IMPACTO ECONÓMICO DE LA COLABORACIÓN Y SEGURIDAD DE DATOS EN LAS ORGANIZACIONES

PRESENTADO POR:

JEIMMY NATHALIA LAVERDE ROMERO

PROGRAMA:

ECONOMÍA

CODIGO:
2101983

PRESENTADO A:

MANUEL ENRIQUE WAGNER

DIPLOMADO BUSSINES INTELLIGENCE, ANALISIS DE DATOS CON EXCEL Y SAP ANALYTICS CLOUD

BOGOTÁ. D.C.

2022

INTRODUCCIÓN

Hoy por hoy el tema de tratamiento de datos personales ha tomado relevancia en el mundo empresarial, el uso de estos es usado por múltiples compañías, empresas y organizaciones que buscan un posicionamiento en el mercado digital, como alternativa a los nuevos dinamismos imperantes de mercado.

Desde la creación de las redes de comunicación masiva a larga distancia, la que se remonta a la guerra fría, la cual es reconocida como la antesala a lo que más adelante inició la Red de Internet, con la transferencia de virtual de datos conocida como ARPANET, esta facilito la información entre los altos mandos y aliados de esta guerra bélica, este primer sistema de información creo el escenario conocido hoy por hoy como ciberespacio y con ello los diferentes riegos y amenazas al mismo.

En la actualidad los individuos hacen uso de la tecnología como una herramienta de uso diario que involucran en sus actividades diarias, en las cuales depositan información personal y general de suma importancia que queda en el internet. Esta información es útil para las empresas y organizaciones que desean estudiar más a fondo el comportamiento de los consumidores y así establecer estrategias que permitan lograr un mayor alcance y posición en el mercado, sin embargo, el efecto de recibir esta información a través de internet o canales electrónicos no es del todo confiable, pues son redes que guardan mucha información y no existe la seguridad por completo.

Es por ello por lo que las grandes compañías tecnológicas se están acomodando a la necesidad del mundo creando paquetes de software que protejan los ciberataques y delitos en sus equipos, así mismo aumentan las empresas que ofrecen pólizas para la protección digital, esto

representa una inversión para las organizaciones pues a pesar de que implican un costo, las perdidas serían aún mayores sin el uso de estas herramientas que permiten asegurar los datos.

DESARROLLO

La utilización masiva del internet como mecanismo de comunicación cotidiano, entre los individuos del mundo, fue uno de los factores mas relevantes de la llamada globalización de medios, esta ha sido de gran provecho en el ámbito empresarial, ya que se ha logrado en las últimas décadas derribar fronteras de comercio y el acercamiento entre mercados se volvió optima.

La utilidad de esta herramienta, aunque ha mostrado eficiencia en el acercamiento hacia los clientes y una oportunidad única de correspondencia hacia los servicios que se brindan en cada empresa, esta presenta vulnerabilidad en cuanto a los sistemas informáticos que son implementados por las industrias, las entradas y salidas de información por medio de códigos ASCII, presentan un sistema de seguridad estándar en cuanto a resistir ataques informáticos o virus como gusanos, bombas lógicas y troyanos, pero en medio de los avances que se dan a diario en cuanto a seguridad en la red, se siguen presentando robo de información y ciberataques en el mundo empresarial.

La implementación global de dispositivos móviles, laptops y Softwares de Gestión tanto empresarial como de inteligencia de negocios, han generado cambios significativos en las transformaciones de mercados y en el ámbito social, que hoy son evidentes en el diario vivir, estos sistemas son objetivo de individuos que pretende afectar de manera negativa a sus propietarios.

