Revista Científica Mundo de la Investigación y el Conocimiento

DOI: 10.26820/recimundo/7.(2).jun.2023.441-452
URL: https://recimundo.com/index.php/es/article/view/2074
EDITORIAL: Saberes del Conocimiento
REVISTA: RECIMUNDO
ISSN: 2588-073X
TIPO DE INVESTIGACIÓN: Artículo de Investigación
CÓDIGO UNESCO: 1203 Ciencias de Los Ordenadores
PAGINAS: 441-452

Mapeo del panorama actual de la ciberseguridad en la era moderna digital

Mapping the current cybersecurity landscape in the modern digital age

Mapeamento do atual panorama da cibersegurança na era digital moderna

Fausto Manuel Coronel Ayala[1]; Galo Mauricio López Sevilla[2]

RECIBIDO: 29/06/2023 **ACEPTADO:** 22/07/2023 **PUBLICADO:** 21/08/2023

1. Ingeniero en Electrónica y Redes de Información; Pontificia Universidad Católica del Ecuador; Ambato, Ecuador; fmcoronel@pucesa.edu.ec; https://orcid.org/0009-0001-4968-3792
2. Magíster en informática; Diploma Superior en Gerencia informática; Ingeniero en Sistemas; Pontificia Universidad Católica del Ecuador; Ambato, Ecuador; glopez@pucesa.edu.ec; https://orcid.org/0000-0003-4699-4875

CORRESPONDENCIA

Fausto Manuel Coronel Ayala
fmcoronel@pucesa.edu.ec

Ambato, Ecuador

RESUMEN

Los riesgos y amenazas que enfrenta la ciberseguridad no son comprendidos en toda su magnitud por los usuarios hasta que son víctimas de algún tipo de ataque cibernético, que afecta tanto a individuos como a organizaciones en diferentes magnitudes y que, generalmente, son ejecutados por especialistas. Por otra parte, actualmente en casi todos los rincones del mundo se emplea algún sistema digital donde los datos no están debidamente protegidos, siendo vulnerables a todo tipo de amenazas, situación que fue magnificada por la pandemia, donde el abrupto cambio al método de trabajo a distancia requirió prestar más atención a la ola de posibles ataques informáticos. Algunos estudios afirmaron que a fines del año 2020 aproximadamente el 31% de la información registrada en las plataformas digitales fue objeto de robo con fines delictivos, estimando que el costo del cibercrimen se incremente hasta los 8 billones de dólares en los próximos años, cifra en extremo preocupante para las organizaciones. Este documento se elaboró con la finalidad de compilar datos relevantes acerca de la ciberseguridad y seguridad informática, considerando el creciente aumento dentro de la era digital, resaltando la opinión de expertos y líderes en el área sobre el presente y futuro de la ciberseguridad y seguridad informática.

Palabras clave: Ciberseguridad; Seguridad Informática; Era Digital; Ataques Informáticos.

ABSTRACT

The risks and threats faced by cybersecurity are not fully understood by users until they become victims of some kind of cyber-attack, which affects individuals and organizations to varying degrees and is usually executed by specialists. Moreover, currently, in almost every corner of the world, some digital system is used where data is not properly protected, making it vulnerable to all kinds of threats. This situation that was magnified by the pandemic, where the abrupt shift to remote work required more attention to the wave of possible cyberattacks. Some studies stated that by the end of 2020, approximately 31% of the information recorded on digital platforms was subject to theft for criminal purposes, estimating that the cost of cybercrime will increase up to $8 trillion in the coming years, a highly concerning figure for organizations. The purpose of this document is to compiling relevant data about cybersecurity and information security, considering the growing increase within the digital era, highlighting the opinions of experts and leaders in the field regarding the present and future of cybersecurity and information security.

Keywords: Cybersecurity; Informatic Security; Digital Age; Computer Attacks.

RESUMO

Os riscos e ameaças enfrentados pela cibersegurança não são totalmente compreendidos pelos utilizadores até que se tornem vítimas de algum tipo de ciberataque, que afecta indivíduos e organizações a vários níveis e é normalmente executado por especialistas. Além disso, atualmente, em quase todos os cantos do mundo, é utilizado algum sistema digital em que os dados não estão devidamente protegidos, tornando-os vulneráveis a todo o tipo de ameaças. Esta situação foi ampliada pela pandemia, onde a mudança abrupta para o trabalho remoto exigiu uma maior atenção à onda de possíveis ciberataques. Alguns estudos afirmam que, no final de 2020, aproximadamente 31% da informação registada nas plataformas digitais foi sujeita a roubo para fins criminosos, estimando que o custo da cibercriminalidade aumentará até 8 biliões de dólares nos próximos anos, um valor altamente preocupante para as organizações. O objetivo deste documento é compilar dados relevantes sobre a cibersegurança e a segurança da informação, tendo em conta o crescente aumento na era digital, destacando as opiniões de especialistas e líderes na área sobre o presente e o futuro da cibersegurança e da segurança da informação.

Palavras-chave: Cibersegurança; Segurança Informática; Era Digital; Ataques Informáticos.

