22(4): 275-282, 2019

SCIÉNDO

Problemática en Ciberseguridad como protección de sistemas informáticos y redes sociales en el Perú y en el Mundo

Problematic in cybersecurity as protection of computer system and social networks in Peru and the World

Alexis Enrique Poma Vargas*; Raquel Lucía Vargas Vásquez

AT Poma Vargas, Mz 2 lote 2. Urb. Los Jardines del Golf. Distrito de Víctor Larco. Trujillo-Perú.

*Autor correspondiente: **alexisepoma@gmail.com** (A. Poma).

Fecha de recepción: 15 09 2019. Fecha de aceptación: 18 11 2019.

RESUMEN

El presente trabajo tiene por objetivo investigar si la Ciberseguridad protege los sistemas informáticos y redes sociales en el Perú y el mundo, puesto que existen lugares tales como empresas y entidades propensas a todo tipo de ataques cibernéticos realizados por hackers, quienes sustraen información valiosa de estas. Dicha investigación es cuantitativa, de diseño no experimental y descriptivo. Basada en análisis documentario, por lo que se buscó información local, nacional e internacional de fuentes confiables, que pudiesen aportar alcances estadísticos y casos de protección a medios informáticos, a fin de proporcionar conocimientos sobre vulnerabilidad de sistemas por no contar con los recursos que permitan salvaguardar datos reservados, así como, las soluciones respectivas al caso. Los resultados fueron favorables, en el sentido que se pudo apreciar que, mediante la adopción de medidas rígidas, los sistemas informáticos; así como las redes sociales, se vuelven potencialmente seguros en un 70%. En tal sentido se concluye que la Ciberseguridad como protección de medios informáticos potencializa las buenas prácticas en las empresas y protege la información.

Palabras clave: Ciberseguridad; protección; informática.

ABSTRACT

The purpose of this work is to investigate whether Cybersecurity protects computer systems and social networks in Peru and the world, since there are places such as companies and entities prone to all types of cyber attacks by hackers, who subtract valuable information from these. This research is quantitative, non-experimental and descriptive design. Based on documentary analysis, for which local, national and international information from reliable sources was sought, which could provide statistical scopes and cases of protection to computer means, in order to provide knowledge about system vulnerability because they do not have the resources that allow safeguard reserved data, as well as, the respective solutions to the case. The results were favorable, in the sense that it could be seen that, through the adoption of rigid measures, the computer systems; as well as social networks, they become potentially safe by 70%. In this sense, it is concluded that Cybersecurity as a protection of computer means enhances good practices in companies and protects information.

Keywords: Cybersecurity; protection; computing.

DOI: http://dx.doi.org/10.17268/sciendo.2019.034

INTRODUCCIÓN

Las personas vinculadas a la sociedad del conocimiento, la comunicación y la informática en la actualidad, es vulnerable a ataques virtuales con mucha frecuencia, por lo que ignoran como debe ser la postura adecuada para enfrentar estos actos, que suelen en algunos casos muy complejo evitarlos.

Al respecto, las empresas y entidades son el centro de todo ataque cibernético, debido a que en muchos casos los trabajadores son quienes ingresan a sistemas informáticos y redes sociales, siendo muchas veces presas de los virus informáticos o de información no apropiada para ellos, y en otras ocasiones han proporcionado datos privados siendo participes de violaciones a su integridad física y moral; así como, del hurto agravado de información reservada de la empresa.

La ciberseguridad es una herramienta que permite en muchos casos evitar ser víctima de proporcionar información privada de la persona, evitando en todo caso que personas ajenas se apropien de la identidad de usuario para fines inapropiados, como pornografía, violación intima, robos, extorciones, entre otros.

Los sistemas informáticos son vulnerables los ataques cibernéticos elaborados por hackers, en cuanto la protección no sea la correcta para dichos dispositivos, tal es el caso de virus como virus básicos, troyanos, Gusanos, Spyware, Rogueware, Ransomware, Keylogger entre otros.

Es por ello que, Poggy (2019) y Gestión (2019) indican que se necesita repotenciar a las Tecnologías para luchar contra los ataques masivos.