Desde este contexto, se puede evidenciar un proceso de reconocimiento en cuanto a la ruta que toman los datos que los usuarios por medio de los sistemas de transferencia consentida, en cuanto a la recolección de datos, (En este punto es importante resaltar que, aunque los usuarios de los diferentes sistemas informáticos usen herramientas de revocatoria de los mismos, estos no son devolutorios y las compañías los usan para estimar posibles compradores de productos o servicios a futuro), las compañías y empresas que recolectan información de los clientes y usuarios implementan estrategias para que la calidad de los datos que son recolectados sean adecuados y actualizados para logran lo fines para lo cual fueron creados, en este ámbito la categorización de los mismos como número de identificación, números de cuenta bancaria, acceso a tarjeta de créditos, son categorías que empresas proporcionan una mayor protección, debido a las complicaciones que acarrea el robo de la misma, la cual en la gran mayoría de los casos da pie al fraude financiero e informático.

La utilización de los datos personales y patrones de conducta de los usuarios son determinados en el marco del desarrollo tecnológico y es puesto en marcha con la implementación de estrategias de marketing en este (marketing digital), se puede identificar que es un proceso de mejora e innovación continua que toma mayor relevancia con el paso del tiempo, en los últimos años se ha convertido en una vía de comunicación, distribución y comercialización asertiva en la en todas las industrias del mundo, ya que brinda la congruencia de integrar un mercado tradicional con estrategia de globalización en sus productos, las experiencias que brinda estos canales de ventas, visibiliza que las tomas de decisiones de los consumidores son más asertivas y la satisfacción frente a los productos, son más óptimas.

Las estrategias de protección de datos personales e información privilegiada, que las empresas manejan es sus bases de datos, es lo que se conoce como ciberseguridad, la cual es una

forma de protección de infraestructura informática, que se implementa sobre un software y hardware, su finalidad descansa en contrarrestar amenazas generadas en la red, y de este modo encontrar herramientas que a su vez la contrarresten. No se puede limitar a la ciberseguridad a un simple conjunto de mecanismos de programación informática, los complementos de la ciberseguridad también pueden producirse por medio de políticas nacionales, que marque ciertos requerimientos que propendan a disminuir el riesgo de perdida o hurto de la información. (Cano, 2016)

La problemática de la ciberseguridad radica as específicamente en la ciberguerra y el ciberterrorismo, es por ello que la ciberseguridad es considerada como un asunto global, ya que ha involucrado a lo largo de la historia contiendas ente países, ataques entre grandes industrias y robo de información entre grupo de fuerzas militares. Cuando hablamos de violaciones a la ciberseguridad entre países podemos traer a colación: el robo de información a empresas petroleras, la injerencia de ciberataques en elecciones presidenciales, daño a los sistemas de centrales eléctricas entre otros. (Ospina & Sanabria, 2020).

Así como sucede en los ámbitos gubernamentales, estos dinamismos también suceden en las pequeñas medianas y grandes empresas, compañías y organizaciones alrededor del mundo que cada día en su intención por expandir el mercado a través de canales electrónicos está expuesto a daños informáticos o de seguridad en sus nubes, afectando al público y a su misma organización.

En el ámbito empresarial podemos denotar, que los ataques a la ciberseguridad toman un tono diferente, en este caso el robo de información no se hace con el fin de crear estrategias de ataque o destrucción , más bien, se usan para la divulgación de información privilegiada que puede influir en el comportamiento del mercado, que la competencia tiene amparado, esta

competencia desleal de una empresa a otra de la misma industria, ha generado la carrera de patentes y registros con los cuales los ciberataques han disminuido.

Las industrias del mundo cada día se automatizan aun mas en cuanto a sus sistemas de producción y eficiencia en el mercado, dando paso a una nueva generación, en la cual los sistemas digitales y la implementación de plataformas como E – comerce han marcado la pauta.

Los mecanismos en los que se enfoca la ciberseguridad en cuanto a mitigar los riesgos informáticos a los que están expuestos son el mejoramiento de la infraestructura computacional de sus dispositivos o equipos, protección a la información circulante, implementación de normas como la ISO 27001, esto garantiza de manera efectiva la protección a la información relevante de las empresas en todos sus ámbitos de comercio.