Introducción

En pleno siglo XXI, toda la población mundial, tanto personas como organizaciones, utilizan algún tipo de sistema digital y, por tanto, son vulnerables a ciberataques porque los datos no están protegidos. Así se tiene que los robos de información ocurren con mucha regularidad, descubriendo direcciones de correo electrónico, contraseñas, información de tarjetas de crédito y otros datos excepcionalmente confidenciales.

La gravedad de esta situación no es comprendida en toda su magnitud por los usuarios hasta que son víctimas de los ciberataques, siendo afectados, tanto individuos como organizaciones, de manera fraudulenta y, por lo general, por expertos. Esto lo confirma Experian [1], empresa de calificación crediticia con oficinas en todo el mundo, que ha publicado estadísticas para finales del 2020, donde se muestra que el 31% de la información personal robada, condujo a robos de identidad completos. En el caso de las organizaciones el robo de datos es más sutil, debido a que el efecto del ciberataque puede manifestarse unos meses después de que se produzca, y rara vez o nunca se nota inmediatamente para abordar los problemas.

Las listas publicadas de datos confidenciales, de clientes o datos ultrasecretos de creación y perfeccionamiento de productos de investigación y desarrollo en la dark web, son desastrosas para la operación de las organizaciones. Sin embargo, el riesgo de filtraciones de información aparentemente se ha convertido en un hecho ineludible en la actualidad, lo cual determina la importancia de la preparación, manejo y enfoque necesario de ciberseguridad para manejar este tipo de ataques y filtraciones, considerando, además, que prepararse en ciberseguridad representa un constructo que incluye políticas, algo de hardware, software y, especialmente, la concientización de los usuarios [2].

Caso especial merece la ciberseguridad durante la pandemia de coronavirus COVID-19, considerando que los ciberdelincuentes redefinieron, tanto los objetivos como la forma de ciberataques, siendo dirigidos estos ataques, principalmente, a organizaciones gubernamentales, instituciones de atención médica o entidades de infraestructura crítica, con efectos que amenazaron la salud y la vida de las personas al paralizar las instalaciones médicas [3], [4].

Los piratas informáticos explotaron principalmente el miedo de las personas a una pandemia, lo que generó grandes pérdidas para entidades de diversas industrias, los ejecutivos de negocios de varias industrias enfrentaban un entorno de amenazas cibernéticas que cambiaba rápidamente a causa de una pandemia. Además, el cambio del modo de trabajo estacionario a remoto requirió prestar más atención a la ola de posibles ataques de piratería, lo que generó costos adicionales en seguridad. Según Global Risk Survey 2020, el 79% de los ejecutivos admitió que las organizaciones no estaban lo suficientemente preparadas para enfrentar una crisis de seguridad informática [5].

Este documento se elaboró con la finalidad de compilar datos relevantes acerca de la ciberseguridad y seguridad informática, considerando el creciente aumento dentro de la era digital, resaltando la opinión de expertos y líderes en el área sobre el presente y futuro de la ciberseguridad y la seguridad informática.

Metodología

Para el desarrollo de la presente investigación se considerará a la estructura de revisión sistemática de la literatura propuesta por Kitchenham [6], por medio de la cual se encontrará información relevante acerca de las preguntas de investigación propuestas.

Este proceso metodológico establece tres etapas:

- Planificación de la búsqueda.
- Ejecución de la búsqueda.
- Análisis y documentación de resultados.

Planificación de la búsqueda

El objetivo primordial del presente estudio es recabar datos relevantes sobre ciberseguridad y seguridad informática, considerando el creciente aumento dentro de la era digital, destacando información de expertos y líderes en el área acerca del presente y futuro de la ciberseguridad y la seguridad informática.

Para abordar este tema de manera sistemática, se proponen las siguientes preguntas de investigación:

P1: ¿Cuáles son los principales riesgos que enfrenta la ciberseguridad?

P2: ¿Cuáles son las cifras actuales que maneja la ciberseguridad?

P3: ¿Cuáles son las expectativas a futuro de la ciberseguridad de acuerdo a los expertos?

Se recurrió a bases de datos digitales de consulta, como son IEEE eXplorer, Science Direct, ACM Digital Library, SCOPUS, Springer Link y páginas WEB especializadas que tratan sobre temas asociados a la seguridad informática, ciberseguridad, tendencias en el área de seguridad digital y proyecciones y expectativas de la seguridad de los datos. Se examinaron revistas académicas y publicaciones técnicas como fuentes de información confiables, publicadas entre los años 2018 y 2022, para obtener datos relevantes.

El método de búsqueda se centró en aspectos enfocados a las preguntas de investigación propuestas, utilizando las palabras claves a continuación citadas: “seguridad informática”, “ciberseguridad”, “seguridad de la información”, “era digital”, “ataques informáticos”, “estrategias de defensa digital”, así como también traducciones en inglés. Además, con la finalidad de depurar la selección se aplicaron los siguientes criterios de inclusión/exclusión (ver Tabla 1).

Tabla 1. Criterios de selección

Criterios de inclusión	Criterios de exclusión
Artículos que tratan temas acerca de los riesgos que enfrenta la ciberseguridad y la seguridad informática, estadísticas de ataques informáticos y expectativas a futuro del área de ciberseguridad.	Información publicada en sitios web generales.
Documentos que presentan análisis de líderes y especialistas en el área de ciberseguridad.	Documentos con aportes irrelevantes.
Artículos con información acerca de los más actuales métodos de defensa desarrollados para evitar los ataques informáticos.	Información de blogs.