Un ejemplo de ellos son las organizaciones gubernamentales y empresas financieras quienes han sido el objetivo principal de muchos ciberataques, en particular los perpetrados en nombre del hacktivismo. Sin embargo, debido a lo fácil que es tener una infraestructura débil con una internet abierta, permite que las instituciones sean fáciles de que cualquier persona, pueda realizar un ciberataque, debido a que no hay implementación en el sector público de soportes que permitan contrarrestar a los inescrupulosos que intentan violentar la privacidad de los trabajadores.

Cualquier persona con habilidades básicas necesarias puede realizar un ciberataque, puede utilizar un software malicioso e introducirse en los sistemas operativos, con lo cual conseguiría hacerse se los Backus. Por lo tanto, la Ciberseguridad se convierte en una prioridad para cualquier empresa que disponga de activos digitales valiosos y esté presente en Internet (Akamai, 2019).

Según Kaspersky (2019), en el 2019, Perú se encuentra ubicado en el puesto número 40, como país más vulnerable a ataques cibernéticos, asimismo, El Peruano (2019) indicó que la explotación de vulnerabilidades es uno de los métodos más comunes que utilizan los ciberdelincuentes para atacar a sus víctimas.

ISACA (2012) indica que, en relación al tema de ciberseguridad, el COBIT 5, como cascada de metas es importante porque prioriza la implementación, se encarga de la mejora y también del aseguramiento del gobierno de las tecnologías de la información y comunicación (TI) de la entidad, que se basa en metas corporativas (estratégicas) de la empresa; asimismo, el riesgo relacionado. En la práctica, dicha cascada de metas, se define como los objetivos y metas relevantes y sensibles a varios niveles de responsabilidad; además, filtra la base de conocimiento de COBIT 5, sobre la base de las metas corporativas, para extraer las guías relevantes con la finalidad de incluir proyectos específicos de implementación, mejora o aseguramiento; asimismo, localiza claramente y comunica cómo los catalizadores son importantes para alcanzar metas de la institución.

Freire y Lenin (2017) indican que la transcendencia de la Ciberseguridad para el diseño de políticas de seguridad de la información es limitada, a pesar de la reciente introducción del Sistema de Gestión de Seguridad de la Información de la Armada del Ecuador. Lo cual constituye un llamado a la elaboración y el establecimiento de La ciberseguridad, y su incidencia en las políticas de la seguridad de la información de la Armada del Ecuador. Asimismo, Anchundia (2017), señala que el impacto de la globalización que va acompañando la creciente implantación de las tecnologías, están trayendo grandes beneficios a organizaciones y empresas de toda índole, pero a la vez están produciendo grandes problemas de seguridad y de

DOI: http://dx.doi.org/10.17268/sciendo.2019.034

protección de datos y privacidad con los cuales las organizaciones tendrán que enfrentarse. También, Machín y Gazapo (2016), explican que la realidad ha demostrado que la combinación de ciberataques con ataques físicos tradicionales puede ser la fórmula perfecta para paralizar completamente las infraestructuras críticas de un país. Los ejemplos del virus Stuxnet, el virus Flame o los (ciber) enfrentamientos entre Estonia y Rusia ponen de relieve que los ciberataques son armas sumamente dañinas; además, eficaces, puesto que requieren pocos recursos en comparación con su ilimitada capacidad de destrucción.

El problema radica en que, en muchos lugares del mundo, existen especialistas en informática dedicados al hurto de información conocidos como hackers, quienes, manipulando virus informáticos, consiguen apropiarse ilícitamente de información de carácter reservado. En ese sentido, ¿De qué manera la Ciberseguridad protegerá los sistemas informáticos y las redes sociales en el Perú y el mundo?; a lo que según expertos en la informática como la CGR (2019), explican como la Gestión de incidentes, tendría posibles efectos: Evento de seguridad de la información, donde la ocurrencia identificada en el estado de un sistema, servicio o red, indica una posible violación de la seguridad de la información, política o falta de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

En el caso del Incidente de seguridad de la información, es indicado por un único o una serie de eventos de seguridad de la información indeseable o inesperada, que tiene una probabilidad significativa de comprometer las operaciones de negocios y de amenazar la seguridad de la información.

