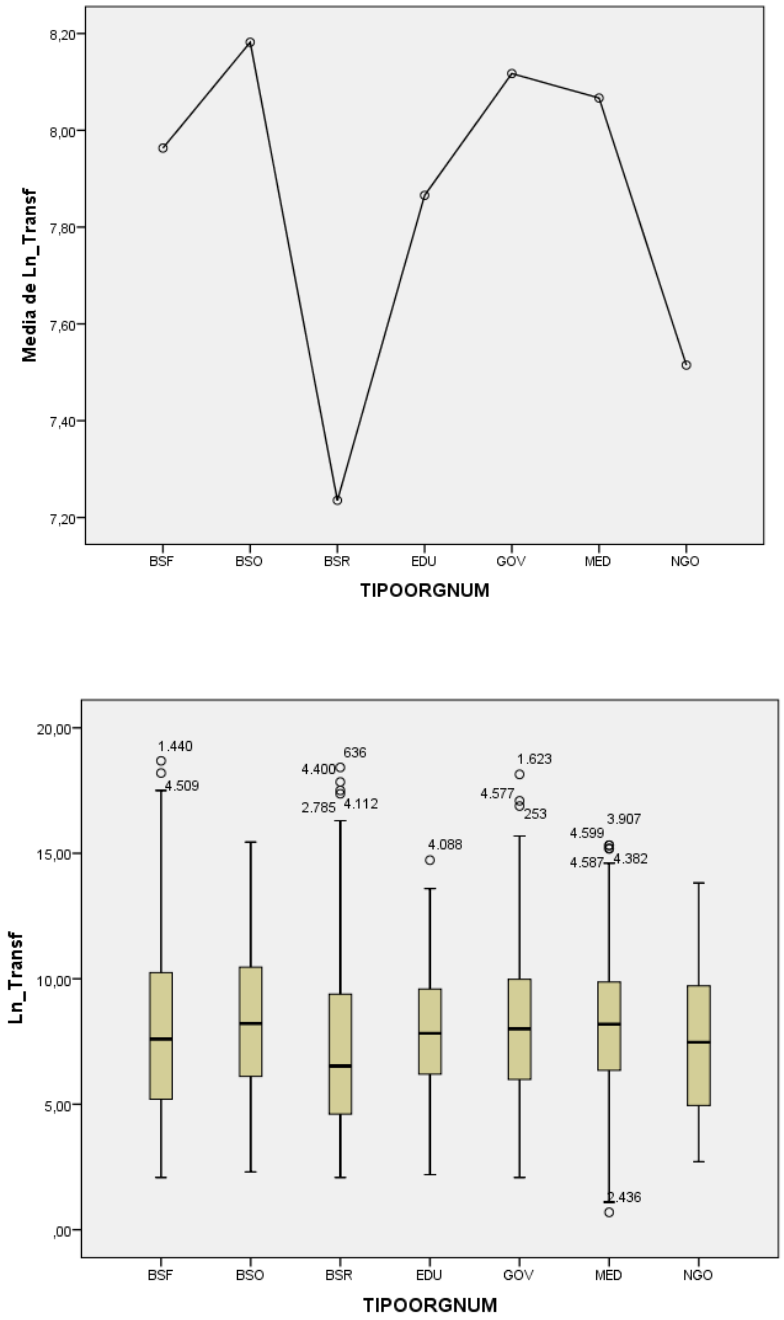


Gráfico 8. Comparación medias Tipo Organización vs Severidad Transformada

De igual manera podemos establecer dos grupos aunque a simple vista pareciera homogeneidad de varianzas y de medias, en un primer grupo se encontrarían los negocios de tipo BSF, BSO, GOV, EDU y MED como los tipos de negocios con mayor severidad y en un segundo grupo con menor severidad NGO y BSR.

4.6 La modelación actuarial con redes neuronales.

Las redes neuronales son una herramienta que pertenece a una categoría denominada Data-mining o minería de datos y que incluye otras herramientas como árboles de decisión, algoritmos genéticos, regresión y splines, técnicas que se utilizan para encontrar patrones en los datos. Estas herramientas son entrenadas para obtener relaciones y la ventaja que presentan sobre modelos tradicionales como la regresión y la ANOVA es que pueden encajar datos donde la relación entre variables dependientes e independientes es no lineal o desconocida.
(Francis , 2001).

El objetivo es mostrar la aplicación que podrían tener las redes neuronales en la modelación actuarial del ciber riesgo, no corresponde explicar el funcionamiento de las mismas.

Se toma como referencia los hallazgos encontrados por Louis Francis, en su artículo Desmitificando las redes neuronales (Francis , 2001).