El entorno empresarial que actualmente rige a nivel global es altamente competitivo y dependiente de las ventajas competitivas que entrega la tecnología y la globalización, (eficiencia en mano de obra, costos, vetas etc), la implementación de seguridad en la adquisición de productos y servicios en medios digitales, se ha usado como estrategia en la competitividad y las ventajas comparativas de las industrias a nivel local, logrando posicionamientos de empresas y marcas en tiempo récord y ajustándose gradualmente a los avances tecnológicos del contexto, los cuales también son cambiantes en su entorno.

Aunque como ya se ha mencionado, una preocupación en común son las ciberamenazas y los ciberataques, también es cierto que los mecanismos de contraataque son cada vez más sofisticados, amenazas como gusanos, Phishing y Pharming, en la actualidad no presentan un peligro latente como si lo eran hace una década. (OEA, 2020)

El tema de ciberseguridad, aunque viene desde décadas atrás, en países emergentes y de tercer mundo es algo relativamente nuevo, a nivel local es necesario destacar que las pequeñas y medianas empresas conocida como MiPyme, son un blanco fácil de ataque cibernéticos con el Phishing, ya que, al no poseer sistemas de protección de datos sofisticados, el robo de información se convierte en algo muy recurrente. La poca relevancia que los administradores de estas empresas le dan a la ciberseguridad, ha ocasionado que muchas industrias pierdan competitividad a nivel interior de sus países, y en ocasiones las pérdidas económicas sean muy considerables.

La automatización de las empresas en países de tercer mundo ha sido un atractivo inmenso a los hackers y creadores de malware que ven en ellas escenarios propicios de prueba a sus avances en el ciberespacio, es por ello que nace la necesidad de la colaboración empresarial, debido a los altos costos de adquisición de sistemas informáticos de protección.

Es por ello que las grandes compañías tecnológicas se están acomodando a la necesidad del mundo creando paquetes de software que protejan los ciberataques y delitos en sus equipos, así mismo aumentan las empresas que ofrecen pólizas para la protección digital, esto representa una inversión para las organizaciones pues a pesar de que implican un costo, las perdidas serían aún mayores sin el uso de estas herramientas que permiten asegurar los datos.

Las pocas medidas de seguridad de la información, la escasa capacitación del personal de las empresas y las deficientes políticas de seguridad informática en las Mipymes han tenido un impacto negativo en el desarrollo en sus actividades empresariales en regiones como América latina, donde este tipo de empresas representa mas de un 70% de la industria Total.

La implementación de la norma ISO 27001, ha sido considerada como una de las herramientas mas eficiente en cuanto a la implantación de estrategias de combaten contra los ciberataques, la creación de estándares, métodos, protocolos y reglas para logra minimizar los riegos cibernéticos, la aplicación de restricciones y previa autorizaciones de los propietarios de los datos que entran por medio de tránsito de red o por creación de usuarios por medio de remotos como VPNs, ha reducido el secuestro o envenenamiento del DNS. Las políticas de privacidad y seguridad de la información deben presentar una codificación única que impida su hurto y su malversación en cuanto a su uso.

Como se ha indicado, algunas de las técnicas usadas son los ataques por suplantación que involucra una o varias víctimas y el atacante. Algunas de las técnicas usadas son el ARP spoofing, DNS spoofing, IP spoofing y ataque de estación base falsa. Estos ataques permiten, a través de la interceptación de las comunicaciones, obtener la información suficiente y necesaria para suplantar, lo que conlleva vulnerar el sistema (Álvarez & Montoya, 2020).

Las amenazas a la seguridad informática aparecen principalmente por las siguientes razones

a) Usuarios Con Permisos innecesario
b) Programas Maliciosos o Malware
c) Errores De Programación o programación débil.
d) Acceso De Intrusos
e) Generación De Siniestros, Robos E Incendios
f) Acceso De Personal Técnico Interno no autorizado
g) Catástrofes Naturales
h) Ingeniería Social (Errores Humanos, Falta De Precaución Al Compartir Contraseñas, Claves, Códigos O Por Descarga De Archivos.

