[[1]](#footnote-1)

Desarrollo de estrategias que ayuden a fomentar la cultura de la población en ciberseguridad

Sarah Hernández Serrano, Ingeniería en Tecnologías de la Información y la Comunicación

*Abstracto*—Al decir que un sistema informático es vulnerable, significa que está susceptible ante posibles ataques. Para una empresa es muy importante que sus redes y sistemas operen con seguridad pues la información que ellos manejan es de enorme valor.

Empresas como lo es Microsoft Corporation, disponen de departamentos dedicados exclusivamente a la seguridad, como el Microsoft Security Response Center (MSRC).

Entre sus funciones son evaluar los informes que los clientes proporcionan sobre posibles vulnerabilidades en sus productos, preparar y divulgar revisiones y boletines de seguridad informática.

Los 3 elementos para proteger en cualquier sistema informático son: el software, hardware y por supuesto, los datos siendo los más amenazados y difíciles de recuperar [1].

Hay muchas situaciones que nos han llevado a ser vulnerables y por tanto que exista amenaza. Entre ellas está el incremento de la "ingeniería social" y la falta de capacitación y conocimiento respecto al uso de la tecnología.

*Índice de términos*— ciberseguridad: se enfoca principalmente en la información en formato digital y los sistemas interconectados que la procesan, almacenan o transmiten, por lo que tiene un mayor acercamiento con la seguridad informática.

Seguridad de la información: se sustenta de metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnología y otros elementos, que soportan la idea de protección en las distintas facetas de la información

# Introducción

L

as actividades que se realizan en el espacio cibernético también tienen impacto en el mundo físico, por lo que resulta de gran importancia contar con materia y conocimientos referentes a la ciberseguridad con diversos objetivos: impulsar la innovación tecnológica y económica, fortalecer instituciones públicas y el respeto a los derechos humanos.

Meterse con la información ajena es una violación de los derechos que como humanos tenemos.

La expansión de Internet y del uso de las tecnologías de la información y la comunicación (TIC) durante los últimos años permite, como nunca antes, la circulación de grandes cantidades de información y también establecer comunicaciones de manera fácil. Cada vez en mayor medida las actividades sociales, económicas y hasta militares de un Estado se hacen más dependientes del uso de estas tecnologías, lo que implica a su vez una mayor vulnerabilidad y exposición a ciberataques.

Es esencial mantener tu computadora segura para proteger tu privacidad, reducir el riesgo del robo de identidad y evitar que los hackers controlen tu computadora.

Desafortunadamente, no siempre es fácil proteger tu computadora. Los hackers con frecuencia parecen estar un paso más adelante del público, incluso de las personas que utilizan los mejores métodos de seguridad.

Para proteger tu privacidad e información sensitiva es necesario tomar varias medidas, incluyendo prevenir, detectar y responder a una gran variedad de ataques. Hay muchos riesgos, y unos son más serios que otros. Algunos de los peligros son:

• Virus que infectan todo tu sistema.

• Personas que entran a tu sistema y hacen modificaciones a tus archivos.

• Hackers que usan tu computadora para atacar a otros.

Ladrones que roban tu computadora y tu información personal.

# Marco teórico

Cada gobierno debe tener la preocupación de brindar a la población un espacio de seguridad aún en el ámbito informático, porque como ya vimos, lo que sucede en el mundo cibernético trae repercusiones en el mundo real; ejemplo de esto es el Titan Rain [2].

## Estrategia Nacional de ciberseguridad

En México, el Gobierno de la República, promovió espacios de diálogo, discusión y aprendizaje mediante foros y talleres en un proceso de colaboración denominado “Hacia una Estrategia Nacional de Ciberseguridad” de marzo a octubre de 2017. En estos espacios, los distintos actores de la sociedad compartieron ideas, inquietudes y propuestas en materia de ciberseguridad que arrojaron grandes coincidencias sobre las necesidades que debía atender la Estrategia, ​ ​tales​ ​como:

● Que la ENCS articule el desarrollo de las acciones de ciberseguridad que sirvan a individuos, ​empresas​ ​e​ ​instituciones​ ​públicas​ ​del​ ​Estado​ ​mexicano.