Según Andina (2018) indicó que Elder Cama, socio de consultoría de EY Perú, afirmó que solo el 9% de las empresas peruanas consideran que están aptas para detectar un ciberataque a tiempo.

Eso quiere decir que, las entidades tienen la guardia baja, por lo que, el atacante entra a la red, evalúa por semanas o hasta un año, el movimiento de la empresa. En ese sentido, hay que vigilar comportamientos raros, por ejemplo, archivos que no se encontraban previamente en una carpeta. Así también, considerarse el hecho de no pagar al ciberdelincuente a fin de recuperar la información, la cual ha sido secuestrada de las instalaciones de la empresa. Asimismo, indico que según EY Perú, el 6% de las empresas incrementarán su presupuesto de ciberseguridad en 25%. Sin embargo, la falta de cultura de prevención suele ser el mayor problema que enfrenta una compañía en el Perú.

El objetivo del presente estudio es investigar si la Ciberseguridad protege los sistemas informáticos y redes sociales en el Perú y el mundo.

MATERIAL Y MÉTODOS

Los estudios descriptivos son útiles para analizar cómo es y cómo se manifiesta un fenómeno y sus componentes. Se revisó material documentario y bibliográfico de fuentes fidedignas como revistas, periódicos digitales y reportes anuales. Asimismo, se utilizó la ficha electrónica lecturas, para extraer resúmenes de las citadas fuentes, relacionadas al tema de ciberseguridad.

Se contó con la información proporcionada por la web de Kaspersky (2019), quien cuenta con datos actualizados a la primera semana de setiembre del 2019.

RESULTADOS Y DISCUSIÓN

De los resultados obtenidos de Kaspersky (2019), se puede apreciar que a nivel mundial los países afectados mayormente por diversos ataques cibernéticos a sistemas informáticos y redes sociales son los siguientes:

Tabla 1
Ciberamenaza Mundial al 7 de setiembre de 2019 en cuanto a infecciones locales

Puesto	País	Porcentaje
1	República del Congo	19,86%
2	Yemen	18,71%
3	Kirguistán	18,66%
4	Tayikistán	18,44%
5	Uzbekistán	18,16%
6	Camerún	18,12%
7	Guinea Ecuatorial	17,58%
8	Birmania	17,09%

Fuente: Kaspersky (2019).

Del ranking mundial de los ocho (8) países más atacados por medios virtuales a sus sistemas informáticos, se puede verificar que la República del Congo es quien ocupa el primer lugar por infecciones locales con un 19,86% (Tabla 1). Al

respecto, esto es corroborado por Kapersky (2019) y Akamai (2019), quienes afirman que esto se debe a que existes pocos expertos, capaces de hacer frente a los ataques de hackers a nivel mundial.

Tabla 2
Ciberamenaza Mundial al 7 de setiembre de 2019 en cuanto a Amenaza web

Puesto	País	Porcentaje
1	Albania	13,99%
2	Túnez	13,23%
3	Argelia	12,35%
4	Nepal	12,19%
5	Yibuti	11,01%
6	Filipinas	10,58%
7	Birmania	10,01%
8	Libia	9,80%

Fuente: Kaspersky (2019).

Del ranking mundial de los ocho (8) países más atacados por medios virtuales a sus sistemas informáticos, se puede verificar que Albania es quien ocupa el primer lugar por Amenaza web con un 13,99% (Tabla 2).Es de precisar que, Poggy (2019), hace de conocimiento que Albania y Túnez son países que su debilidad radica en los direccionamientos de páginas web, es decir que no están completamente protegidos por softwares que permitan bloquear paginas indebidas, y por consiguiente están propensos a los ataques.

Tabla 3
Ciberamenaza Mundial al 7 de setiembre de 2019 en cuanto a Análisis por pedido

Puesto	País	Porcentaje
1	Guinea Ecuatorial	22,46%
2	Mongolia	21,15%
3	República del Congo	20,73%
4	Yemen	20,59%
5	Algeria	20,55%
6	Ruanda	20,22%
7	Tayikistán	20,18%
8	Nepal	20,08%

Fuente: Kaspersky (2019).