Ejecución de la búsqueda

En esta etapa se identificaron los artículos más relevantes considerando las palabras clave y los criterios de selección. En cada documento, se revisó los títulos, el desarrollo y las conclusiones, con lo cual se estableció el aporte que brindan a las preguntas planteadas.

Luego de ejecutar la búsqueda, se obtuvo un total de 43 documentos, de los cuales se seleccionaron 17, mismos que cumplieron con los criterios antes definidos.

Antes de conocer los datos más relevantes acerca de la seguridad informática y ciberseguridad en la actual era digital, es importante conocer los riesgos en la operación de las tecnologías de la información y las comunicaciones, lo cual se respondió al desarrollar la P1: ¿Cuáles son los principales riesgos que enfrenta la ciberseguridad?

Los principales riesgos que enfrenta la ciberseguridad se derivan, principalmente, de dos amenazas fundamentales que son el sabotaje y el Internet. Donde el sabotaje

se refiere a un problema interno de recursos humanos que debe ser resuelto por medio de prácticas eficientes y actualizadas dirigidas a la ciberseguridad, encontrando que las mejores defensas están bien determinadas en la política de recursos humanos propuesta por ISO 27001[7].

Sin embargo, es complicado alcanzar una protección completa de las amenazas cibernéticas, incluso si estas normas son implementadas a fondo, principalmente debido que las organizaciones deben confiar en los empleados hasta cierto punto, asegurándose que los procedimientos de respaldo sean sólidos y diversificados. Por otra parte, el Internet, representa una ventana muy peligrosa por estar abierta a los piratas informáticos y otros ciberdelincuentes [8].

Existen múltiples riesgos dentro de la seguridad informática, entre los cuales se puede mencionar el malware, nombre común para muchas versiones maliciosas de programas que usualmente, están representadas por un código informático destinado a destruir datos o procesos, así como adquirir accesos no autorizados a una red. Por lo general, se proporcionan como un enlace o un archivo adjunto a un correo electrónico para que el usuario pueda hacer clic o abrir el archivo de malware. Los ciber-atacantes están mejorando sus técnicas, incluyendo tácticas de robo o cifrado de información confidencial para solicitar un rescate por la misma, lo cual se conoce como ransomware [9].

En términos de malware, un informe de 2016 del Cisco Security Research Group señala que las redes sociales y los blogs son los sitios más vulnerables a los ataques cibernéticos debido al fácil acceso, las funciones gratuitas y la gran popularidad entre los usuarios, lo que facilita el robo de información sin ser detectados. Por citar un ejemplo de plataforma, tenemos, WordPress donde son comunes los ataques de robo de identidad o fraudes bancarios, se ha identificado una gran cantidad de sistemas (complementos) que propician la ejecución de todo tipo de malware[10].

También vale la pena mencionar el phishing, que es un tipo de ataque de ciberseguridad en el que los expertos informáticos, conocidos como phishers, envían mensajes maliciosos haciéndose pasar por una persona u organización de confianza, para engañar a los usuarios y de esta manera que ejecuten una acción, como subir un archivo malicioso, hacer clic en un enlace falso o exponer información confidencial como credenciales de inicio de sesión. Esta vulnerabilidad representa una forma común de ingeniería social, un término general que describe los intentos de manipular o engañar a los usuarios de computadoras. La ingeniería social es la amenaza más comúnmente utilizada, estando presente en casi todos los incidentes de seguridad, y que, a menudo, combina el phishing con otras amenazas, como malware, la inyección de código y los ataques de red [11].

El ransomware se conoce como un tipo de malware que tiene como objetivo encriptar información y datos valiosos de las organizaciones para exigir un pago como condición para acceder a ellos. Además, a menudo se usa para robar información confidencial de las organizaciones, exigiendo un pago considerable para no difundir o compartir esta información con competidores, autoridades o público en general. Este tipo de ataques se centran principalmente en datos o estructuras importantes de la organización, bloqueando o deteniendo operaciones, lo cual representa un dilema para la alta gerencia; por un lado, cancelar el monto del rescate y esperar que los atacantes cumplan con la promesa de permitir de nuevo el acceso a los datos sin hacerlos públicos; y, por otro lado, no pagar el rescate e intentar utilizar métodos de recuperación con el fin de restablecer las operaciones [12].

Así también, existe lo que se denomina como denegación de servicio distribuida (DDoS) que es uno de los tipos de ataques más peligrosos que afectan a las computadoras. El objetivo principal de este ataque es inutilizar una determinada máquina y hacer que los servicios no estén disponibles para

los usuarios legítimos, esto se consigue principalmente cuando varias computadoras envían una gran cantidad de paquetes hacia el equipo objetivo con el fin de consumir sus recursos y hacerlo que deje de trabajar [13].

En lo relativo a la seguridad física de un dispositivo, se considera como un factor crucial dentro de la ciberseguridad, debido a que la propiedad puede cambiar dependiendo de las necesidades [14]. Si un dispositivo con alta vulnerabilidad es compartido por varios usuarios puede causar mucho más daño que si se usa personalmente. Si bien el uso compartido se considera una característica, puede hacer que toda la base de usuarios sea vulnerable, por lo que este aspecto debe tenerse en cuenta [15], [16].

