La Importancia de la Inteligencia Artificial en la Seguridad Cibernética

Yamil Rosario Martinez
Ciencias de Computadoras, Manejo y Seguridad de la Tecnología de la Informática
Dr. Nelliud D. Torres
Departamento de Ingeniería y Ciencias de Computadoras
Universidad Politécnica de Puerto Rico

Resumen *— El mundo se está digitalizando a un ritmo sin precedente. Los sistemas de información y la tecnología están cambiando o evolucionando muy rápido. Con los adelantos en la tecnología, la velocidad de los procesos y la cantidad de datos que se genera diariamente es casi imposible que los sistemas puedan ser protegidos y monitoreados por seres humanos sin la ayuda de aplicaciones o sistemas inteligentes que faciliten el trabajo. Debido a la gran cantidad de dispositivos electrónicos que hay conectados a la Internet los expertos en seguridad cibernética van a enfrentar muchos retos para poder proteger los sistemas adecuadamente. En el tiempo presente se necesita de todo el apoyo que se pueda conseguir para prevenir y mitigar los ataques cibernéticos y las violaciones de datos. En este documento se va a presentar la importancia de la inteligencia artificial en la seguridad cibernética y los costos que implicaría no aplicar esta tecnología.*

Términos Clave *— Aprendizaje Automático, Criminales Cibernéticos, Inteligencia Artificial, Seguridad Cibernética, Violaciones de Datos.*

INTRODUCCIÓN

Durante los pasados años se ha visto un aumento en la cantidad de ataques cibernéticos que las compañías están recibiendo. Cada vez estos ataques se vuelven más complejos, sofisticados y difíciles de detectar. Algunos de los para este aumento podría ser la gran cantidad de dispositivos que se conectan diariamente a la Internet, ya sean teléfonos inteligentes, computadoras portátiles, computadoras de escritorio, tableta, consolas de juegos o incluso cámaras de seguridad por solo mencionar algunos. Esto ha ocasionado que el tráfico de datos aumente considerablemente, así como la cantidad de vectores de ataque que se pueden identificar.

Muchos de los equipos que se utilizan hoy día para conectarse a la Internet no están protegidos correctamente ya sea porque están mal configurados, no cuentan con los últimos parchos de seguridad o simplemente cuando fueron diseñados la seguridad no era la prioridad del manufacturero. Los ataques cibernéticos generan millones de dólares en ganancias. De acuerdo con un estudio realizado por IBM y el Instituto Ponemon en el año 2019, el costo promedio total de las violaciones de datos ha aumentado un 12% en los últimos 5 años [1]. Las violaciones de datos durante el año 2019 tuvieron un costo total aproximado de $3.92 millones de dólares y el tiempo promedio que se tardaron las compañías en identificar y contener la falla fue de 280 días [2]. Los costos de las violaciones de datos van a seguir aumentado, por eso es necesario establecer mejores medidas de seguridad [2]. La introducción de la inteligencia artificial en los sistemas de seguridad puede ayudar a reducir las amenazas que cada vez van a ser mayores [3].

¿QUÉ ES LA SEGURIDAD CIBERNÉTICA?

La seguridad cibernética es la diciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en los sistemas de información. Se diseñó basada en reglamentos, modelos y estándares para poder proteger las redes, los dispositivos electrónicos, los programas y los datos contra ataques, daños o acceso no autorizado [4]. La seguridad cibernética es importante porque las compañías almacenan datos y generan miles de transacciones es sus sistemas. Una parte importante de esos datos y transacciones puede ser información

confidencial, ya sea propiedad intelectual, datos financieros, información de sus empleados o clientes u otros tipos de datos para los cuales el acceso o la exposición no autorizada podría tener consecuencias negativas. El objetivo final de la seguridad cibernética es poder proteger la economía, la infraestructura crítica y el país de los daños que pudieran ser resultado del uso indebido, accidental o intencional de los sistemas de información.

Desafíos de la Seguridad Cibernética

Para poder establecer un plan de seguridad cibernética efectivo, las organizaciones necesitan coordinar sus esfuerzos en todos los sistemas que utilizan [4]. Algunos de los puntos más importante que tocan la seguridad cibernética son:

- Seguridad de la red
- Seguridad de datos
- Seguridad de aplicaciones
- Gestión de identidad
- Seguridad de la infraestructura
- Bases de datos
- Seguridad de la nube
- Seguridad móvil
- Recuperación de desastres

¿Qué es una Violación de Datos?