Del ranking mundial, mostrado en la tabla 3, de los ocho (8) países más atacados por medios virtuales a sus sistemas informáticos, se puede verificar que Guinea Ecuatorial es quien ocupa el primer lugar por Análisis de pedido con un 22,46%.
Anchundia (2019) afirma que esto se puede apreciar, en el contexto de que se utilizase un antivirus potente, ya que el usuario se podrá dar cuenta de cuantas amenazas se han producido en el tiempo, debido a las grandes descargas de información de páginas dudosas que se realizan por internet.

Tabla 4
Ciberamenaza Mundial al 7 de setiembre de 2019 en cuanto a Ataque de redes

Puesto	País	Porcentaje
1	Etiopia	18,02%
2	Irán	14,03%
3	Costa Rica	14,12%
4	China	13,29%
5	Pakistán	12,12%
6	Indonesia	11,63%
7	Sudan	11,36%
8	Bangladés	10,93%

Fuente: Kaspersky (2019).

En la tabla 4, del ranking mundial de los ocho (8) países más atacados por medios virtuales a sus sistemas informáticos, se puede verificar que Etiopia es quien ocupa el primer lugar por Ataque de redes con un 18,02%. Según Freire Y Lenin (2019) las redes sociales son muy atacadas frecuentemente en Etiopia; es el caso de personas inescrupulosas que envían mensajes con la finalidad de ser aceptadas en las amistades de las víctimas, dando por hecho que si aceptan están invitaciones, pueden ser vulnerables ante cualquier virus o robo de información.

Tabla 5
Ciberamenaza Mundial al 7 de setiembre de 2019 en cuanto a Basura

Puesto	País	Porcentaje
1	China	18,25%
2	Estados Unidos de América	13,26%
3	Brasil	4,94%
4	Rusia	4,88%
5	Turquía	3,04%
6	Alemania	3,03%
7	India	2,60%
8	Singapur	2,08%

Fuente: Kaspersky (2019).

Del ranking mundial de los ocho (8) países más atacados por medios virtuales a sus sistemas informáticos, se puede verificar que China es quien ocupa el primer lugar por Basura con un 18,25% (Tabla 5). Son elementos acumulables en los emails, como los spams que diariamente se remiten con la intensión de saturar el correo de la víctima. Es en ese caso que, al existir mayor número de cibernautas en China, mayor serán los elementos basuras que se acumulen si no se toman las medidas del caso, para identificar qué tipo de información es la que el usuario a diario usa, o recibe. (Akamai, 2019).

Tabla 6
Ciberamenaza Mundial al 7 de setiembre de 2019 en cuanto a Botnet

Puesto	País	Cantidades
1	China	6584
2	Estados Unidos de América	1867
3	South África	230
4	Corea del Sur	107
5	Reino Unido	70
6	Holanda	26
7	Canadá	17
8	Alemania	15

Fuente: Kaspersky (2019).

Del ranking mundial de los ocho (8) países más atacados por medios virtuales a sus sistemas informáticos, se puede verificar que China es quien ocupa el primer lugar por Botnet con 6584 unidades. Machín y Gazapo (2016) hacen un interesante análisis, dando a entender que este programa malicioso tuvo su ingreso a partir del año 2000, iniciando un ataque de negación de servicio desde Canadá contra páginas web. Al respecto, debido a la gran abundancia de personas que utilizan páginas web en China, son vulnerables a este tipo de programa, el cual realiza conflictos y sobrecargas en las redes.

Tabla 7
Ciberamenaza Mundial al 7 de setiembre de 2019 en cuanto a Correo Infectado

Puesto	País	Cantidades
1	Fiyi	4,47%
2	Mónaco	3,53%
3	Grecia	2,96%
4	Moldova	2,89%
5	Emiratos Árabes	2,67%
6	Montenegro	2,41%
7	Catar	2,37%
8	Chipre	2,14%

Fuente: Kaspersky (2019).

Del ranking mundial de los ocho (8) países más atacados por medios virtuales a sus sistemas informáticos, se puede verificar que Fiyi es quien ocupa el primer lugar por Correos Infectados con un 4,47%. Según Isaka (2012) generalmente los correos infectados son aquellos que tienen malware y los cuales pueden provocar alteraciones en los sistemas informáticos como el caso de robo de contraseñas.
Del ranking mundial de los ocho (8) países más atacados por medios virtuales a sus sistemas informáticos, se puede verificar que Las Bahamas es quien ocupa el primer lugar en Vulnerabilidad con un 1,08%.