Entre las principales cifras estadísticas de ciberseguridad reportadas por diversos informes especializados para el año 2022 [17], resalta el hecho que sucedieron 2200 ataques cibernéticos diarios, es decir, la ocurrencia de un ataque cibernético en promedio es de 39 segundos, además se resaltan otros datos importantes entre los cuales se puede mencionar:

- El 92% del malware se entregó por correo electrónico.
- El área de la salud es el objetivo principal de los ataques de ransomware.
- 4,1 millones de sitios web tienen malware en un momento dado.
- 49 días es el tiempo promedio que toma identificar un ataque de ransomware.
- El 97% de todas las infracciones de seguridad explotaron los complementos de WordPress.
- Se reportó el robo de 3 mil millones de dólares en criptomonedas.
- Las estadísticas de seguridad cibernética del trabajo remoto muestran que el 74% de los expertos en TI creen que representa una amenaza extrema para la seguridad cibernética.

Todo este conjunto de riesgos informáticos evidencia que los problemas de ciberseguridad se han convertido en una amenaza latente, tanto para las personas como para las organizaciones, considerando que el panorama de la ciberseguridad cambia frecuentemente, además está claro que las amenazas cibernéticas aumentan constantemente. Por esta razón, es fundamental una preparación actualizada, basada en el conocimiento de los últimos datos estadísticos, tendencias y hechos [18].

P2: ¿Cuáles son las cifras actuales que maneja la ciberseguridad?

De acuerdo con la información recopilada se puede mencionar algunos datos interesantes y estadísticas de ciberseguridad que alcanzan cifras alarmantes para el año 2022, resumidas de la siguiente manera:

- Se ha comprobado que el 85% de las infracciones de seguridad cibernética son originadas por errores humanos [19].
- El 96% del malware detectado es enviado por correo electrónico [20].
- Cada 10 segundos se registra un ataque de ransomware, lo cual no es extraño si se considera que los consumidores y organizaciones se enfrentan a diario a 100 mil sitios web maliciosos y 10 mil archivos maliciosos [21].
- El 71% de todos los ataques cibernéticos registrados poseen una motivación económica, seguidos por el robo de propiedad intelectual y el espionaje [19].
- Para el 2021 se registró que el costo global anual de la ciberdelincuencia fue de aproximadamente 6 billones de dólares, estimando que para el año 2025 será de 10.5 billones de dólares [22].

Con respecto al costo de los delitos cibernéticos se puede mencionar algunos datos interesantes, entre los cuales destacan:

- Durante la pandemia por COVID-19 el cibercrimen aumentó en un 600%.
- El costo del cibercrimen constituye un valor equivalente al 1% del PIB mundial.
- En términos generales, una empresa enfrenta un costo promedio superior a los 2,5 millones de dólares debido a un ataque de malware, el cual engloba tanto el desembolso económico directo como el tiempo necesario para solucionar dicho ataque [23].
- Para el año 2021 el ransomware fue 57 veces más destructivo en comparación con el 2015.
- Más del 50% de todos los ataques cibernéticos se realizan en SMB (Server Message Block), solo en EEUU existen 30 millones de SMB y más del 66% registraron al menos 1 incidente entre 2018 y 2020.
- El rango de costos en forma promedio de una filtración de datos para una empresa pequeña oscila entre 120 mil y 1,24 millones de dólares.
- Los costos de filtración de datos aumentaron de 3,86 millones a 4,24 millones de dólares en 2021, representando el costo total promedio más alto en 17 años.
- En cuanto al promedio de costos de las infracciones fue de 1,07 millones, lo que representa un aumento significativo, siendo el trabajo remoto un factor crucial en este incremento [23].
- Se registró un aumento del 10% en el costo total promedio de una infracción entre 2020 y 2021.
- En promedio las empresas experimentaron 130 brechas de seguridad por año.
- Durante el año 2021, se registró un aumento del 22,7% en el costo anual de ciberseguridad en las diferentes organizaciones a nivel mundial.
- Se observó un incremento del 27,4% en el número anual de brechas de seguridad en organizaciones empresariales.
- Las empresas requirieron en promedio de 23 días para recuperarse de ataques de ransomware y alrededor de 50 días para resolver ataques internos [23].
- 71,1 millones de personas son víctimas de delitos cibernéticos cada año.
- En promedio los individuos pierden 4,476 dólares por cibercrimen y por estafas de phishing 225 dólares, mientras que en conjunto la población pierde 318 mil millones [23].

En el transcurso del 2022, los principales delitos cibernéticos matizaron su prevalencia, entre ellos se encuentran los ataques de phishing, el robo de identidad, la extorsión, la falta de pago, la violación de datos personales, entre otros. Además, como dato relevante se conoce que una inversión mensual de 34 dólares puede generarle a un delincuente hasta 25.000 dólares mensuales [23].