Una violación de datos se define como un evento o incidente en el que la información de una persona ya sea su información privada, registro médico, información financiero o información de tarjeta de crédito fue accedida sin autorización [5].

¿Qué es un Récord Comprometido?

Un récord es la información que identifica a una persona. Cuando se habla de un récord comprometido es un récord que ha sido robada. Algunos ejemplos de récords podrían ser la información que se guarda de los clientes en las bases de datos, información sobre tarjetas de crédito o los récords médicos de los pacientes.

INTELIGENCIA ARTIFICIAL

La inteligencia artificial es un término que lleva rondando en el campo de la tecnología desde la década de los 50 cuando Alan Turing propuso la pregunta ¿Puede pensar una maquina? La posibilidad de poder construir aplicaciones y sistemas más inteligentes que los seres humanos ha sido desde el principio el horizonte de la inteligencia artificial [6]. La inteligencia artificial es la combinación de algoritmos con el propósito de crear máquinas que puedan simular la inteligencia humana. La inteligencia artificial tiene muchas aplicaciones posibles. Algunas de las que se utiliza hoy día son en biotecnología, salud, comercio, servicios financieros, redes sociales y seguridad cibernética.

TÉCNICAS DE LA INTELIGENCIA ARTIFICIAL

Se han producido numerosas técnicas útiles en el campo de la inteligencia artificial. Se ha hecho evidente que muchos problemas de defensa cibernética pudieran ser resueltos con éxito solo cuando se utilizan métodos de inteligencia artificial [6]. La inteligencia artificial se puede dividir en diferentes técnicas. Alguna de estas técnicas son la red neuronal, los sistemas expertos, los agentes inteligentes y el aprendizaje automático.

- **Sistemas de red neuronal:** Se distinguen sobre las demás técnicas por su alta velocidad de operación. Son muy utilizados para el aprendizaje de patrones de reconocimiento, la clasificación y selección de respuestas a ataques. Estos sistemas se pueden implementar tanto en *hardware* como *software* [6]. Estos sistemas aprenden sin ninguna ayuda externa y se pueden reprogramar a sí mismos [3].
- **Sistemas expertos:** Es la herramienta de inteligencia artificial más utilizada. Un sistema experto utiliza conocimientos humanos almacenados para resolver problemas que normalmente un experto en la materia podría resolver [6]. Existe una extraordinaria variedad

de sistemas expertos, desde sistemas de diagnóstico poco especializados hasta sistemas híbridos utilizados para resolver problemas complejos [3].

- **Agentes inteligentes:** Son componentes de programas que poseen algunas características de comportamiento inteligente que los hacen especiales [6]. Los agentes inteligentes pueden aprender o utilizar la información que es suministrada para lograr sus objetivos [7]. Estos sistemas se pueden ajustar en tiempo real y aprender cosas nuevas rápidamente a través de la comunicación con el entorno [3].
- **Aprendizaje automático:** Utiliza métodos computacionales para adquirir nuevos conocimientos, nuevas habilidades y formas de organizar los conocimientos existentes [6]. Es una técnica que se utiliza en la inteligencia artificial para crear sistemas que aprenden automáticamente. Permite que los sistemas puedan aprender de los datos, en vez de aprender mediante la programación explicita.

Ventaja de las Técnicas utilizadas en la Inteligencia Artificial

A continuación, se muestra un resumen del uso que se le puede dar en la seguridad cibernética a algunas de las técnicas utilizadas en la inteligencia artificial.

Tabla 1
Técnicas Utilizadas en la Inteligencia Artificial

Técnica	Uso
Agentes Inteligentes	Proactividad, Reactivo, Defensa contra DDoS
Red Neuronal	Sistemas de Detección y Prevención de Intrusos, Alta Velocidad de Operación, Investigaciones Forense, Detección de Calor
Sistemas Expertos	Apoyo a Decisión, Detección de Intruso en la Red, Base de Conocimientos, Motores de Inferencia
Aprendizaje Automático	Aprendizaje Supervisado y No Supervisado, Detección de Malware, Detección de Intrusos

¿PORQUE ES NECESARIA LA IMPLEMENTACIÓN DE LA INTELIGENCIA ARTIFICIAL?