Tabla 8
Ciberamenaza Mundial al 7 de setiembre de 2019 en cuanto a Vulnerabilidad

Puesto	País	Cantidades
1	Las Bahamas	1,08%
2	Guinea-Bisau	0,74%
3	Estados Unidos de América	0,70%
4	República del Congo	0,68%
5	Canadá	0,63%
6	Australia	0,60%
7	Alemania	0,57%
8	España	0,53%

Fuente: Kaspersky (2019).

En el 2019, Perú se ubica en el puesto número 40 a nivel mundial, como uno de los países más vulnerable a ataques cibernéticos (Tabla 9).
La vulnerabilidad se detecta por la falta de controles; es decir que existen diversidad de riesgos en los sistemas informáticos. Las Bahamas, según Kapersky (2019) es un lugar que sufre los ataques cibernéticos de manera frecuente y cuyos sistemas en cada momento tiene que ser actualizado; puesto que se necesita de buenos soportes y detectores de software maliciosos, a fin de evitar que estos ingresen a las máquinas y se apropien de información confidencial.
Al respecto, las normas Cobit son herramientas que sirven para realizar controles informáticos y a la vez permite que las auditorias informáticas ejecuten un registro completo de las causas que originaron los hechos maliciosos, permitiendo de eso modo realizar las recomendaciones necesarias para realizar la toma de medidas correctivas.

Tabla 9
Ciberamenazas en Perú al 31 de agosto de 2019

N°	Ciberamenaza	Parasito	Porcentaje/ cantidad
1	Infecciones locales	Trojan WinLink Agent gen	11,85%
2	Amenaza web	Trojan Script Miner gen	43,60%
3	Análisis por pedido	Trojan multi agent gen	7,81%
4	Ataque de redes	Intrusion Win Ms 17 010	9,06%
5	Basura	Análysis of Sender Attributes	58,65%
6	Botnet	No hay datos	0,00%
7	Correo infectado	Trojan HTML Fraud gen	22,32%
8	Vulnerabilidad	Exploit win32 Shadowbrockers ae	12,59%

Fuente: Kaspersky (2019).

DOI: http://dx.doi.org/10.17268/sciendo.2019.034

Las empresas y entidades son quienes más sufren atentados por parte de los hackers, y, por consiguiente, se corrobora lo indicado por Freire y Lenin (2017) y Anchundia (2017) quienes sostiene que los sistemas informáticos y redes sociales son vulnerables en la medida que no se tenga un resguardo de los equipos y un conocimiento rígido de resguardar la información.
En ese sentido, los ataques más significativos, según la tabla 9 son por causa de Basura con 58,65%, Amenazas web con un 43,60% y correos infectados en un 22,32%; siendo los virus o parásitos digitales más comunes Análysis of Sender Attributes, Trojan Script Miner gen y Trojan HTML Fraud gen, respectivamente.

En cuanto a ciberseguridad, Perú cuenta con debilidades como en tecnologías, por cuanto sus sistemas necesitan estar en constante actualización, es más, de acuerdo a las normas de control aprobadas en el año 2006, en la sección de tecnologías, a propuestas de la CGR (2019), establece que debe fortalecerse todo tipo de herramienta TIC y de este modo evitar la existencias de riesgos; es por ello que, los ingenieros de sistemas deben estar atentos ante cualquier tipo de amenaza cibernética en las instituciones.

Tabla 10
Ataques de ransomware (secuestro de datos) en Latinoamérica en el 2017

Nª	Prioridades	Porcentaje
1	Perú	25,10%
2	México	19,60%
3	Argentina	14,50%
4	Brasil	14,00%
5	Colombia	9,60%
6	Chile	5,70%
7	Ecuador	4,60%
8	Venezuela	3,20%

Fuente: Andina (2018).