Las redes neuronales utilizan una serie de neuronas denominadas capa oculta (Hidden Layer) que aplican las funciones de activación no lineales para aproximar funciones complejas en los datos. Muchos estadísticos y actuarios son reacios a las redes neuronales considerándolas como una caja negra. Debido a la complejidad de las funciones utilizadas en las aproximaciones a las redes neuronales, el software por lo general no proporciona al usuario información sobre la naturaleza de la relación entre las variables; la relación entre las variables dependientes e independientes no se hace explícita y no se revela la importancia de cada variable mientras otras técnicas si lo hace.

A continuación se enuncian los usos que podrían darse a las redes neuronales para el análisis actuarial:

Cada vez que una red neuronal se entrena produce un valor predicho para una variable, este valor se compara con el valor real de la variable objetivo y se calcula un error para cada observación, los errores representan una retroalimentación para la red, reduciendo el error cada vez que es entrenada nuevamente. Lo anterior corresponde a un proceso de optimización estadística buscando minimizar la suma de los errores al cuadrado.

Las redes neuronales entonces pueden ser comparadas con la regresión lineal, dado que se pueden utilizar para ajustar una curva a los datos, la diferencia es que en una red neuronal la relación es no lineal (Warner & Misra, 1996).

Utilizando el programa SPSS se utilizó un procedimiento de perceptrón multicapa para generar un modelo de predicción de la variable transformada y categorizada de la severidad utilizando como factores explicativos las variables tipo de organización y tipo de ataque.

La red se entrenó con el 70% de los datos y se puso a prueba con el 30% restante. A continuación el resumen del modelo:

Resumen del modelo

Entrenamiento	Error de entropía cruzada	2500,546
	Porcentaje de pronósticos incorrectos	72,3%
	Regla de parada utilizada	1 pasos consecutivos sin disminución del error[a]
	Tiempo de preparación	0:00:01.26
Pruebas	Error de entropía cruzada	1151,795
	Porcentaje de pronósticos incorrectos	75,2%

Variable dependiente: GrupoSev

a. Los cálculos de error se basan en la muestra de comprobación.

Tabla 23. Resumen del modelo de red neuronal.

El porcentaje de pronósticos incorrectos es muy alto, ya es del 72,3%.

Clasificación

Ejemplo	Observado	Pronosticado					
		1,00	2,00	3,00	4,00	5,00	Porcentaje correcto
Entrenamiento	1,00	156	64	35	32	56	45,5%
	2,00	116	57	42	50	71	17,0%
	3,00	88	35	57	46	93	17,9%
	4,00	68	26	80	45	108	13,8%
	5,00	71	30	62	16	141	44,1%
	Porcentaje global	30,3%	12,9%	16,8%	11,5%	28,5%	27,7%
Pruebas	1,00	63	19	12	19	30	44,1%
	2,00	30	20	27	17	27	16,5%
	3,00	30	22	34	20	38	23,6%
	4,00	40	21	30	22	45	13,9%
	5,00	29	15	22	11	55	41,7%
	Porcentaje global	27,5%	13,9%	17,9%	12,8%	27,9%	27,8%

Variable dependiente: GrupoSev

Tabla 24. Pronósticos correctos del modelo de red neuronal.

Puede observarse que tanto con el entrenamiento, como con la prueba el porcentaje de pronóstico correcto es muy bajo ya que tan solo alcanza el 28% aproximadamente de aciertos en el pronóstico, vale la pena anotar que donde la red alcanzó mejor pronóstico, es en las severidades más bajas y en las más extremas, sin embargo no es un valor significativo.

En el Anexo 1 se encuentra el diagrama de la red obtenida con 4 capas ocultas.

En el Anexo 2 se encuentra una aplicación de ajuste de funciones no lineales con redes neuronales a los datos correspondientes a la función de probabilidad de frecuencia de la muestra estudiado sobre ciber ataques, para este ejercicio se utilizó el paquete de redes neuronales de Matlab.

La aplicación de la red neuronal para tratar de explicar la variable severidad muestra que no son suficientes las variables tipo de organización y tipo de ataque para tratar

de explicarla, podrían requerirse otro tipo de variables que permitirían mejorar la aproximación de los valores pronosticados.

5. Conclusiones.

Todo lo que se ha presentado en este trabajo pretende ser un punto de partida para que las organizaciones establezcan un sistema de gestión del Ciber riesgo dado que la sociedad actual es cada vez más dependiente del Ciberespacio, por lo que se hace necesario identificar realmente lo que representa esta dimensión y qué riesgos involucra.