● Colaboración y cooperación entre los diferentes sectores como pieza clave para el desarrollo, ​ ​seguimiento​ ​y​ ​evaluación​ ​de​ ​la​ ​Estrategia.

● Conocer la dimensión de los riesgos y amenazas en el ciberespacio, el estado que guarda la ciberseguridad en el país, la construcción de un diagnóstico nacional, así como obtener evidencia para mejorar la toma de decisiones en materia de ciberseguridad.

● Contemplar el escenario global como parte de la problemática y la diplomacia como vía para entablar diálogos y acuerdos que permitan hacer frente a los riesgos, amenazas​ ​y​ ​ciberdelitos.

● Desarrollar​ ​capital​ ​humano​ ​especializado​ ​en​ ​materia​ ​de​ ​ciberseguridad.

●Promover el uso responsable de las TIC y reforzar una cultura de ciberseguridad que contemple​ ​acciones​ ​de​ ​concientización, ​ ​educación​ ​y​ ​formación.

El ​objetivo general de la Estrategia Nacional de Ciberseguridad es identificar y establecer las acciones en materia de ciberseguridad aplicables a los ámbitos social, económico y político que permitan a la población y a las organizaciones públicas y privadas, el uso y aprovechamiento de las TIC de manera responsable para​ ​el​ ​desarrollo​ ​sostenible​ ​del​ ​Estado​ ​Mexicano [3].

## Monitoreo de Tiendas virtuales

El gobierno mexicano ha provisto una herramienta que permite a los consumidores revisar si los sitios de los proveedores que realizan transacciones a través del comercio digital cumplen con las disposiciones contenidas en la Ley Federal de Protección al Consumidor.

Esta información brinda certeza y seguridad al conocer, antes de realizar una transacción electrónica, si el proveedor cumple o no con los elementos necesarios para proteger sus derechos, lo que ayuda a fortalecer el consumo inteligente.

De esta manera, Si quieres buscar una tienda virtual basta con escribir el Nombre Comercial o Dirección electrónica del sitio virtual de ventas. [4]

## Prevenir, detectar y mitigar amenazas

Cisco aconseja estos pasos para prevenir, detectar y mitigar las amenazas, con el propósito de minimizar los riesgos:

- Hacer de la seguridad una prioridad empresarial: El liderazgo ejecutivo debe ser dueño y concientizar al resto con respecto a la importancia de la seguridad y financiarla como una prioridad.

- Medir la disciplina operacional: revisar las prácticas de seguridad y controlar puntos de acceso a sistemas de red, aplicaciones, funciones y datos.

- Comprobar la eficacia de la seguridad: Establecer métricas claras. Utilícelos para validar y mejorar las prácticas de seguridad.

- Adoptar un enfoque de defensa integral: Hacer de la integración y la automatización una prioridad en la lista de criterios de evaluación para aumentar la visibilidad, agilizar la interoperabilidad y reducir el tiempo de detección y detención de ataques. Los equipos de seguridad pueden enfocarse en investigar y resolver amenazas verdaderas [6].

Finalmente, tengo a bien proponer algunas estrategias para fomentar la cultura de la ciberseguridad en la población actual:

Desarrollo del plan de estudia en las escuelas que implemente la cultura de seguridad informática.

Los mismos medios de comunicación son el medio más eficiente para poder generar este alcance de información a la mayor parte de la población.

Finalmente, las redes sociales es el otro medio para difundir esta información. Sería muy importante también, la creación de un formato o documento oficial que contenga las diversas medidas de seguridad que se pueden tomar ante cada situación.

# Estado del arte

Ahora bien, debe existir un equilibrio entre la implementación de la seguridad cibernética y la operabilidad y agilidad de los sistemas. “Con la intención de alcanzar un ciberespacio seguro se corre el riesgo de limitar la agilidad de los sistemas informáticos. Además, es prácticamente imposible imaginar un ciberespacio 100% seguro” [5].