Andina (2018) indicó que, Perú ha sido en el 2017, el país más atacado de Latinoamérica en robo de información, denominado secuestro de datos o ransomware, tal como se muestra en la tabla 10.
Según Gestión (2019) esta modalidad maliciosa, se encarga de secuestrar datos informáticos de mucha importancia y luego el hacker pide rescate por ello. En ese sentido cuando estos malos eventos ocurren, es necesario no hacer caso, para no caer en trampas de personas inescrupulosas. Si la información ya fue tomada del ordenador, no se puede permitir que el hacker tenga acceso a más de esta y se recomienda buscar la mejor manera de proteger los datos, y sobretodo evitar en todo momento caer ante sus pedidos de rescate.

Tabla 11
Ataques cibernéticos en América Latina en el periodo 2018

Nª	Prioridades	Porcentaje
1	México	23,00%
2	Perú	14,00%
3	Brasil	12,00%

Fuente: El Peruano (2019).

Según el Peruano (2019), se ha registrado en América Latina a finales del periodo 2018, ataques cibernéticos, siendo los países más afectados por esta vulnerabilidad: México (23,00%), Perú (14,00%) y Brasil (12,00%), tal como se muestra en la tabla 11.
Las estrategias más efectivas según Poggy (2019) para proteger los sistemas informáticos y que tengan efectos positivos ante cualquier ataque cibernético por parte de virus, son las siguientes: Seguridad informática (Tabla 12) y Cuidados con sistemas informáticos (Tabla 13).

Tabla 12
Estrategias de la Ciberseguridad (Seguridad informática) en el mundo, periodo 2019

N°	Soluciones/Estrategia
1	70,00% de las organizaciones cree que su riesgo de seguridad creció considerablemente en el 2017.
2	Se estima que para el 2020, el número de contraseñas utilizadas crecerá a 300 billones.
3	Mantenerse actualizado acerca de las últimas amenazas.
4	Invertir en seguridad y estar un paso delante de los atacantes.

Fuente: Poggy (2019).

Al respecto, Machín y Gazapo (2016) confirman que la vulnerabilidad de la tecnología se manifiesta en el sentido de que, si no se efectúa una restricción de ciertos parámetros de accesos a información reservada, es posible que exista hurto o apropiación ilícita de dichos datos. Asimismo, CGR (2019) alcanza propuestas que podrían resguardar la información y de esa manera evitar la posible infiltración de posibles agentes patógenos virtuales, dando soluciones en el caso de ciberseguridad, tal como se muestra en la tabla 13:

Tabla 13
Soluciones al problema en Ciberseguridad (Cuidados con sistemas informáticos) en Perú en el periodo 2019

N°	Soluciones
1	Normas para la conducta y desempeño del personal.
2	Documentos de identificación, cuyo uso es personal, intransferible y obligatorio.
3	Informar oportunamente a quien corresponda sobre situaciones o acciones.
4	Asignación, acceso, uso y revocación de los recursos informáticos.
5	No usar software ajeno a la institución para acceder a información no autorizada.
6	No hacer mal uso de los códigos para acceder a información no autorizada.
7	No realizar declaraciones públicas o a través de medios de difusión o comunicación.
8	Cuidar y dar uso apropiado a los equipos y bienes bajo su responsabilidad o custodia.
9	Desconectar o apagar las maquinas, equipos y fluido eléctrico al término de su jornada diaria.
10	El personal que maneja información clasificada como secreta, reservada y confidencial, asume el compromiso de no divulgar la información durante y después del ejercicio de sus funciones.
11	Se encuentra prohibido almacenar información clasificada en computadoras, unidades de almacenamiento u otros dispositivos que no sean de la entidad.
12	No brindar información restringida sin autorización previa, a quienes efectúen solicitudes vía Messenger o whassaps.
13	Las contraseñas para el acceso a las computadoras o sistemas informáticos deben ser utilizadas con reserva.
14	El personal que por la naturaleza de su función maneja información de accesos restringido, asume la responsabilidad de cautelar el acceso a la misma.

Fuente: CGR (2019).

En relación a la citada información, ISACA (2012) y Akamai (2019) sostienen que la mejor manera de combatir los ataques cibernéticos es basarse en el COBIT 5, que es una herramienta fundamental para aplicar estrategias de prevención de dispositivos informáticos, como el caso sistemas informáticos y redes sociales; así como, la seguridad de información digital.