El Ciber riesgo debe entenderse como la probabilidad de que una amenaza proveniente del Ciberespacio se materialice con consecuencias sobre los ciberactivos que posee una organización, estos ciberactivos pueden clasificarse en personales y empresariales.

Queda claro que el Ciber riesgo es hoy en día uno de los principales riesgos a los que se enfrentan las organizaciones, el Foro Económico Mundial lo deja claro ubicándolo como uno de los 10 principales riesgos en la actualidad e incluso se llega a considerar como un riesgo de naturaleza catastrófica.

No se ha logrado determinar aún la naturaleza catastrófica del ciber riesgo. De acuerdo a los análisis realizados a la frecuencia y severidad de la base de datos estudiada el Ciber riesgo podría modelarse como un riesgo de la ramo no vida tradicional, sin embargo podría pensarse que en la medida que la sociedad sea más ciber dependiente el carácter catastrófico de este tipo de riesgo cobrará más relevancia.

La Norma ISO 31000:2009 proporciona los estándares necesarios para la creación de un sistema de gestión del Riesgo, su adaptación a cualquier tipo de riesgo

complementado con otras normas tales como la ISO 27005:2011, permite crear un marco de trabajo para la gestión del Ciber riesgo dentro de una organización.

A pesar de que resulta difícil acceder a información cuantitativa sobre el Ciber riesgo, las herramientas tradicionales de cálculo actuarial parecen adecuarse muy bien al análisis de este tipo de riesgo.

Se propone la profundización en trabajos posteriores sobre la relevancia del uso de las redes neuronales para el análisis del ciber riesgo con bases de datos que puedan tener más información, dado que la aplicación de las redes en este trabajo ha demostrado muy poco grado de asertividad.

El marco de trabajo del Ciber riesgo debe seguirse desarrollando para brindar una mejor ciberseguridad garantizando que todas las partes interesadas en el uso del Ciberespacio en su vida cotidiana.

Índice de gráficos.

Índice de tablas.

Índice de figuras.

Índice de ecuaciones.

Bibliografía

Actuarial Standards Board. (2012). *Risk Evaluation in Enterprise Risk Management.*

Australian/New Zealand Standard. (s.f.). *AS/NZS 4360:2004 risk management.* Sydney y Wellington: Standards Australia International Ltd y Standards New Zealand.

Cambridge University Press. (2017). *Cambridge Dictionary*. Obtenido de http://dictionary.cambridge.org/es/

Dodge, M., & Kitchin, R. (2001). *Atlas of cyberspace.* Edinburgh: Pearson Education.

Dykstra, J. (2016). *Essential Cybersecurity Science.* Sebastopol: O'Reilly Media.

Editorial Wall Street Journal. (5 de February de 2013). Barbarians at the Digital Gate. *Wall Street Journal,*.

Eling, M., & Wirfs, J. (2015). *Modelling and Management of Cyber Risk.*

European Network and Information Security Agency. (2012). *and barriers of the cyber.*

Fischer, E. (2009). *Creating a national framework for cybersecurity: An analysis of issues and options.* New York: Nova Science Publishers.

Francis , L. (2001). Neural Networks Demystified. *Casualty Actuarial Society Forum*, 253-320.

Guía ISO/CEI 73. (2009). *Gestión de riesgos – Terminología – Líneas directrices para el uso en las normas.*

Henry, S. (24 de October de 2016). CYBER TERRORISTS AND RANSOMWARE . (BRINK, Entrevistador)

Holton, G. A. (2004). Defining risk. *Financial Analysts Journal*, 19-25.

Instituto Nacional de Ciberseguridad. (2017). *Glosario de términos de ciberseguridad.*

ISO/IEC 27005:2011. (2011). *Information technology -- Security techniques -- Information security risk management.* Ginebra.

ISO/IEC 27032. (2012). *Information technology - Security techniques - Guidelines for cybersecurity.*

Kendrick, R. (2010). *Cyber Risks for Business Professionals.* United Kingdom: IT Governance Publishing.

Lachapelle, E., & Halili, R. (2015). *Whitepaper ISO/IEC 27005.* Carstedt Inc.

Lipovsky , R., & Cherepanov, A. (4 de January de 2016). *welivesecurity*. Obtenido de https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/

Lloyd's. (2015). *The insurance implications of a cyber attack on the US power grid.* Londres: Centre for Risk Studies University of Cambridge.

Luhmann, N. (1993). *Risk: A Sociological Theory.* Berlín: Walter de Gruyter.