He aquí se prensentan las principales estadísticas sobre cibersegridad del 2017:

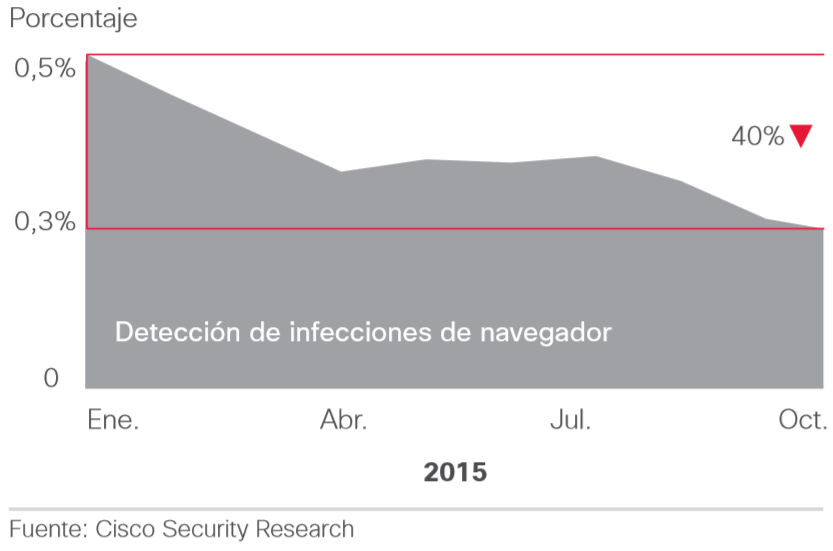
## Trabajos y desempleo de las Tecnologías de la Información

Hay 1 millón de puestos de trabajo de seguridad cibernética en 2017 y se prevé que superen los 1,5 millones en 2019. Esto crea oportunidades para una fuerza de trabajo más diversa – una oportunidad para las mujeres, y las minorías para entrar en el campo de la ciberseguridad son de un billón de dólares.

La tasa de desempleo en ciberseguridad se mantiene en cero por ciento en 2017 (igual que en 2016). El Centro de Investigación de Palo Alto [7] informa que para 2019 la demanda de profesionales de ciberseguridad aumentará a aproximadamente 6 millones a nivel mundial.

## Infecciones de navegador

## A menudo, los equipos de seguridad ven los complementos de navegador como una amenaza de poca gravedad. Sin embargo, deben establecer su supervisión con una prioridad más alta para poder identificar y solucionar rápidamente estos tipos de infecciones [12].



## Fig. 1 Infecciones de navegadores, de enero a octubre de 2015

## La ciberguerra en los medios de comunicación [8]

El Ejército de Brasil y la empresa española de seguridad Panda Security juntos contra la ciberguerra.

Irán sufre un ataque informático contra sus instalaciones nucleares. [9]

Israel militariza la cibernética [10].

Ataques a las páginas Web de la SGAE y Cultura

La Unión Europea prueba sus defensas en un simulacro de «ciberataque» [11].

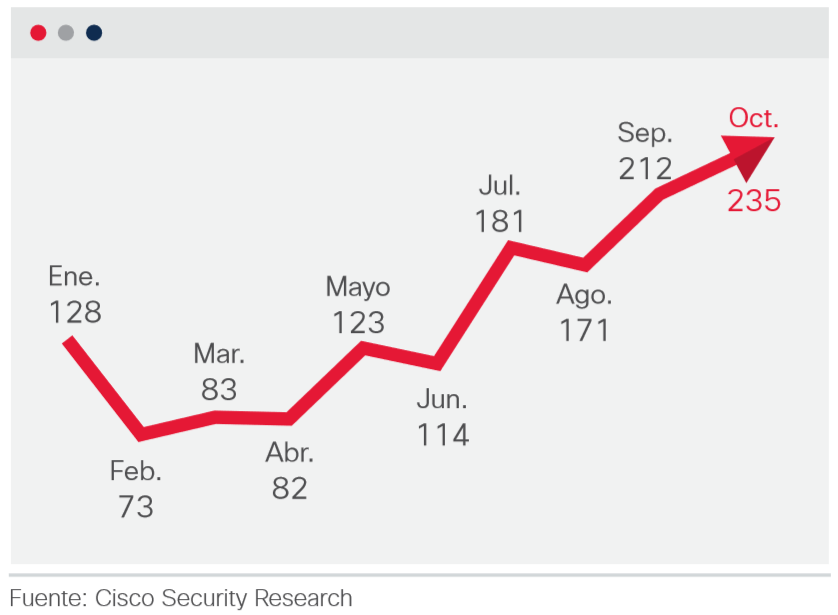
## Cloud computing (la computación en nube) y las innovaciones disruptivas: el impacto en la ciberseguridad

La Cloud Security Alliance se define como una organización internacional sin ánimo de lucro para promover el uso de mejores prácticas para garantizar la seguridad en cloud.