Tabla 14
Prioridades en Ciberseguridad en Perú, periodo 2018

Nª	Prioridades	Porcentaje
1	Educación	67,00%
2	Identificación digital	78,00%
3	Lucha contra el cibercrimen	78,00%
4	Requiere mejorar el nivel de respuesta en tiempo real	59,00%

Fuente: Andina (2018).

Según la tabla 14, los porcentajes establecidos por prioridades en la lucha contra ciberataques teniendo en cuenta a: Lucha contra el cibercrimen, Identificación digital, Educación; así también, se consideró que se Requiere mejorar el nivel de respuesta en tiempo real

Como lo indica Andina (2018), existe un peligro latente en las empresas, puesto que están propensas a percibir y ser atacadas en cualquier momento por ciberdelincuentes, que con ayuda de sus softwares de hackeo, pueden irrumpir en la entidad y extraer sin ningún problema la información reservada.

Viendo esta situación, es que tanto el Perú como los países de mundo tienen que aplicar estrategias certeras que impidan este tipo de actos que puedan perjudicar la seguridad nacional.

CONCLUSIONES

Existen países en el mundo con mayor número de ataques cibernéticos, tales como República del Congo, Albania, Guinea Ecuatorial, Etiopia, China, Fiyi y Las Bahamas.

En Latinoamérica, Perú ocupa el primer lugar en Latinoamérica para el 2017, como país vulnerable a ataques cibernéticos con un 25,10% y para el 2018 con un segundo lugar con un 14% de vulnerabilidad.

En el 2019, Perú se ubica a nivel mundial, en el puesto número 40, como uno de los países afectados por los ataques cibernéticos, siendo las principales causas de dichos ataques por Basura en un 58,65%, Amenaza web en un 43,60% y Correo Infectado en un 22,32%.

Se indagó que las empresas y entidades peruanas generalmente son atacadas por virus informáticos como: Análysis of Sender Attributes, Trojan Script Miner gen y Trojan HTML Fraud gen.

Se averiguó que el 70% de las organizaciones cree que su riesgo de seguridad creció considerablemente en el 2017, lo que se presume que los sistemas informativos y redes sociales son potencialmente seguro.

Se obtuvo información referente a soluciones para mejorar el sistema de ciberseguridad proporcionada por la CGR, las cuales son descritas en el presente artículo.

Se recomienda tomar en consideración el presente artículo para futuras investigaciones relacionadas a Ciberseguridad y Tecnologías.

DOI: http://dx.doi.org/10.17268/sciendo.2019.034

REFERENCIAS BIBLIOGRÁFICAS

Poggy, N. 2019. 24 Estadísticas de Seguridad Informática que Importan en el 2019. Disponible en: https://preyproject.com/blog/es/24-estadisticas-seguridad-informatica-2019/

Akamai .2019.Ciberataques.Disponible en: https://www.akamai.com/es/es/resources/cyber-attacks.jsp

Kaspersky. 2019. Cibernamenaza en tiempo real. Disponible en: https://cybermap.kaspersky.com/es

El Peruano. 2019. Ciberataques en crecimiento. Disponible en: https://elperuano.pe/noticia-ciberataques-crecimiento-74748.aspx

ISACA .2012. Cobit 5. Evento Técnico 3 de Mayo de 2012. pp. 1-46.

Freire, A.; Lenin, A. 2017. La ciberseguridad, y su incidencia en las políticas de la seguridad de la información de la Armada del Ecuador. Yura: Relaciones internacionales 11: 306 – 323.

Anchundia, C. 2017. Ciberseguridad en los sistemas de información de las universidades. Dom. Cien 3: 200-217.

Machín, N.; Gazapo, M. 2016. La Ciberseguridad como factor crítico en la Seguridad De La Unión Europea. UNISCI / UNISCI Journal 42: 47-68.

CGR. 2019. Seguridad de la Información. Contraloría General de La Republica. pp 1-17.

Andina. 2018. ¿Cuáles son los ciberataques más comunes en el Perú? Disponible en: https://portal.andina.pe/edpespeciales/2018/ciberataques-peru/index.html

Gestión 2019. Radiohead responde a hackers: libera sesiones robadas de música inédita. Disponible en https://gestion.pe/tecnologia/radiohead-responde-hackers-libera-sesiones-robadas-musica-inedita-269828-noticia/