Mapfre. (05 de Mayo de 2017). *www.mapfre.es*. Obtenido de https://www.mapfre.es/seguros/empresas/seguros-de-responsabilidad-civil/seguro-ciberriesgos/ciber-riesgos/

MathWorks. (21 de Mayo de 2017). *MarhWorks*. Obtenido de https://es.mathworks.com/help/stats/burr-type-xii-distribution.html

Maxwell, L. (2017). Cybersecurity and the Insurance Market. *Joint Risk Management Section*, 9-11.

Net Diligence. (2016). *Cyber Claims Study.*

Oliveira, J., & Jiménez Cano, R. (15 de Mayo de 2017). El ataque de 'ransomware' se extiende a escala global. *EL PAIS*.

Orcutt , M. (6 de Abril de 2017). *MIT Technology Review*. Obtenido de https://www.technologyreview.com/s/603937/insurers-scramble-to-put-a-price-on-a-cyber-catastrophe/

Ploug, T. (2009). *Ethics in Cyberspace.* Heidelberg: Springer.

Posner, R. (2004). *Catastrophe: Risk and Response.* New York: Oxford University Press.

Privacy Right Clearinghouse. (08 de 05 de 2017). Obtenido de www.privacyrights.org

PwC. (2015). *Insurance 2020 & beyond: Reaping the dividends of cyber resilience.* London.

Real Academia de la Lengua Española. (2014). *Diccionario de la lengua española (22a ed)*. Obtenido de https://goo.gl/mSCf3c

Refsdal, A., Solhaug, B., & Stølen, K. (2015). *Cyber_Risk Management.* Heidelberg: Springer.

Rodriguez, R. (1977). A guide to the Burr type XII distributions. *Biometrika*, 129-134.

Solomon, M. (2016). Cyber Risk is Opportunity. *Risk Management Society of actuaries*, 27-30.

Strate, L. (2009). The varieties of cyberspace: Problems in definition and delimitation. *Western Journal of Communication*, 382-412.

Ulsch, N. (2014). *Cyber Threat! How to Manage the Growing Risk of Cyber Attacks.* New Jersey: John Wiley & Sons, Inc.

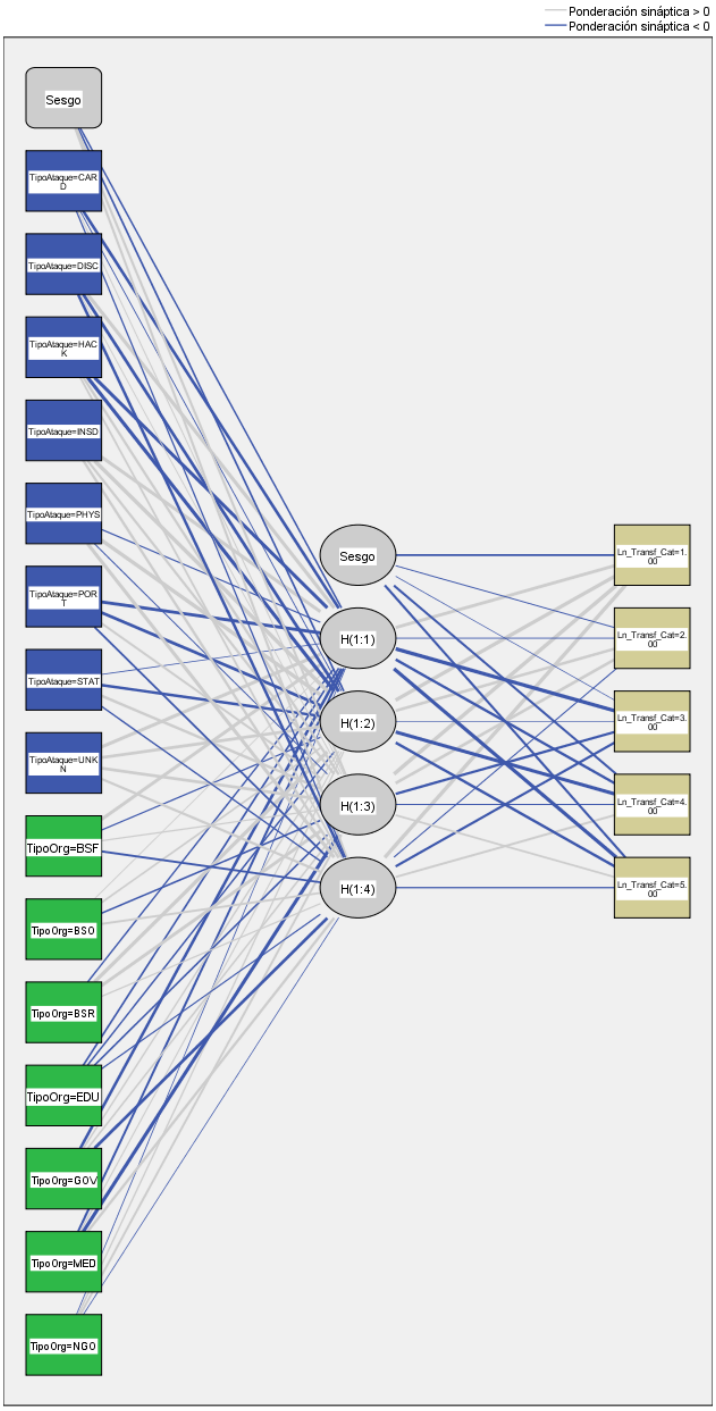
Warner, B., & Misra, M. (1996). Understanding Neural Networks as Statistical Tools. *American Statistician*, 282-293.

