TECTZAPIC
Revista Académico-Científica

Revista de divulgación científica y tecnológica. ISSN: 2444-4944
Tecnológico Nacional de México Campus Ciudad Valles

LA SEGURIDAD INFORMÁTICA EN LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR

COMPUTER SECURITY IN HIGHER EDUCATION INSTITUTIONS

Recibido: 24/09/2021
Aceptado: 6 de noviembre 2021

J.M. Salazar Mata[1]
C. Cruz Navarro[2]
A. V. Balderas Sánchez[3]
H. F. Díaz Uribe[4]

RESUMEN

El incremento exagerado del uso de la internet, de los diferentes dispositivos y de sistemas digitales, tanto para le educación, como para uso de las redes sociales y compras en línea por parte de los usuarios, es generado a consecuencia de la larga contingencia causada por el SARS-COV2 (Covid19). Esto a su vez, ha ocasionado un incremento en los fraudes cibernéticos; alrededor de 500 mil ataques reportados con un costo de 6,000 millones en todo el mundo, y en México está dentro de los primeros 10 países más atacados con un 61%. Estos robos, afectan tanto a personas comunes como a empresas de todo tipo y tamaño (chicas, medianas y grandes), así como empresas privadas y de gobierno.

Esto hechos han generado un déficit en el personal profesional capacitado de 1.8 millones en el mundo y en México de 35 mil, en las áreas de la ciberseguridad, como es hacking ético y cómputo forense y otras más. Con ello se tiene una gran oportunidad, para proponer asignaturas, cursos, capacitaciones en área de ciberseguridad, así como una especialidad de "Administración de redes y ciberseguridad", para la carrera de Ingeniería en Sistemas Computacionales, que genere competencias acordes a esta problemática. Logrando con ello abatir el gran déficit de personal capacitado en estas áreas, logrando así que la información sea más segura en las empresas, considerando que el crimen cibernético es cada vez más recurrente, se puede combatir con la prevención, la ética y el profesionalismo.

PALABRAS CLAVE: SARS-COV 2, fraudes cibernéticos, hacking ético, cómputo forense, ciberseguridad

ABSTRACT

The exaggerated increase in the use of the Internet, different devices and digital systems, both for education, as well as for the use of social networks and online purchases by users, is generated as a result of the long contingency caused by SARS-COV2 (Covid19). This, in turn, has led to an increase in cyber fraud; around 500 thousand attacks reported at a cost of 6,000 million worldwide, and in Mexico it is within the first 10 most attacked countries with 61%. These thefts are affected by both common people and companies of all types and sizes (small, medium and large), as well as private and government companies.

These events have generated a deficit in trained professional personnel of 1.8 million in the world and in Mexico of 35,000, in the areas of cybersecurity, such as ethical hacking and forensic computing and others. Which is a great opportunity to propose subjects, courses, training in the area of cybersecurity, as well as a specialty of "Network Administration and cybersecurity", for the Computer Systems Engineering career, which generates competencies according to this problem. In order to reduce this great personnel deficit, and thus help make information more secure in companies, although cybercrime will never end, if these cybercrimes can be combated ethically and professionally.

KEY WORDS: SARS-COV 2, cyber fraud, ethical hacking, forensic computing, cybersecurity

[1] Profesor del Tecnológico Nacional de México, Campus Ciudad Valles, juan.salazar@tecvalles.mx
[2] Profesor del Tecnológico Nacional de México, Campus Ciudad Valles, claudia.cruz@tecvalles.mx
[3] Profesor del Tecnológico Nacional de México, Campus Ciudad Valles, alba.balderas@tecvalles.mx
[4] Profesor del Tecnológico Nacional de México, Campus Ciudad Valles, hector.diaz@tecvalles.mx

INTRODUCCIÓN

En la actualidad, se sabe que las empresas que invierten en seguridad cibernética son 200 veces más efectivas a la hora de prevenir ataques (Lucie Reynaud, Y., 5 octubre de 202). Todas las instituciones tanto educativas como de negocios, nunca deben de pasar por alto la importancia de la seguridad informática ya que año tras año, estos ataques se producen a un ritmo cada vez más acelerado.

Estadísticamente, cuanto más grande es la organización, hay más probabilidades de sufrir un ataque. Sin embargo, esto no evita que las pequeñas y medianas empresas también estén en riesgo. Ningún negocio en la actualidad que maneje en sus procesos las tecnologías de la información y comunicación (Tic's) es inmune a un ataque cibernético. Para una empresa u organismo, las consecuencias que puedan tener en cuanto a parte legal, física y financiera pueden ser muy catastróficas.