La inteligencia artificial nos ayuda a llegar a una reacción mucho más rápida a las situaciones que ocurren en nuestro entorno cibernético. Las compañías hoy día tienen que ser capaces de manejar y monitorear grandes cantidades de datos en tiempo real, para así poder descubrir y analizar los eventos que ocurren en sus alrededores. El análisis de estos datos les puede ayuda a tener una mejor visión y poder tomar decisiones correctas, ya que cada vez los ataques cibernéticos se van a volver más frecuentas y persistentes [8], [9].

La inteligencia artificial está en todos los lugares. Se está utilizando en cosas tan sencillas como predicciones de compras, reconocimiento de imágenes, reconocimiento de voz con las aplicaciones de Cortana de Microsoft, Siri de Apple y Alexa de Amazon, hasta en áreas más complejas como lo son las redes sociales o los autos autónomos. Con la ayuda de la inteligencia artificial la recopilación de datos es mucho más fácil. Esto es debido a que las capacidades de almacenamiento y eficacia de los sistemas han aumentado y sus costos han bajado, los algoritmos matemáticos que se utilizan han mejorado y los procesos de computación son mucho más rápidos [8].

La realidad es que en tiempo real las enormes cantidades de datos que se transmiten cada segundo son sumamente difíciles de manejar y analizar por seres humanos. Con la ayuda de la inteligencia artificial el análisis de estos datos podría reducirse a milisegundos. Con estos resultandos las empresas podrían fácilmente identificar, reaccionar y recuperarse de amenazas [10], [11]. Orli Gan, jefa de Gestión y Mercadeo de Productos, Prevención de Amenazas en *Check Point Software Technologies, Ltd.* dice que la inteligencia artificial va a producir la próxima revolución industrial de nuestro tiempo. Esto es debido a que el gasto mundial en inteligencia artificial para el año 2019 llego a $35.8 billones de dólares. Un aumento de

44% sobre la cantidad gastada en 2018. La industria va a empezar a reemplazar el cerebro humano por maquinas, maquinas que sean más inteligentes, maquinas que puedan hacer el trabajo mucho más rápido, que no se cansen, no se aburran, no necesiten descansar, dormir y no se rompan [8].

¿La Amenaza es Real?

Si bien las ventajas y beneficios en el tiempo que estamos viviendo son muchos, también esto trae consigo varios aspectos negativos. Una de las amenazas más significativas y destructivas que estamos enfrentado es que nuestra información privada y persona está en constante peligro [11]. En los últimos años se han visto un aumento significativo en los ataques cibernéticos que hemos estado recibiendo, esto trae por consiguiente pérdida de dinero para los usuario o compañías que han sido afectadas. Las pérdidas financieras son un riesgo muy significativo para las empresas, además de que la reputación que estás compañías han creado se vería afectada. En los últimos años hemos visto como algunas de las compañías más importantes del mundo han sufrido ataques cibernéticos y la información de sus clientes o empleados ha sido comprometida [12].

A continuación, se mostrará las violaciones de dato que han tenidos algunas de las compañías más reconocidas en el mundo [13].

Tabla 2
Algunas Compañías Comprometidas en los últimos 8 años

Compañía	Fecha	Consecuencia
Heartland Payment Systems	2008	134 millones de tarjetas de créditos expuestas
MySpace	2013	360 millones de cuentas de usuarios comprometidas
Adobe	2013	153 millones de cuentas comprometidas
Yahoo	2013 2014	3 billones de cuentas de usuarios comprometidas
eBay	2014	Información de 145 millones de usuarios expuestos
NetEase	2015	235 millones de cuentas de usuarios comprometidas
Adult FriendFinder	2016	412.2 millones de cuentas de usuarios comprometidas
LinkedIn	2012 2016	165 millones de cuentas de usuarios comprometidas
Equifax	2017	147.9 millones de cuentas consumidores comprometidas
Marriot International	2014 2018	500 millones de cuentas de clientes comprometidas
Dubsmash	2018	162 millones de cuentas de usuarios comprometidas
My Fitness Pal	2018	150 millones de cuentas de usuarios comprometidas
Zynga	2019	218 millones de cuentas comprometidas
Canva	2019	137 millones de cuentas comprometidas
Sina Weibo	2020	538 millones de cuentas comprometidas

Los ataques cibernéticos no discriminan y afectan a los individuos, empresas privadas y organizaciones gubernamentales, por igual. Se está avanzando en una era en la que los criminales cibernéticos pueden estudiar y atacar a sus víctimas desde cualquier parte del mundo a cualquier hora. Cualquier organización independientemente de su tamaño o ubicación geográfica puede ser un objetivo potencial. La necesidad de integrar la inteligencia artificial en la seguridad cibernética nunca ha sido más critica que ahora [11].