World Economic Forum. (2017). *The Global Risks Report.* Ginebra.

World Energy Council. (2016). *Managing Cyber Risks.*

Anexos

Anexo 1. Red neuronal que explica la Severidad por el tipo de ataque y el tipo de organización.

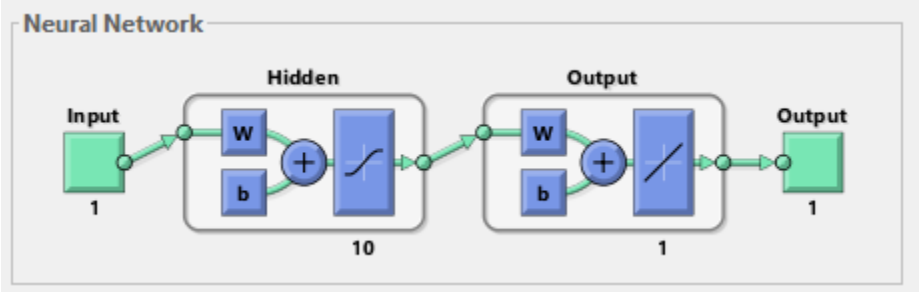


Función de activación de capa oculta: Tangente hiperbólica

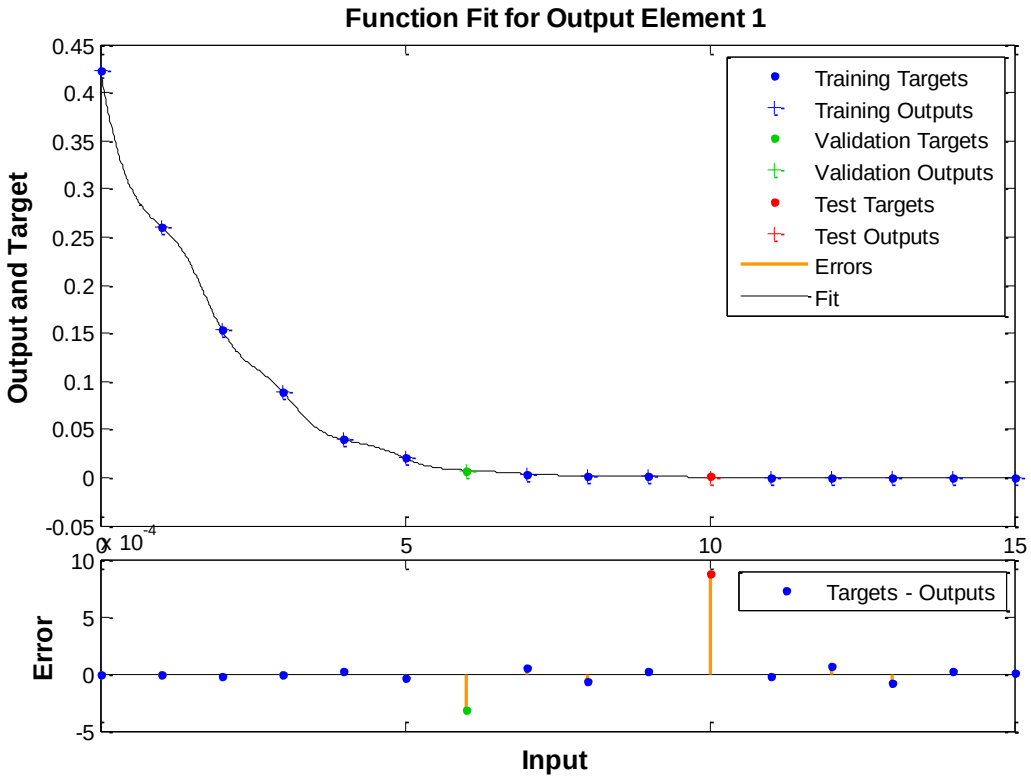
Función de activación de capa de resultado: Softmax

Anexo 2. Ajuste de la distribución de la frecuencia de la muestra con redes neuronales.