En las últimas décadas, las tecnologías de la información se han convertido en parte integral de todo lugar de trabajo. Hoy en día vivimos en un mundo más avanzado tecnológicamente, además de aprovechar el entorno empresarial, también corremos un mayor riesgo debido a nuestra vulnerabilidad que representan los ciber ataques (Inoguchi Rojas, A., & Macha Moreno, E. (2017)..

Según la Asociación Nacional de Facultades y Escuelas de Ingeniería (ANFEI) que en la actualidad tiene un total de 213 Instituciones de Educación Superior afiliadas en México y en el último informe acerca del estado actual de las TIC's en las Instituciones de Educación Superior, en materia de seguridad, refiere que el 76% de las instituciones cuentan con una política de seguridad a cargo del responsable de TI (Tecnologías de la Información) en las instituciones (ANFEI, 2021).

"Las instituciones de educación superior, deben reconocer que sus activos de información son esenciales para la continuidad del negocio y el cumplimiento de su misión y visión; por lo cual es fundamental protegerlos, restringiendo su acceso, uso y revelación, acorde al cumplimiento de sus objetivos institucionales" (ANFEI, 2021).

El reto actual en materia de seguridad es mayor debido a la contingencia sanitaria, desde el 2020, que obligo a profesores y estudiantes a requerir adaptarse a nuevos entornos virtuales para la impartición de clases (lo que implico para muchos un gran reto), se requirió del uso de diferentes alternativas tanto de herramientas digitales, así como, el obligarse a utilizar diferentes dispositivos, pc, laptop, tabletas y otros móviles como celulares, entre otros. Además, del uso con gran demanda del internet y el incremento de compras en línea.

Lo anterior provocó que los usos de estos dispositivos volvieran excesivamente vulnerables a los usuarios de ello; todo por el desconocimiento en materia de seguridad informática de los mismos. Es por esto que, es necesario que se atiendan desde la formación de futuros profesionistas éstos temas, y que en las retículas de las IES (Instituciones de Educación Superior) se proponga que exista una asignatura de ciberseguridad básica.

Esto fue propuesto de manera de manera extraoficial ante la ANUIES (Asociación Nacional de Universidades e Instituciones de Educación Superior), en la planeación de trabajo por parte de la Comisión de Seguridad de ANUIES y, que a su vez se haga la propuesta en las reuniones de directores de las IES y lograr este objetivo.

Esto es un gran reto; ya que, hay que convencer a los directivos o rectores y, que vean la necesidad e importancia que es la seguridad informática o ciberseguridad dentro de la infraestructura de la IES y fuera de ella.

Con este contexto, el presente trabajo pretende crear conciencia de la importancia que tiene hoy en día el tema de seguridad informática, y la necesidad de que se incluya en la formación de las habilidades de los estudiantes de todas las carreras de la IES y específicamente lograr mejorar el campo laboral de un Ingeniero en Sistemas Computacionales.

DESARROLLO

Pero ¿Qué es la ciberseguridad? IBM México (2021), menciona que: *"Es la práctica de proteger sistemas críticos e información confidencial de ataques digitales".* Por otro lado, Galiana (2021); indica que, proteger los activos digitales es una obligación para todas las empresas. Menciona que, las amenazas que existen en la red y la seguridad de la información, software, datos y sistemas ponen en peligro uno de los activos tecnológicos. Provocando que los ataques tuvieran un costo promedio de una filtración de datos fue de USD 2.56 millones en Latinoamérica. Además de que contiene los costos de exploración y las reacciones al ataque, el costo de detener las operaciones y las pérdidas de ingresos, así como las pérdidas a largo plazo del prestigio de la empresa.

La crisis del Covid-19, ha multiplicado el trabajo en línea y las compras remotas, lo que representan altos puntos de riesgo por el uso de Internet, de acuerdo con la publicación en Holloway (2020). Los encargados de la seguridad de los sistemas y las tecnologías de la información han trabajado rápidamente en esto, pero muchas cosas no han sido resueltas, por lo que los usuarios y sistemas quedaron vulnerables ante estos peligros inminentes. Ante estos retos, el siguiente paso será centrarse en la protección de datos más minuciosa, la autenticación de los usuarios y del control de acceso, así como implementar mejores restricciones de seguridad y numerosas supervisiones en todas las aplicaciones. En lo más crítico de la pandemia, el comercio electrónico se ha convertido en la única forma en la que los consumidores adquieran sus productos. Aquellos que no realizaban compras en línea, tuvieron que hacerlas para cubrir una necesidad, lo cual incremento los ataques cibernéticos.