En general, durante el 2022 el mercado global de ciberseguridad cerró con un crecimiento de 156 mil millones de dólares y se estima que para el 2023 sea de 177 mil millones, tendencia que se fundamenta en lo relevante en que se ha convertido la prevención y protección contra ciberataques en el sector empresarial. Además, se prevé que el costo del cibercrimen se incremente hasta los 8 billones de dólares, cifra en extremo preocupante para las organizaciones, por lo cual se seguirá recurriendo a especialistas en ciberseguridad que evalúen los sistemas, evitando de esta forma pérdidas millonarias por los ataques cibernéticos [24].

P3: ¿Cuáles son las expectativas a futuro de la ciberseguridad de acuerdo con los expertos?

A finales del año 2022 Security Magazine [25] publicó un artículo donde resume la opinión de líderes de seguridad acerca de los pronósticos de la ciberseguridad y la se-

guridad informática para el 2023, ofreciendo además opiniones de mejores prácticas de gestión de riesgos cibernéticos, basado en la planificación de resistencia a la ciberseguridad, prioridades y hoja de ruta para evitar o minimizar los ataques, entre los cuales se pueden mencionar los siguientes:

Aumento sustancial de la demanda de seguridad cibernética: Para el primer trimestre de 2022, las primas de seguro cibernético aumentaron un 28% aproximadamente, en comparación con el cuarto trimestre de 2021. Esta situación es consecuencia de la mayor conciencia de los riesgos financieros y de reputación de los incidentes cibernéticos, tal como ataques de ransomware, violaciones de datos y explotación de la vulnerabilidad, entre otros. Por otra parte, las compañías aseguradoras han aumentado los requisitos para obtener un seguro cibernético, siendo estos mucho más estrictos, lo cual requiere incrementar la tecnología como la autenticación de dos factores y la adopción de tecnologías específicas como EDR, XDR y más; lo cual propiciará el incremento de las primas de seguro cibernético, además que con requisitos más estrictos será más complicado el obtener un seguro. Adicionalmente, se evidenciará un incremento en la demanda, debido a la creciente incidencia de problemas en la cadena de suministro, lo que originará que las compañías comiencen a exigir cada vez más que proveedores o terceros que les presten algún servicio cuenten con un seguro cibernético imprescindible [26].

Aumento del enfoque basado en la ciberresiliencia por líderes y especialistas de seguridad. Si bien la protección de las organizaciones contra las amenazas cibernéticas siempre será un área central de enfoque para los programas de seguridad, se espera un mayor énfasis en el enfoque de la resiliencia cibernética, que se expande más allá de la protección para incluir la recuperación y la continuidad en caso de un incidente cibernético. No se trata únicamente de invertir recursos en la protección contra amenazas cibernéticas, sino de invertir en las personas, los procesos y la tecnología para mitigar el impacto y garantizar la continuidad de las operaciones en caso de un incidente cibernético [27].

Incremento en el aprendizaje y entrenamiento en el área de ciberseguridad. En el 2023 se observarán avances continuos en la capacitación en ciberseguridad, debido que los seres humanos no han evolucionado para detectar peligros en el mundo digital y los sistemas escolares no enseñan defensa contra las artes oscuras del ciberataque. Por lo tanto, es responsabilidad y está en cada líder de ciberseguridad equipar a los individuos con las habilidades necesarias para mantenerse a salvo de los ataques cibernéticos [25], [25].

La automatización, el aprendizaje adaptativo, la inteligencia artificial o aprendizaje automático pueden ayudar a brindar capacitación personalizada a escala, siendo esto muy importante; considerando que las personas necesitan participar con frecuencia con un entrenamiento relevante que se mantenga al borde de su nivel de habilidad para mejorar y mantenerse comprometidos. Además, recompensar a las personas a medida que adquieren habilidades en un entorno de aprendizaje dinámico confiere una mejora medible. Este enfoque describe ampliamente la gamificación, cuyo éxito demostrado se basa en principios establecidos de ciencia y negocios conductuales y es fundamental para proteger a las organizaciones de todos los tamaños [28], [29].

Se afianzarán conceptos básicos cibernéticos de higiene y conciencia cibernética. Fundamentado en la necesidad de convertirse en una sociedad de ciberseguridad, lo cual significa que la higiene cibernética y la conciencia serán una prioridad en 2023, con un incremento del número de organizaciones que buscan obtener un seguro cibernético, como una red de seguridad financiera, para proteger sus negocios de una exposición financiera grave como resultado de violacio-

nes de datos y ataques de ransomware. Por lo tanto, la necesidad de establecer una estrategia cibernética sólida tendrá el mandato de obtener un seguro, lo cual significa el retorno a lo básico para aumentar los límites de ciberseguridad. El trabajo remoto continuo y la transformación en la nube significan que se necesitará una estrategia sólida de gestión de acceso para ser compatible con la autenticación multifactorial, la gestión de contraseñas y la verificación continua para reducir los riesgos [30].

Además de implementar mejores controles de seguridad de acceso, los empleadores deberán capacitar a los trabajadores con una mejor conciencia de ciberseguridad, lo cual implicará capacitación y educación continua para garantizar que a medida que evolucionan las amenazas, los empleados estén informados y listos para ser defensores fuertes en las estrategias cibernéticas [31].