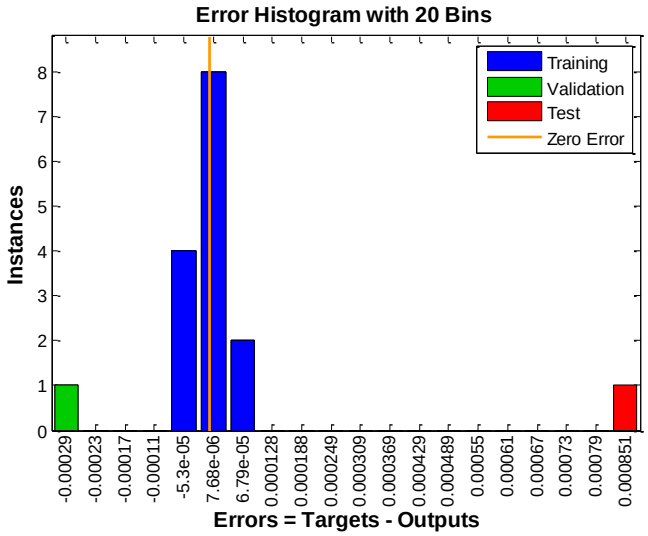
Primer ensayo. Se ejecuta una red con 10 capas ocultas.



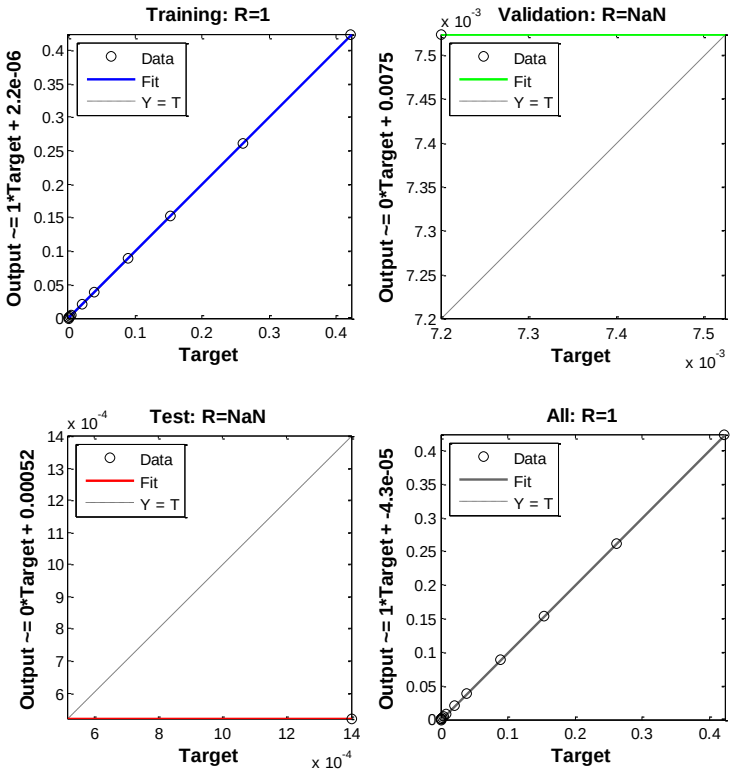
Estos son los valores obtenidos después de varios entrenamientos realizados a la red con 10 nodos ocultos.



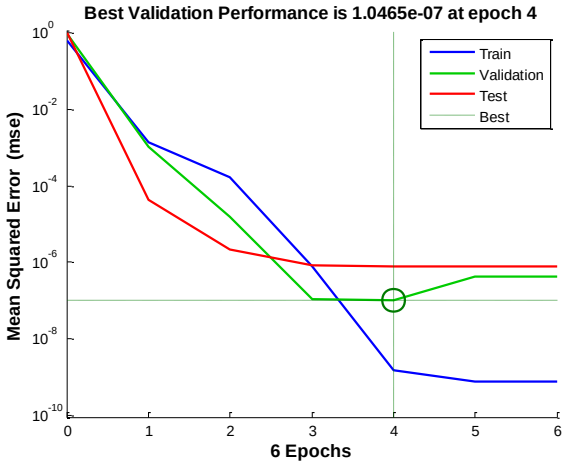
Histograma de los errores.