La tecnología está cambiando constantemente. Al igual que la tecnología cambia, también la forma que los criminales cibernéticos utilizan para distribuir sus virus o programas malignos. La realidad es que la detección de los programas malignos se ha vuelto mucho más difícil a cómo era en el pasado. No es raro que los criminales cibernéticos utilicen múltiples técnicas para disfrazar sus códigos, hacer que sus códigos malignos sean indetectables para los antivirus y utilicen la encriptación para evitar ser examinados. Esto hace que las posibilidades de que los criminales cibernéticos puedan comprometer un sistema sin ser detectados sean mayores.

Las amenazas están constantemente cambiando y nuevas vulnerabilidades son descubiertas diariamente. Ningún aplicación, equipo, sistema o tecnología es inmune a las vulnerabilidades de seguridad, sin importar la cantidad de pruebas de seguridad que se realicen. Con la complejidad y las

capacidades que tienen los criminales cibernéticos hoy día es muy probable que la mayoría de las redes se vean comprometidas en algún momento.

USO DE LA INTELIGENCIA ARTIFICIAL EN LA SEGURIDAD CIBERNÉTICA

Entre los muchos beneficios que la inteligencia artificial le puede brindar a la seguridad cibernéticas estos son solo algunos [14]:

- La inteligencia artificial tiene la capacidad de analizar el comportamiento de los usuarios. Lo que esto significa es que los algoritmos que utilizan pueden aprender y crear patrones de comportamiento [9]. Esto lo hace analizando como los usuarios utilizan sus equipos electrónicos y a cuáles sistemas en línea se conectan. Básicamente analiza todo lo que el usuario hace desde que inicia su sesión, la dirección IP que tiene su sistema, las direcciones web que visita, los patrones de escritura y búsqueda. Si en algún momento los algoritmos detectan actividades inusuales o cualquier comportamiento que se salga de lo normal, el sistema puede alertar debido a que ha detectado un comportamiento sospechoso e incluso podría bloquear esa cuenta [9],[11].
- Los sistemas de seguridad basados en inteligencia artificial y aprendizaje automático se pueden configurar para que estén proactivamente buscando posibles vulnerabilidades que puedan ser identificadas. Esto ayuda ya que se puedan identificar las vulnerabilidades mucho más rápido y preciso. De esta forma se disminuyen los ataques de *zero day exploits*. Basándose en la información que estos sistemas están recopilando de su entorno constantemente pueden determinar cuándo y cómo la amenaza podría llegar a los sistemas que están vulnerable [15].
- Ayudan a compensar la escasez de personal diestro en el campo de la seguridad cibernética que están sufriendo las compañías y ayudan a reducir costos operacionales.
- Debido a que estos sistemas cuentan con la capacidad de aprendizaje automático pueden adaptar y utilizar sus algoritmos basándose en los datos recibidos, de este modo aprendiendo y comprendiendo mejor los cambios que necesitan hacerse. Esto significa que el aprendizaje automático permite al sistema predecir las amenazas y observar cualquier anomalía con mucha más precisión que cualquier ser humano [11].
- La inteligencia predictiva de amenazas ayuda a exponer mucho más fácil los centros de comando y control desconocidos y los dominios maliciosos [8].
- Se pueden utilizar para eliminar datos no deseados, de esta forma ayudará a los expertos en seguridad cibernética a comprender mucho mejor el entorno cibernético con el fin de poder detectar las actividades anormales [15].
- Beneficia a la seguridad cibernética con la automatización de técnicas que se puedan generar cuando se detectan amenazas cibernéticas [15].
- Esta tecnología es capaz de analizar grandes cantidades de datos, esto permite que se puedan desarrollar sistemas y aplicaciones de manera apropiada con el fin de poder reducir los ataques cibernéticos [15].
- Ayuda a proporcionar normas de seguridad efectivas y a desarrollar mejores estrategias de prevención y recuperación [15].
- Ayuda a mejorar las defensas contra los contenidos digitales manipulados o los *DeepFake* [9].Esta es una técnica de la inteligencia artificial que permite editar videos falsos de personas aparentando ser reales. Esto lo hace utilizando algoritmos de aprendizaje no supervisados. El resultado final es poder crear un video muy realista, aunque ficticio [14].
- Pueden identificar de inmediato el tráfico inusual en las redes, esto ayuda a reducir lo que es la minería de Bitcoin, la ejecución de archivos remotos e incluso los inicios de sección de Fuerza Bruta [15].