El análisis de riesgo informático es hoy por hoy, un mecanismo que permite la prevención de robo informático, este consiste en hacer una identificación de los activos y propiedades de la empresa incluyendo sistemas de software, hardware, vías de comunicación, documentación digital, entre otros. (OpenNAC Enterprise, 2019).

La gestión de riesgos es un proceso interactivo que permite la obtención de posibles impactos sobre diferentes activos de información, para lo cual un riesgo es la posibilidad que una amenaza explote una vulnerabilidad en un activo determinado y genere un impacto negativo al sistema. (Álvarez & Montoya, 2020).

La determinación de riesgos y amenazas enmarca uno de los pasos más importante de esta herramienta ya que las amenazas pueden ser de diferente naturaleza e índole, estas pueden ser externas, por factores humanos, por mal proceso de entrada y procesamiento de datos, la identificación de vulnerabilidades es el siguiente paso, el cual centra su atención en la actualización y debido licenciamiento de la infraestructura informática que posee la empresa.

Los métodos de prevención y control, en este punto toman relevancia, ya que, con la identificación de factores amenazantes y vulnerables, el objetivo se centra en la mitigación de riesgos de malware, los sistemas de seguridad en la nube automatizados y planes de Disaster Recovery hoy por hoy es el mecanismo más usado como método de control. (Rodríguez, s. f.).

No obstante, las empresas siempre están en busca de mecanismos cada vez mas eficientes, es por ello por lo que la simulación de ciberataques y las evaluaciones de desempeño de los sistemas de infraestructura información propios, se ha posicionado como un determinante de debilidades y por este medio, preparar posibles estrategias en el momento de recibir una amenaza informática.

La preparación de escenarios hipotéticos de ataques a las bases de información de las empresas se debe empezar a implementar a nivel de la industria, si bien cada empresa o compañía tiene un recelo en proteger su información de la competencia, es una realidad que la colaboración empresarial en cuento a ampliar la extensión de protección es algo que debe tomar relevancia.

Por ello, en los últimos años algunas empresas principalmente del estado buscan crear un tipo de uso compartido de los datos de tal manera que la información que se reciba pueda ser útil para varias organizaciones haciendo que los usuarios no tengan que regar información en varias plataformas sino en una sola que los pueda recopilar e intercambiar con otras con una misma finalidad, lo que lleva consigo más inversión en la seguridad cibernética de las empresas que participen de esta iniciativa y a su vez ayuda a las pequeñas empresas que tienen pocos recursos para recopilar información.

Sin embargo, se encuentra la realidad de hallar empresas que no están implementado ningún tipo de seguridad y protección en sus procesos, exponiendo de forma significativa no solo su producción, si no las seguridad personal de sus clientes, se puede identificar que la principal razón por lo que ello ocurre, subyace en, la resistencia al cambio que pueden conllevar a un cambio radical en los procesos de la empresa, deben capacitar a cada una de las personas que hacen parte de esta y todo este rediseño se logran en parte a la utilización de recursos económicos, lo que lo hace aún más complicado. Las estrategias de detección temprana deben ser una prioridad en las empresas que no cuentan con sistemas automatizados de infraestructura informática.

Los avances a pasos agigantados de los creadores de malware asombran cada vez mas a los creadores de sistemas de infraestructura informática de protección, ya que su evolución en

rápida y es por ello que la implementación de intercambio de información, distribución e industrialización de sistemas más complejos de protección es hoy mas urgente que nunca, la colaboración entre lo publico y lo privado debe ser una realidad, para mitigar las perdidas por los ataques dañinos causados por programa maliciosos.