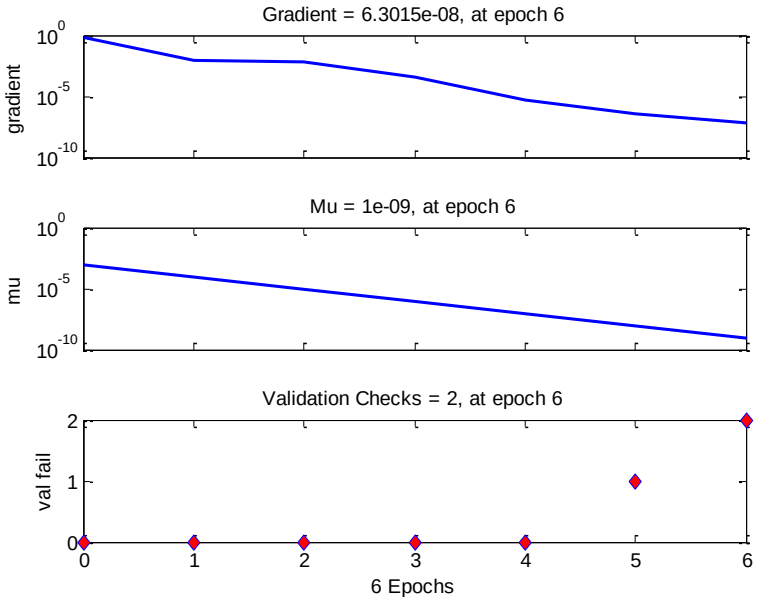
Plot de la regresión.



Performance



Estado del training

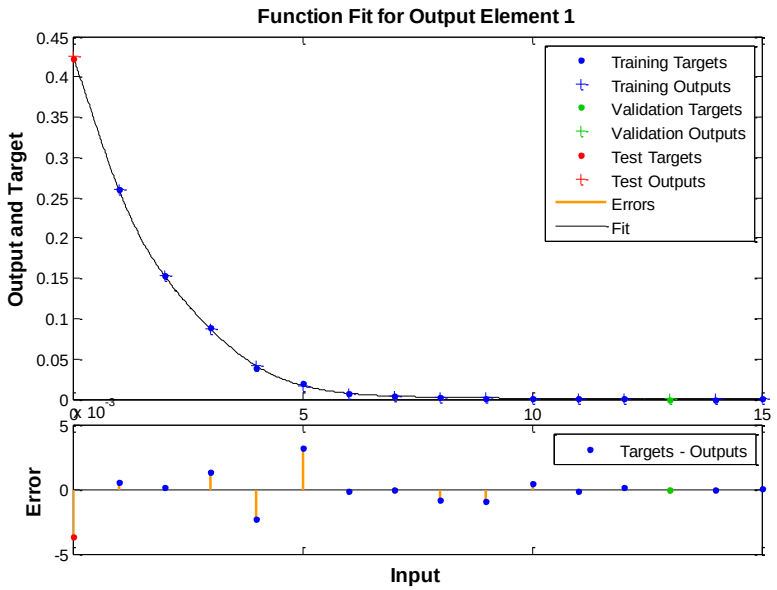


Diferencia entre los valores reales y los valores estimados por la red neuronal.

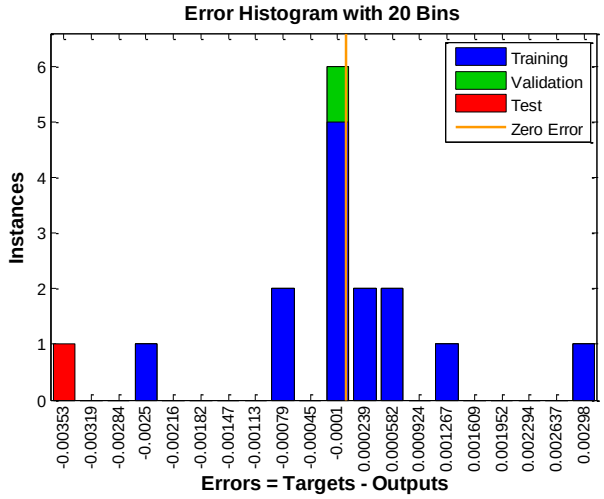
Red Neuronal 10 Nodos

Categoría	*NN Estimate*	*Diferencia*
0	0.4222	0.0000
1	0.2610	0.0000
2	0.1529	0.0000
3	0.0887	0.0000
4	0.0392	0.0000
5	0.0203	-0.0001
6	0.0075	-0.0003
7	0.0037	0.0001
8	0.0019	-0.0001
9	0.0009	0.0000
10	0.0005	0.0008
11	0.0002	0.0000
12	0.0001	0.0001
13	0.0001	-0.0001
14	-1.87E-05	0.0000
15	0.0002	0.0000