En marzo del 2010 publicó un informe «Top Threats to Cloud Computing V1.0» [13] sobre las siete mayores amenazas de la infraestructuras cloud, con el propósito de asistir a las organizaciones en la toma de decisiones y en la adopción de estrategias que incluyan cloud computing.

## Los delincuentes en línea aumentan la actividad de los servidores en WordPress

Los delincuentes en línea buscan continuamente métodos para agregar eficacia y ahorro de costos a sus operaciones, junto con nuevas formas de evadir la detección. Cada vez más, los ciberdelincuentes están encontrando esta eficacia en sitios web creados con WordPress, la conocida plataforma de desarrollo de sitios web y blogs [12].



## Fig. 2 Cantidad de dominios de WordPress utilizados por los creadores de malware

# Referencias

*Publicaciones periódicas y libros:*

1. Depto. de seguridad informática de la Universidad Nacional de Luján “Amenazas a la Seguridad de la Información”. Disponible en: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12
2. Time Archive by Nathan Thornburgh (2005) “The Invasion of the Chinese Cyberspies (The Man Who Tried to Stop Them)”. Disponible en: https://courses.cs.washington.edu/courses/csep590/05au/readings/titan.rain.htm
3. Gobierno de México, "Estrategia Nacional de ciberseguridad". Disponible en: https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad
4. Gobierno de México, “Monitoreo de tiendas virtuales”. Disponible en: https://www.profeco.gob.mx/tiendasvirtuales/index.html
5. Torres, (2018, feb), Aanálisis GESI “Estrategias Nacionales de Ciberseguridad en América Latina”. Disponible en: http://www.seguridadinternacional.es/?q=es/content/estrategias-nacionales-de-ciberseguridad-en-am%C3%A9rica-latina
6. San José CA, 2017, “Asociación Colombiana de Ingenieros de Sistemas” Disponible en: http://www.acis.org.co/portal/content/reporte-anual-de-ciberseguridad-cisco-2017-jefes-de-seguridad-revelan-el-verdadero-costo-de
7. PARC (Palo Alto Reach Center). Disponible en: https://www.parc.com/
8. J.A. Luis, “Estado del arte de la ciberseguridad”. Disponible en: file:///C:/Users/sahar/AppData/Local/Packages/Microsoft.MicrosoftEdge\_8wekyb3d8bbwe/TempState/Downloads/Dialnet-IntroduccionEstadoDelArteDeLaCiberseguridad-3837217.pdf
9. Ángeles ESPINOSA, El País, 28 septiembre de 2010, p. 6. Además de El País, ese día prácticamente toda la prensa nacional e internacional recogían la noticia: Financial Times, «Online attack was aimed at nuclear work, says Teheran», p. 2; La Vanguardia, «Irán sufre un masivo ataque informático», pp. 8-9; ABC, El Mundo, etc. fueron otros periódicos españoles que recogieron la noticia.
10. La Vanguardia, “Israel militariza la cibernética”. Disponible en: http://www.lavanguardia.com/internet/20101012/54022503624/israel-militariza-la-cibernetica.html
11. El mundo site web, “La UE prueba sus sistemas de defensa en un simulacro de 'ciberataque' paneuropeo”. Disponible en: http://www.elmundo.es/elmundo/2010/11/04/navegante/1288869308.html
12. CISCO, “Informe anual de seguridad 2016”. Disponible en; https://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/annual\_security\_report\_2016\_es-xl.pdf
13. CSA, (2010, marzo), “Top Threats to Cloud Computing V1.0”. Disponible en: https://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

*Escritos presentados en conferencias:*

1. ENCS “Documento de trabajo hacia una Estrategia Nacional de ciberseguridad” Disponible en: https://www.gob.mx/cms/uploads/attachment/file/239446/Documento\_de\_trabajo\_ENCS\_v0.pdf

1. [↑](#footnote-ref-1)