METODOLOGÍA

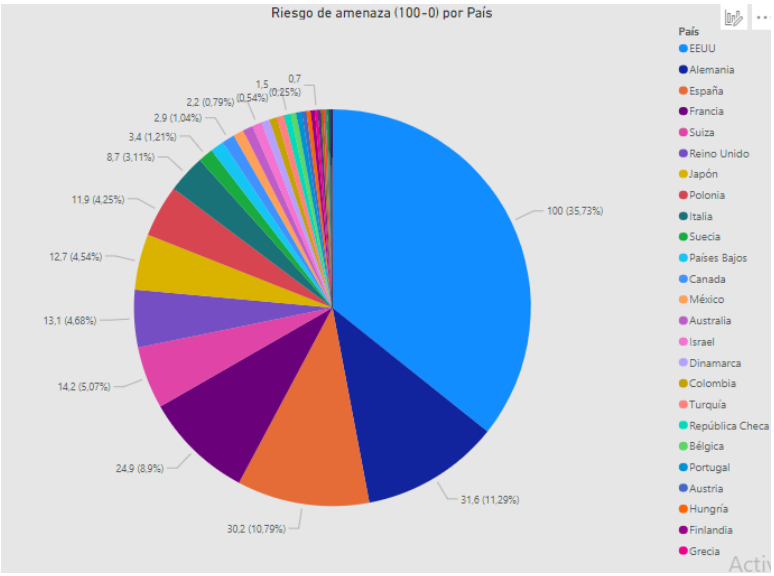
Con el fin de poder dar un análisis más profundo de los sistemas de protección en las organizaciones del mundo y el acceso a la información para la integración y colaboración de datos empresariales, se recolectaron bases de datos de los Informes de defensa digital de Microsoft en el año 2020, que permitieran conocer el alcance a la data y su seguridad. Para la recolección de esta información se tuvo en cuenta principalmente el acceso a internet de los países, el riesgo informático, y las estadísticas de colaboración empresarial en el mundo. Con la recolección de estos datos se realizó primero un arreglo de las bases de tal forma que solo quedara la información más relevante y útil para el análisis y posteriormente se cargaron las bases a Power BI para poder segmentar y relacionar los datos de la mejor manera. A través de esta información se plantea conocer el impacto económico que la seguridad y colaboración analítica tiene en el mundo.

ANALISIS DE DATOS

De acuerdo con la información recolectada en las bases de datos para el análisis se segmentó de acuerdo con el país y a la relación con cada variable de tal forma que fuera más visible identificar las naciones que tienen mayor relación en cuanto a ciberseguridad. Con información suministrada por el Informe de defensa digital de Microsoft para el año 2020 en la figura 1, se relaciona el riesgo de amenaza de ciberseguridad por país en un rango de 100 a 0,

siendo 100 el país que registra un mayor riesgo de amenaza y 0 quienes representan un menor peligro, estos rangos son utilizados para detectar los lugares que son atacados con mayor frecuencia.

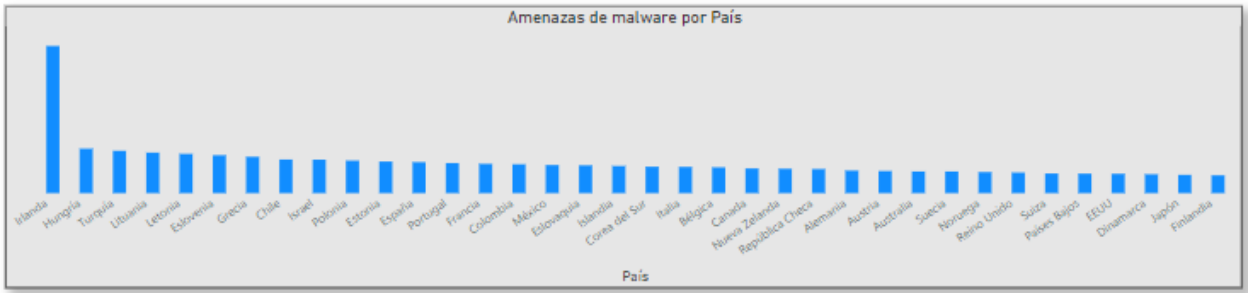
Figura 1. Riesgo de amenaza (100 – 0) por País.