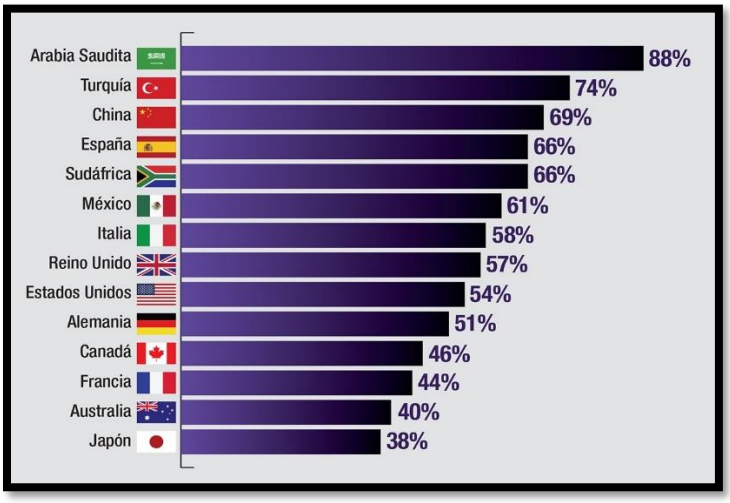
Además, Holloway (2020), da las siguientes cifras que proporciona Kaspersky, las cuales deben ser consideradas como referente en los planes de seguridad informática:

- México es el noveno país más afectado por el crimen cibernético, con 605 casos reportados. En América Latina solo es superado por Brasil.
- Más de $6,000 millones de dólares se estima que se perderán globalmente derivado de la actividad cibercriminal en 2021.
- 467,351 incidentes de ciberseguridad fueron reportados globalmente en 2019.
- 71% de los robos de información tuvieron como motivo obtener dinero; 25% fueron con fines de espionaje.
- El método elegido en el 52% de los casos de robo de información fue el hackeo directo, en el 33% de los casos se recurrió a phishing o ingeniería social y el 28% correspondió a malware.
- 43% de los ciberataques afectan a pequeños negocios. Los ataques entre un año y otro

a estas organizaciones crecieron 424%

- El tiempo promedio para identificar un robo de información es de 206 días. Desde que sucede hasta su contención puede pasar 314 días.
- El fraude por pagos en línea costará al eCommerce por lo menos $25,000 millones de dólares al año para 2024.
- El 34% de las 11,000 vulnerabilidades cibernéticas no tiene un parche conocido.
- En el 63% de las compañías los datos estuvieron potencialmente comprometidos en los últimos 12 meses por culpa de una vulnerabilidad de hardware. En 28% de los casos, las empresas no están contentas con el manejo de seguridad de sus proveedores.
- 65% de los grupos cibercriminales utilizan spear-phishing como su principal vector de infección.

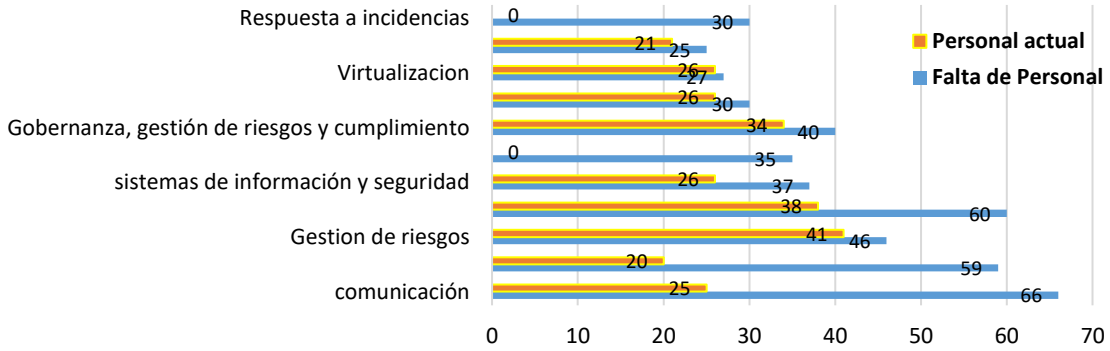
Kaspersky América Latina, menciona que no es solo el tema de secuestro de sistema e información corporativa que está en boga, sino que las tácticas se han vuelto muchos más peligrosas. Uno de esos programas es Ransomware, el cual ha pasado de bloquear sistemas altamente relacionados con los negocios a extraer información confidencial y amenazar a las empresas con la divulgación o el intercambio con la competencia. Muchas empresas en México (61%), como se muestra en la gráfica 1 han sufrido de estos ataques y robo de información para amenazas (CICE, 2021).