Los dispositivos conectados requerirán una seguridad más sólida. El número de dispositivos IoT conectados ha aumentado durante años, sin signos de desaceleración, considerando que, en los últimos tres años, el número de dispositivos IoT aumentó exponencialmente, debido a la transformación digital acelerada debido al COVID-19 y a la proliferación de la computación basada en la nube, así se tiene que durante el 2022 el mercado de IoT creció un 18%, con 14.400 millones de conexiones activas. A medida que más consumidores y organizaciones confían en dispositivos conectados, estas soluciones conectadas se vuelven más vulnerables a los ataques cibernéticos. Con esto, los miles de millones de dispositivos enviados por los fabricantes de equipos originales requerirán una mayor seguridad para mitigar el riesgo de intrusiones de malware y su contribución a la Denegación Distribuida de Servicios (DDoS). Para prevenir y mitigar ataques devastadores, los fabricantes y proveedores de fabricantes de equipos originales deben diseñar la seguridad dentro de los dispositivos, incrustándola en cada capa de un dispositivo conectado [32].

La gestión del riesgo cibernético será una prioridad para los líderes empresariales. Cuando se trata de la gobernanza y la supervisión del riesgo cibernético, la mayoría de los sistemas están rotos, debido a la acelerada evolución que presenta, además que enfrenta mayores intereses y una reputación corporativa frágil. Como resultado de esto, en 2023, se observa que las organizaciones duplicarán la gestión de riesgos cibernéticos. Las juntas deberán tener un papel y una responsabilidad mucho más claros cuando se trata del proceso de garantizar controles adecuados e informar sobre los ataques cibernéticos. La gobernanza del riesgo cibernético no es solo el dominio de la persona responsable de velar por la ciberseguridad de la empresa, ahora es claramente una preocupación a nivel de la Dirección General [33].

El auge de la inteligencia artificial (IA) y el aprendizaje automático. Estos desarrollos tecnológicos se han convertido rápidamente en importantes herramientas en el campo de la ciberseguridad, debido a la creciente cantidad de datos y amenazas cibernéticas sofisticadas, son utilizadas para fortalecer la seguridad de organizaciones e individuos, así como también para el análisis de grandes cantidades de datos e identificación de patrones que pueden indicar la presencia de una amenaza cibernética. Esto permite a las organizaciones detectar y responder a las amenazas cibernéticas con mayor rapidez y precisión que los métodos tradicionales[34].

Sin embargo, es importante destacar que, aunque la inteligencia artificial facilita los procesos de identificación de falencias y vulnerabilidades; el acompañamiento para la evaluación manual mediante hacking ético, es decir, expertos especializados en pruebas de penetración de sistemas informáticos y software, con la finalidad de valorar, fortalecer y mejorar la seguridad; será de gran utilidad para los próximos años. Considerando que implementar soluciones sin estrategias de seguridad claras puede tener un resultado desfavorable, debido a

que originan diagnósticos desacertados con falsos positivos o falsos negativos [24].

Otra área importante es el desarrollo del enfoque en la protección de datos personales y el cumplimiento de las regulaciones, con respecto a esto, la publicación de Compliance Aspekte de finales del 2022 [35] señala que, desde la perspectiva de los procesadores de datos, el entorno de privacidad de datos se vuelve más duro cada año y las sanciones contenidas en el Reglamento General de Protección de Datos (GDPR) son cada vez más frecuentes, considerando los permanente retos que enfrenta la gestión de protección de datos, que incluyen los silos de datos, la falta de sistemas consolidados, los datos dispersos y el trabajo manual.

Por lo cual las organizaciones a nivel mundial se proyectan hacia una rápida digitalización y al cumplimiento de las normas de seguridad y privacidad de datos. Además, de acuerdo a los especialistas, se estima una serie de cambios inminentes en el sector de la seguridad de datos frente a la privacidad en los próximos años, tales como la ampliación de las funciones de protección de datos, la protección de datos como servicio, adopción de herramientas de cumplimiento multiestándar para la gestión de la privacidad de datos y el fortalecimiento de la influencia del GDPR a nivel mundial.

Conclusiones

El costo de los ciberataques en el mundo, tal como malware, ransonware, phishing, DDoS, entre otros, se ha duplicado en los últimos años, dejando a muchas organizaciones inoperantes y con pérdidas de clientes, razón por la cual, en la actualidad las organizaciones están constantemente difundiendo mensajes sobre la importancia de crear más medidas de ciberseguridad, que no requieren grandes conocimientos sobre ordenadores o redes, ni equipamiento tecnológico muy avanzado, solo se necesitan los dispositivos, el sentido común y seguir una serie de consejos que son recopilados como medidas de ciberseguridad que cada vez más se encuentran a la disponibilidad de todos.

Sin embargo, el enfrentamiento entre los piratas informáticos y la ciberseguridad continuará en los próximos años con mayor intensidad, debido que los atacantes trabajan permanentemente con el fin de desarrollar y explotar técnicas maliciosas, utilizando sistemas más sofisticados, lo cual obliga que la seguridad evolucione de manera continua. Para lograr el máximo desarrollo los líderes y especialistas en ciberseguridad deben mantenerse a la vanguardia, contando actualmente con un instrumento importante basado en la Inteligencia Artificial, tecnología que puede brindar grandes soluciones a las brechas de ciberseguridad, aunque también puede convertirse en un arma para los ciberdelincuentes.