- Pueden detectar patrones de comportamiento malicioso en el tráfico de la red, en los archivos y sitios web que se introducen en las redes. Esto es debido a que las redes basadas en inteligencia artificial pueden detectar ataques que no serían posible detectar por sistemas regulares de defensa [15].
- Detección y mitigación de ataques DDoS con éxito. Se ha demostrado que compañías con escasos recursos de defensa han tenido éxito contra ataques de gran escala de DDoS cuando utilizan inteligencia artificial [6].
- Los sistemas bancarios y comerciales están utilizando la inteligencia artificial para ayudar a prevenir los delitos financieros. Esto es posible ya que estos sistemas ayudan a detectar el fraude y pueden realizan análisis de riesgos en caso de que alguna transacción sea considerada de alto peligro o sospechosa. Gracia a esto se pueden acelerar los procesos de detección de fraudes [15].

IMPACTO DE LA INTELIGENCIA ARTIFICIAL

Es sumamente importante entender que el uso de sistemas de inteligencia artificial en el campo de la seguridad cibernética puede tener tres tipos de impactos [14].

- Ampliar las amenazas
- Cambiar el comportamiento típico de esas amenazas
- Introducir nuevas amenazas

Si no se utiliza adecuadamente esta tecnología la cantidad de actividades cibernéticas maliciosas se podría ampliar y a la misma vez la velocidad a la que estos ataques se realizan se pudiera acelerar. Es bien importante entender que al igual que se utiliza la inteligencia artificial para proteger los sistemas, también los criminales cibernéticos la pueden utilizar para atacarlos. No importa si las compañías de seguridad desarrollan mejores mecanismos o técnicas para detectar vulnerabilidades o códigos maliciosos, los criminales cibernéticos van a intentar desarrollar ataques más difíciles de detectar [9]. Algo también muy importante y que crea tensión, es que los criminales cibernéticos también pudieran utilizar la inteligencia artificial para realizar ataques más eficaces, dirigidos y sofisticados debido a la eficiencia, escalabilidad y adaptabilidad de estos sistemas. Los objetivos potenciales serían más fáciles de identificar y controlar [9].

La tecnología tradicional depende en gran medida de los datos recolectados del pasado. Es difícil que la tecnología tradicional puede seguir el ritmo de los nuevos mecanismos y metodología que los criminales cibernéticos están utilizando [16]. La mayoría de las soluciones de seguridad cibernética utilizan una metodología basada en reglas o firmas que requiere demasiada intervención humana [9]. Además, el volumen de amenazas cibernéticas con las que los administradores de seguridad tienen que lidiar diariamente es demasiado, por tal razón es mejor que se introduzca la inteligencia artificial.

COSTO DE LAS VIOLACIONES DE DATOS

A continuación se muestra la recopilación de datos de las violaciones de datos que tuvieron 524 organizaciones alrededor de 17 países y regiones entre los meses de agosto 2019 y abril 2020. Esta información fue recopilada por *IBM Security* [1]. Un dato muy importante que hay que mencionar es que hubo una reducción en el costo total promedio de violaciones de datos del 2019 al 2020. En el 2019 se tuvo un costo total promedio de $3.92 millones de dólares vs el 2020 que ha tenido hasta este momento un costo total promedio de $3.86 millones de dólares. Una reducción de 1.5%, esta reducción fue posible gracias a que muchas de estas compañías adoptaron medidas de seguridad más estrictas e implementaron sistemas de seguridad y procesos de respuesta a incidentes automatizados. El 80% de las organizaciones reportaron que la información personal de los clientes se vio comprometida durante la violación de datos, mucho más que cualquier otro tipo de récord.