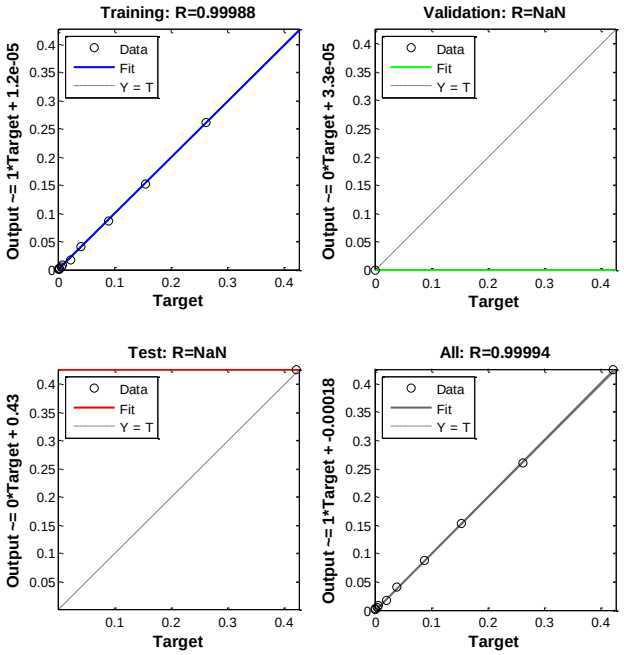
Con 4 nodos ocultos predice mucho mejor.



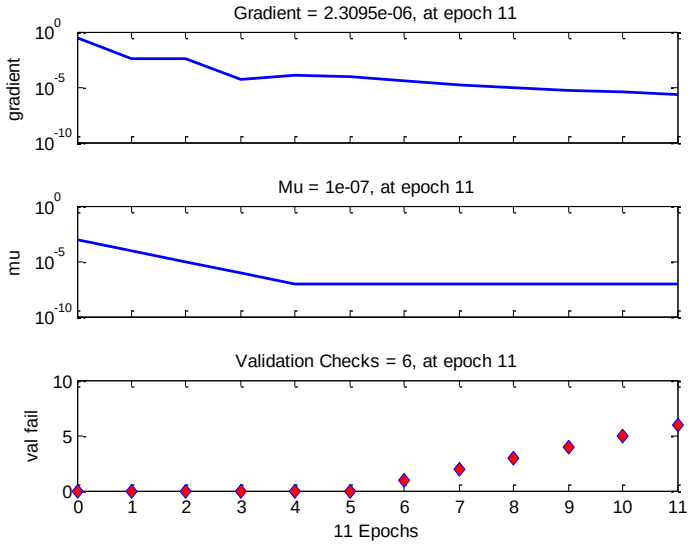
Histograma de los errores.



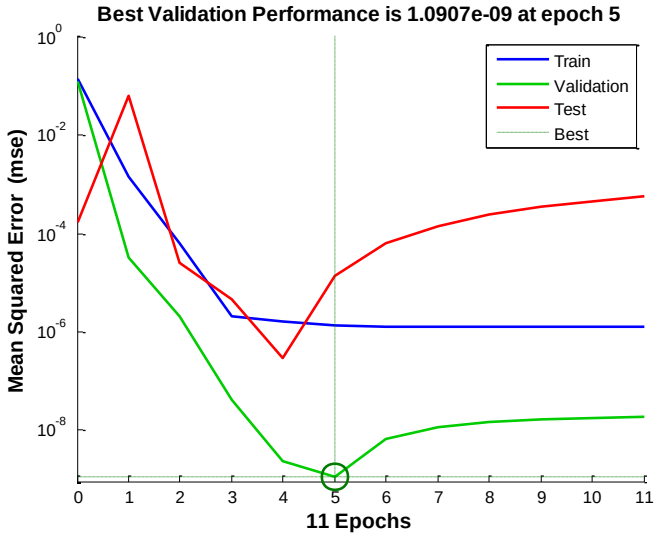
Regresión.



Training State



Performance.



Error cuadrático entre los valores predichos por la red neuronal de 4 nodos y los valores originales.

Red Neuronal 4 Nodos Ocultos

Categoría	*NN Estimate*	*Error (MSE)*
0	0.42589961	-0.004
1	0.26046347	0.001
2	0.15270483	0.000
3	0.08735912	0.001
4	0.04153062	-0.002
5	0.01714922	0.003
6	0.00734458	0.000
7	0.00388512	0.000
8	0.00262344	-0.001
9	0.00183986	-0.001
10	0.00093761	0.000
11	0.00030312	0.000
12	0.00008052	0.000
13	0.00003303	0.000
14	0.00005963	0.000
15	0.00017892	0.000
		-0.2%