Por otra parte, las medidas de seguimiento, monitoreo y control del cumplimiento normativo es un componente clave de cualquier programa de ciberseguridad, por tanto, la creación y aplicación de un plan de monitoreo de cumplimiento capaz de evaluar continuamente las actividades de cumplimiento de las organizaciones en tiempo real representa la mejor manera de desarrollar un sistema exitoso de monitoreo de cumplimiento que incluya la comprensión de leyes y reglamentos que se aplican a la organización, y cómo se encuentra el cumplimiento de los mismos. Esto permitirá realizar un análisis de brechas, determinar cuáles son los controles de cumplimiento y procesos comerciales actuales, así como el establecimiento de controles de seguridad adicionales que deban ser implementados.

Bibliografía

Experian plc, «Experian plc: la ciberdemia continuará, según el Pronóstico de la Industria de Violación de Datos de Experian para 2022», 2021. https://www.experianplc.com/media/latest-news/2021/the-cyberdemic-will-continue-according-to-the-2022-experian-data-breach-industry-forecast (accedido 6 de enero de 2023).

Strategic Direction, «Digital defenses: The importance of cybersecurity in entrepreneurial ventures in the digital age», Strategic Direction, vol. 38, n.o 2, pp. 24-26, ene. 2022, doi: 10.1108/SD-12-2021-0159.

A. I. G. Ibrahim, «CYBERSECURITY: PANORAMA AND IMPLEMENTATION IN 2021», presentado en SAFE 2021, Rome, Italy, dic. 2021, pp. 41-54. doi: 10.2495/SAFE210041.

M. Alawida, A. E. Omolara, O. I. Abiodun, y M. Al-Rajab, «A deeper look into cybersecurity issues in the wake of Covid-19: A survey», Journal of King Saud University - Computer and Information Sciences, vol. 34, n.o 10, Part A, pp. 8176-8206, nov. 2022, doi: 10.1016/j.jksuci.2022.08.003.

J. Antczak, «The impact of the covid-19 pandemic on business entity cyber security», Inżynieria Bezpieczeństwa Obiektów Antropogenicznych, n.o 1, Art. n.o 1, mar. 2022, doi: 10.37105/iboa.128.

B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, y S. Linkman, «Systematic literature reviews in software engineering – A systematic literature review», Information and Software Technology, vol. 51, n.o 1, pp. 7-15, ene. 2009, doi: 10.1016/j.infsof.2008.09.009.

ISOTools, «ISO 27001 - Software ISO 27001 de Sistemas de Gestión», Software ISO, 2021. https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/ (accedido 16 de diciembre de 2022).

Net at Work Team, «The Role of HR Mitigating Cyber Security Threats», Net at Work, 6 de junio de 2018. https://www.netatwork.com/the-role-of-hr-mitigating-cyber-security-threats/ (accedido 16 de diciembre de 2022).

R. Krishnamurthi, A. Kumar, y S. S. Gill, Autonomous and Connected Heavy Vehicle Technology. Academic Press, 2022.

Cisco, «Cisco 2016. Informe anual de seguridad», Cisco Systems, Inc., San José, CA, 2016. Accedido: 6 de julio de 2022. [En línea]. Disponible en: https://www.cisco.com/c/dam/m/es_es/internet-of-everything-ioe/iac/assets/pdfs/security/cisco_2016_asr_011116_es-es.pdf

CheckPoint, «¿Qué es el phishing? Tipos de ataques de phishing - Software de Check Point», What is Phishing? Types of Phishing Attacks, 2020. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/# (accedido 11 de febrero de 2022).

W. C. Barker, W. Fisher, K. Scarfone, y M. Souppaya, «Ransomware Risk Management: A Cybersecurity Framework Profile (Spanish Translation)», National Institute of Standards and Technology, abr. 2022. doi: 10.6028/NIST.IR.8374.spa.

B. H. Ali, N. Sulaiman, S. A. R. Al-Haddad, R. Atan, S. L. M. Hassan, y M. Alghrairi, «Identification of Distributed Denial of Services Anomalies by Using Combination of Entropy and Sequential Probabilities Ratio Test Methods», Sensors (Basel), vol. 21, n.o 19, p. 6453, sep. 2021, doi: 10.3390/s21196453.

G. Lally y D. Sgandurra, «Towards a Framework for Testing the Security of IoT Devices Consistently», en Emerging Technologies for Authorization and Authentication, A. Saracino y P. Mori, Eds., en Lecture Notes in Computer Science. Cham: Springer International Publishing, 2018, pp. 88-102. doi: 10.1007/978-3-030-04372-8_8.

E. Ahmed, A. Islam, M. Ashraf, A. I. Chowdhury, y M. M. Rahman, «Internet of Things (IoT): Vulnerabilities, Security Concerns and Things to Consider», en 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India: IEEE, jul. 2020, pp. 1-6. doi: 10.1109/ICCCNT49239.2020.9225283.

A. Chorti et al., «Context-Aware Security for 6G Wireless: The Role of Physical Layer Security», IEEE Communications Standards Magazine, vol. 6, n.o 1, pp. 102-108, mar. 2022, doi: 10.1109/MCOMSTD.0001.2000082.

J. Nivedita, «Cybersecurity Statistics: Updated Report 2023», 19 de diciembre de 2022. https://www.getastra.com/blog/security-audit/cyber-security-statistics/ (accedido 22 de mayo de 2023).