En la Figura 1 se puede ver los costos totales promedios de las violaciones de datos en los último 7 años. Desde el 2014 el costo total promedio ha aumentado en un 10%. Para el 2020 el costo total promedio ascendió a $3.86 millones de dólares.

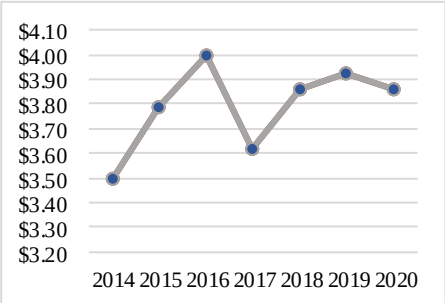

Figura 1
Costo Total Promedio de las Violaciones de Datos

Como se observa en la Figura 2, cuando ocurrieron las violaciones de datos la información de los clientes es la que más a menudo es robaron. Cuando ocurre una violación de datos, en el 80% de los casos los datos de los clientes son comprometidos.

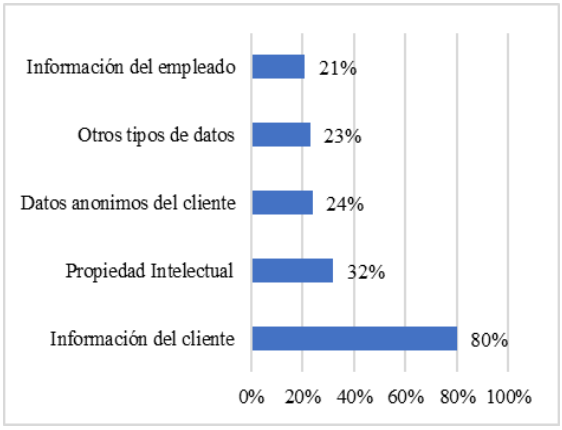

Figura 2
Tipos de Archivos Comprometidos

CAUSAS DE LAS VIOLACIONES DE DATOS

Las razones principales por las cuales ocurren las violaciones de datos pueden ser divididas en 3 grupos. El primer grupo incluye las fallas de sistema, ya sean fallas en los procesos de negocio o de los sistemas. El segundo grupo es de los errores humanos. En este grupo podemos mencionar los empleados que son negligentes y contratistas que involuntariamente ocasionan la violación de datos. Por último, los ataques maliciosos, que pueden ser causados por criminales cibernéticos o personal interno.

Como se observa en la Figura 3, los ataques maliciosos fueron la mayor causa de las violaciones de datos con un 52%. Casi el doble en comparación con el 25% que es causado por fallas del sistema y el 23% que es causado por lo errores humanos.

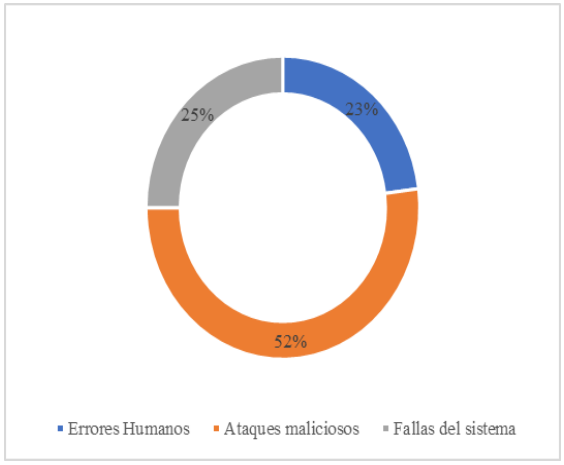

Figura 3
Desglose de las Violaciones de Datos

La Figura 4 presenta como los ataques maliciosos han ido en aumento desde el año 2014. En un periodo de 7 años ha habido un aumento de 10%. Este número podría cambiar si las compañías empezaran a implementar sistemas de seguridad inteligentes.