Fuente: Elaboración propia con datos tomados del Informe de defensa digital de Microsoft (2020)

Según la información segmentada en la figura1, se puede apreciar que en un rango de 100 a 0 el país que muestra un mayor riesgo por amenazas cibernéticas es Estados Unidos, con una cifra del 35,73% , seguido por Alemania con un 31,6 % , dentro del mismo se puede inferir que después del país norteamericano son los países de Europa los que presentan un mayor impacto en el riesgo de su seguridad en la información, esto se debe a que tienen mayor información en sus nubes y por tanto se encuentran más expuestos a los ataques. Por el contrario, los países de Latinoamérica como México o Colombia se encuentran un rango inferior ya que aún son países que no poseen una gran interacción en la nube de datos y por tanto son menos propensos a recibir ataques.

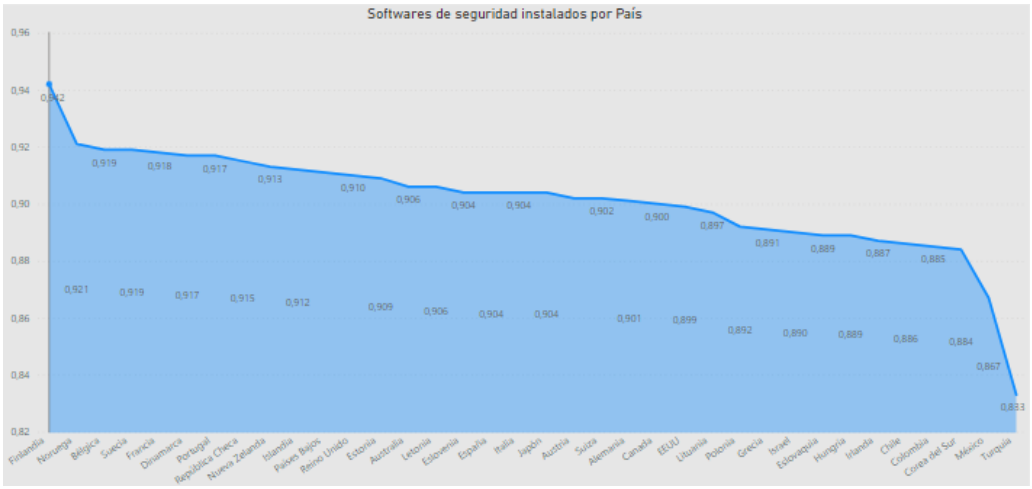
Figura 2. Amenazas de Malware por país.



Fuente: Elaboración propia con datos tomados del Informes de defensa digital de Microsoft (2020)

De acuerdo con la segmentación de malware por país en la figura 2, se puede resaltar que Irlanda representa en gran proporción la mayor amenaza por malware con un 96%, este dato es bastante significativo ya que Irlanda ha sido el país que en los últimos años ha sufrido más ataques cibernéticos en el mundo, hasta el punto de tener que suspender los sistemas de información para poder protegerse de robos y de acceso indebido a la información especialmente en su sistema de salud. Por otro lado, el país que menos amenazas por malware posee es Finlandia con un 11,60%, una cifra muy positiva ya que se encuentra por debajo de países como Estados Unidos que posee el mayor rango de riesgo (Figura 1).

Figura 3. Software de seguridad instalados por país



Fuente: Elaboración propia con datos tomados del Informes de defensa digital de Microsoft (2020)

En esta figura, se tomó el porcentaje de software de seguridad que fueron instalados en cada país en, en primer lugar, se encuentra Finlandia con un 94,20%, este dato concuerda con la información de la figura 2, pues es el país que presenta una menor amenaza de malware, lo cual confirma que un sistema fuerte de seguridad reduce el riesgo de caer en un ataque cibernético. Entre las cifras más preocupantes se encuentra Turquía con un 83,30% y que de acuerdo con la figura 2, es el tercer país que tiene mayores amenazas de malware. Otro dato interesante es Estados Unidos el cual tiene una cifra del 89,90% sin embargo es de los lugares que más ataques cibernéticos tiene al año.