M. Ahlgren, «Estadísticas, tendencias y hechos de ciberseguridad que importan para 2022», Website Rating, 11 de diciembre de 2022. https://www.websiterating.com/es/research/cybersecurity-statistics-facts/ (accedido 16 de diciembre de 2022).

Verizon Business, «2021 DBIR Master's Guide», Verizon Business, 2021. https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (accedido 16 de diciembre de 2022).

M. Rosenthal, «Phishing Statistics (Updated 2022) - 50+ Important Phishing Stats», Tessian, 12 de enero de 2022. https://www.tessian.com/blog/phishing-statistics-2020/ (accedido 16 de diciembre de 2022).

P. Muncaster, «One Ransomware Victim Every 10 Seconds in 2020», Infosecurity Magazine, 25 de febrero de 2021. https://www.infosecurity-magazine.com/news/one-ransomware-victim-every-10/ (accedido 16 de diciembre de 2022).

S. Morgan, «Cybercrime To Cost The World $10.5 Trillion Annually By 2025», Cybercrime Magazine, 2021. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (accedido 16 de diciembre de 2022).

Purplesec, «2022 Cyber Security Statistics Trends & Data», PurpleSec, 2022. https://purplesec.us/resources/cyber-security-statistics/ (accedido 16 de diciembre de 2022).

F. Gómez, «Las diez predicciones de ciberseguridad para 2023», Forbes Ecuador, 2022. https://www.forbes.com.ec/innovacion/las-diez-predicciones-ciberseguridad-2023-n26513 (accedido 7 de enero de 2023).

M. Henriquez, «18 cybersecurity predictions for 2023», Security Magazine, 2022. Accedido: 6 de enero de 2023. [En línea]. Disponible en: https://www.securitymagazine.com/articles/98729-18-cybersecurity-predictions-for-2023

J. France, «(ISC)2 CISO: We aim to lower the barrier to entry in cybersecurity», Silicon Republic, 29 de abril de 2022. https://www.siliconrepublic.com/enterprise/isc2-cybersecurity-infosec-ciso-skills (accedido 6 de enero de 2023).

M. Adams, «2023 Cybersecurity Predictions from Zoom CISO Michael Adams», CRN - India, 8 de diciembre de 2022. Accedido: 6 de enero de 2023. [En línea]. Disponible en: https://www.crn.in/news/2023-cybersecurity-predictions-from-zoom-ciso-michael-adams/

M. Aalto, «How Does Employee Security Engagement Training Transform Your Defense Strategy?», Cybercrime Magazine, 31 de marzo de 2020. Accedido: 6 de enero de 2023. [En línea]. Disponible en: https://cybersecurityventures.com/how-does-employee-security-engagement-training-transform-your-defense-strategy/

E. J. Guaña Moya, M. Chiluisa Chiluisa, P. del C. Jaramillo Flores, D. Naranjo Villota, y E. R. Mora Zambrano, «ATAQUES DE PHISHING Y CÓMO PREVENIRLOS», jul. 2022, Accedido: 21 de mayo de 2023. [En línea]. Disponible en: http://190.57.147.202:90/xmlui/handle/123456789/3361

J. Carson, «2022: The year in review and cybersecurity trends», Delinea, 2022. https://delinea.com/blog/cybersecurity-trends (accedido 6 de enero de 2023).

S. Akter, M. R. Uddin, S. Sajib, W. J. T. Lee, K. Michael, y M. A. Hossain, «Reconceptualizing cybersecurity awareness capability in the data-driven digital economy», Ann Oper Res, ago. 2022, doi: 10.1007/s10479-022-04844-8.

S. Weigand, «2023 tech predictions: AI and machine learning will come into their own for security», SC Media, 30 de diciembre de 2022. https://www.scmagazine.com/feature/emerging-technology/2023-tech-predictions-ai-and-machine-learning-wicome-into-their-own-for-security (accedido 6 de enero de 2023).

K. Worstell, «2023 Cybersecurity Predictions: Cyber Risk Management Will Be a Top Priority for Business Leaders», Enterprise Sec Tech, 8 de diciembre de 2022. https://www.enterprisesecuritytech.com/post/2023-cybersecurity-predictions-cyber-risk-management-will-be-a-top-priority-for-business-leaders (accedido 6 de enero de 2023).

A. P. Singh, «Future of AI and Machine Learning in Cybersecurity», Analytics Vidhya, 1 de febrero de 2023. https://www.analyticsvidhya.com/blog/2023/02/future-of-ai-and-machine-learning-in-cybersecurity/ (accedido 21 de mayo de 2023).

Infopulse GmbH, «What is the future of data privacy and data protection», Infopulse SCM, 7 de diciembre de 2022. https://compliance-aspekte.de/en/articles/main-data-privacy-trends-to-watch-in-2022-2025/ (accedido 21 de mayo de 2023).

CITAR ESTE ARTICULO:

Coronel Ayala, F. M., & López Sevilla, G. M. (2023). Mapeo del panorama actual de la ciberseguridad en la era moderna digital. RECIMUNDO, 7(2), 441-452. https://doi.org/10.26820/recimundo/7.(2).jun.2023.441-452