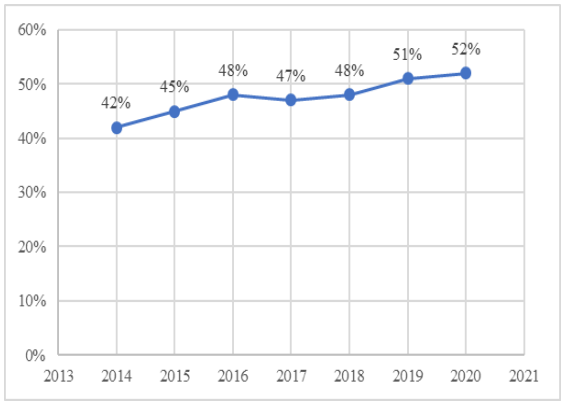

Figura 4
Tendencia en las Violaciones de Datos Causados por Ataques Malicioso

Tendencias y Efectividad de la Automatización de la Seguridad

La automatización de la seguridad se refiere a que las compañías están reemplazando la intervención humana en la identificación y contención de violaciones de datos o ataques cibernéticos por tecnologías que están basada en inteligencia artificial y Aprendizaje Automático.

En la Figura 5 se observa que en los últimos 3 años las compañías han ido cambiando sus sistemas tradicionales de seguridad por sistemas automatizados y mejor preparados para afrontar las amenazas que están surgiendo cada día. De las compañías encuestadas para el año 2020 un 21% ha hecho la implementación total de sus sistemas de seguridad automatizados. Un 38% hizo una implementación parcial y un 41% no implemento ningún sistema automatizado de seguridad.

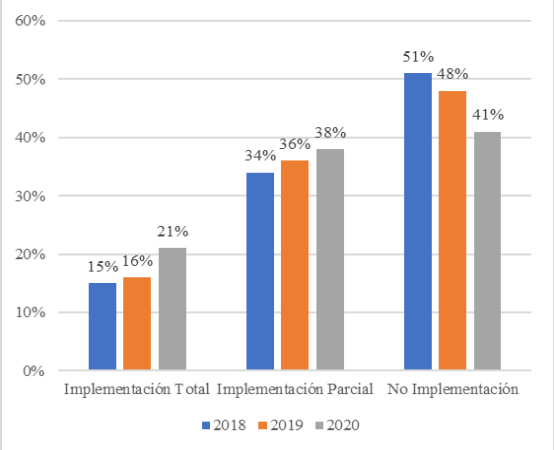

Figura 5
Porciento de Automatización del 2018 al 2020

En la Figura 6 se observa la cantidad de dinero que las compañías que implementaron sistemas automatizados de seguridad tuvieron que invertir debido a las violaciones de datos. El gasto fue mucho menor en comparación con las compañías que no implementaron sistema de seguridad automatizado. Es importante que las compañías entiendan que mientras más rápido se pueda identificar y contener las violaciones de datos, menor van a ser los costos totales. Identificar se refiere al tiempo que se tardan las compañías en detectar que se ha producido un incidente. Contención se refiere al tiempo que tardan las compañías en resolver la situación una vez se ha detectado y se logra restablecer el servicio en un 100%.

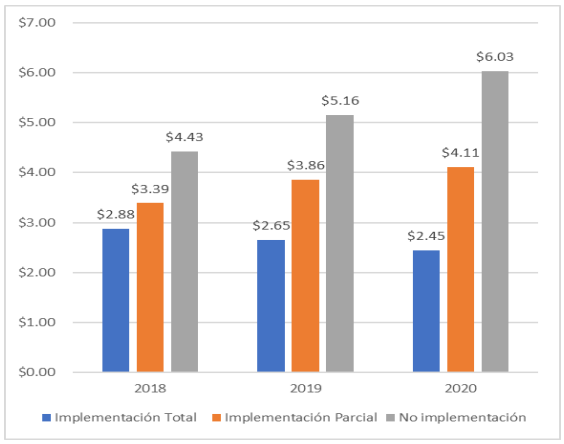

Figura 6
Costo Total Promedio de Violaciones de Datos del 2018-2020

La Figura 7 presenta cómo el tiempo de identificar y contener es mucho menos cuando las compañías utilizan sistemas de seguridad automatizados. En este caso las compañías que tuvieron una implementación total de sus sistemas de seguridad tardaron un promedio de 234 días para completar el ciclo completo desde que se identificaron las amenazas hasta que se restablecieron los sistemas. En comparación con las compañías que no tiene sistemas automatizados que el tiempo total promedio es de 308 días. Una diferencia de 74 días.