CONCLUSIONES

La colaboración de datos en las organizaciones es una herramienta que día a día puede ayudar a mejorar la productividad de las empresas entre sí y a disminuir los gastos en la recolección de información. Con la nueva ola de tecnología que se está viviendo en el mundo después de la pandemia y con la necesidad de avanzar en los modelos de producción y de consumo que se desarrollan en la actualidad a través de internet, es importante que la globalización vaya más allá de el acceso de los individuos a empresas de todo el mundo, sino también el acceso de empresas a la información de que otras empresas hayan recolectado y se cree canales de cooperación en big data. Sin embargo, este mecanismo de cooperación a pesar de que ayuda principalmente a las pequeñas empresas y al fortalecimiento de otras grandes requiere de una responsabilidad y de un uso de la información adecuado.

A pesar de que las empresas puedan almacenar toda su información en una nube y que esta a su vez pueda ser compartida con otras organizaciones para posicionarse en los mercados, el

acceso a la información cada vez debe ser más riguroso y más protegido pues al ser un espacio en el cual se suministra datos todo el tiempo es propensa a sufrir de ataques cibernéticos que conlleven a robos, a perdidas de datos, a daños en las bases y otros problemas que terminan afectando no solo a las grandes industrias sino a los individuos en general. Cuando se habla de tener un sistema de seguridad fuerte, se habla de la inversión de software, el mantenimiento y refresco de programas que sostienen los datos y el uso que se le da a la nube en la cual se almacenan todos estos procesos.

Como se pudo evidenciar en el análisis de los datos puntualmente en el caso de Finlandia la instalación de sistemas de software de seguridad que protejan la nube garantiza una menor probabilidad de sufrir ataques y perdidas irreparables que afecten el buen funcionamiento del almacenamiento de datos, por el contario como fue el caso de Turquía el no asegurar un buen sistema de información generará un mayor ataque de seguridad.

Finalmente el poseer una fuente de información confiable y protegida asegura que los datos no se alteren y se puede dar un uso adecuado de ellos, de igual forma el poder compartir la información entre organizaciones ayuda al crecimiento de la economía, genera expansión en las empresas y un acercamiento entre productores y consumidores; sin embargo si no existe un sistema de protección que cuide toda está data, las organizaciones pueden tener pérdidas irreparables tanto económicas como legales, por eso la colaboración de datos entre organizaciones es un proceso de cooperación y de inversión conjunta entre las partes que pueda proveer el cuidado de los datos y el accesos a ellos para otras organizaciones con el fin de generar un mutuo crecimiento.

REFERENCIAS

Álvarez M, & Montoya H. (2020). *Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos.* Ingeniería y Desarrollo, 38(2), 279-297. https://doi.org/10.14482/inde.38.2.006.31

Cano, J. (2016). *Ciberseguridad y ciberdefensa: Dos tendencias emergentes en un contexto global.* Acis org. https://acis.org.co/archivos/Revista/119/Editorial.pdf

OEA. (2020). *Protección de Datos Personales*. Glosario Departamento de Derecho Internacional (DDI). https://www.oas.org/es/sla/ddi/proteccion_datos_personales_glosario.asp

Ospina M. & Sanabria P. (2020). *Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia*. Revista Criminalidad, 62(2), 199-217. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199&lng=en&tlng=es.

OpenNAC Enterprise. (2019). La identificación de los activos como base de la Ciberseguridad Industrial. Open cloud factory. https://opencloudfactory.com/identificacion-activos-ciberseguridad-industrial/

Rodríguez, P. (s. f.). *Análisis de riesgos informáticos y ciberseguridad*. https://www.ambit-bst.com/blog/an%C3%A1lisis-de-riesgos-inform%C3%A1ticos-y-ciberseguridad

Informe de defensa digital de Microsoft (2020). https://www.microsoft.com/eses/security/business/security-intelligence-report