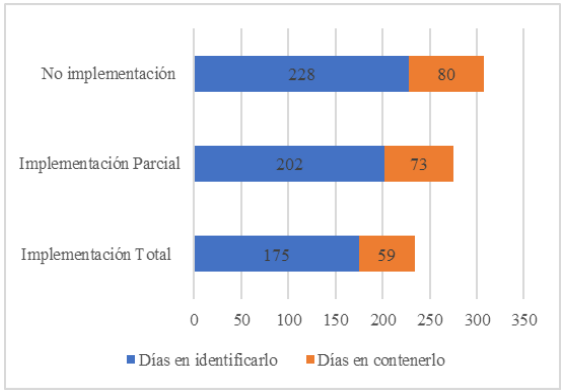

Figura 7
Tiempo Promedio para Identificar y Contener una Violación de Datos

REFERENCIAS

[1] IBM Security, *Cost of Data Breach Report 2020*. Armonk, NY: IBM Corporation, 2020.

[2] B. Fischer. (2020, Marzo 2). *What is the Average Cost of a Data Breach?* [Online]. Available: https://www.scasecurity.com/cost-of-a-data-breach/#:~:text=The%20average%20size%20of%20a,breach%20will%20exceed%20%24150%20million.

[3] S. Bhutada and P. Bhutada, "Application of Artificial Intelligence in Cyber Security," *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE).* vol. 5, no. 4, p. 2014-2019, April 2018.

[4] SecureWeek. (2019, abril 24). *¿Qué es la seguridad cibernética?* [Online] Available: https://www.secureweek.com/que-es-la-seguridad-cibernetica/

[5] NortonLifeLock. (n.d.) *What is a data breach?* [Online]. Available: https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html

[6] C. Czosseck, E. Tyugu and T. Wingfield. "Artificial Intelligence in Cyber Defense". *3rd International Conference on Cyber Conflict*, Tallin, Estonia: Cooperative Cyber Defense Center of Excellence (CCD COE) and Estonia Academy of Science, 2011.

[7] M. R. Gurrola–López y J. C. Macias-Torres. (n.d.) *Agentes Inteligentes* [Online]. Available: https://sitiointeligenciaa.wordpress.com/agentes/

[8] O. Gan. (2018, marzo 21). *Artificial Intelligence: a Silver Bullet in Cyber Security? CPX360* [Online]. Available: https://www.youtube.com/watch?v=ggje-L0ViFM

[9] D. Palmer. (2020, marzo 2). *AI is changing everything about cybersecurity, for better and for worse. Here's what you need to know* [Online]. Available: https://www.zdnet.com/article/ai-is-changing-everything-about-cybersecurity-for-better-and-for-worse-heres-what-you-need-to-know/

[10] A. Laurence. (2019, Agosto 22). *The impact of Artificial Intelligence on Cyber Security* [Online]. Available: https://www.cpomagazine.com/cyber-security/the-impact-of-artificial-intelligence-on-cyber-security

[11] R. Ramachandran. (2019, septiembre 14). *How Artificial Intelligence is Changing Cyber security Landscape and Preventing Cyber Attacks* [Online]. Available: https://www.entrepreneur.com/article/339509

[12] M. Mendoza. (2020, febrero 13). *Ciberataques: una de las principales amenazas para el 2020* [Online]. Available: https://www.welivesecurity.com/la-es/2020/02/13/ciberataques-principales-amenazas-2020/

[13] D. Swinhoe. (2020, abril 17). *The 15 biggest data breaches of the 21st century* [Online]. Available: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

[14] R. Aghemo. (2020, junio 18). *Artificial Intelligence and its us in Cyber Security* [Online]. Available: https://medium.com/ai-in-plain-english/artifical-intelligence-and-its-use-in-cyber-security-5da4be98a108

[15] C.S. Enterprise. (n.d.) *Use of IA in Cyber Security* [Online]. Available: https://ciostory.com/cxo-perspective/use-of-ai-in-cyber-security

[16] N. Wirkuttis and H. Klein, "Artificial Intelligence in Cybersecurity" *Cyber, Intelligence, and Security*, vol. 1, no. 1, p. 103-119, January 2017.