Gráfica 1. Empresas atacadas con ransomware en México, en los últimos 12 meses. Fuente: Safety Detectives.

Lo anterior denota una gran oportunidad en el área laboral en temas de seguridad informática, por la falta de trabajadores especialistas en ciberseguridad, según lo confirma el estudio del Centro Mundial de Seguridad Cibernética y Educación (ISC) en el artículo necesidad trabajadores en ciberseguridad que se realiza cada dos años, en su Estudio Mundial de Seguridad de la Información (GISWS, sus siglas en inglés), que incluye los datos de 20,000 organizaciones de 170 países. Además, afirman que un 66% de las empresas de seguridad de la información tienen muy pocos trabajadores para hacer frente a las amenazas informáticas,

un 4% más que en el anterior estudio. Aunado a ello, pronostican una escasez de 1.8 millones de trabajadores para el 2022. En la gráfica 2 se indica las necesidades en las diferentes áreas de la ciberseguridad a nivel mundial.



Gráfica 2. Habilidades Principales Requeridas del nuevo personal. Fuente CICE 2021.

La tecnología evoluciona tan rápido que toda organización hoy en día, busca optimizar todos los procesos y reducir los costes de las empresas, lo que implica que se descuiden en materia de seguridad de la información, es por ello que se debe enfatizar y profundizar la idea de prevención contra los ataques cibernéticos a las empresas y así puedan considerar planes de ciberseguridad de su información que incluyan la prevención de:

- Riesgos a la información cibernética privada, estos riesgos generan un robo, manejo inadecuado o divulgación prohibida de la ciberinformación de una empresa.
- Riesgos a la infraestructura tecnológica de ciberinformación, estos riesgos generan y provocan la paralización total o parcial y por lapsos de tiempo indefinidos de operaciones, servicios o sistemas vitales para una empresa o País.

Analizando el contexto mundial, el Estudio Mundial de Seguridad de la Información, indica la falta de personal con las competencias académicas especializadas por más de 1.8 millones a nivel mundial, según entrevista con el Dr. Mario Farías, experto en ciberseguridad, menciona que solo en Latinoamérica hace falta más de 800 mil especialistas en seguridad y, en México actualmente se cuenta con un déficit de 35 mil. Las áreas en las que se destaca la necesidad de personal especializado son las áreas de prevención como el Hacking Ético y Cómputo Forense.

RESULTADOS

En la última reunión de seguridad, realizada el año 2020, de la Comisión de Seguridad de ANUIES, se ha mencionado que el 76% de las Instituciones de Educación Superior afiliadas tienen definida su política de seguridad, pero un porcentaje muy pequeño son las que tienen un plan específico de seguridad de la información comparado con el número de éstas (IES 213 al 2020). Solo existen acciones aisladas como cursos, diplomados, especialidades y posgrados, por lo que se propuso elaborar un catálogo en el país con las IES que cuenten con programas, acciones o planes de seguridad.

Los últimos resultados (ANUIES-TIC 2020) reflejan el actual panorama educativo de las Instituciones de Educación Superior en lo referente a la seguridad en la operación de programas académicos, y en las estrategias y acciones de formación, difusión y actualización en temas de seguridad de la información, por otro lado, hace hincapié en la importancia de que exista una política de seguridad y la normatividad aplicable a ella, que se difunda para que se dé el cumplimiento en este aspecto.

El análisis de información presentado permite detectar las necesidades, y definir las áreas de oportunidad para proponer acciones, con la finalidad de fortalecer la seguridad de la información de toda IES.

Los principales resultados presentados fueron:

1. En cuanto presupuesto y la procedencia de los recursos para la seguridad de la información refieren que el 48% de las IES no cuentan con un presupuesto identificable en términos de seguridad, el 21% no cuenta con presupuesto asignado.
2. El 76% de las IES cuenta con una política de seguridad definida, pero de estas, solo el 30% cuenta con una política que incluye objetivos alineados a los institucionales.
3. En lo referente a la responsabilidad de la seguridad el 52% de las IES refieren que el responsable de las TIC's en la Institución es quien se hace cargo de la seguridad.
4. El 50% de las IES encuestadas utiliza algún marco de referencia vigente relacionado con seguridad de la información, implementado en toda la organización, sin embargo, de estas, solo el 23% refiere el estándar ISO/IEC 27001 y el 16% el MAAGTICSI.
5. En cuanto a revisión de la seguridad, el 49% de las IES no realizan auditorías/evaluaciones de seguridad de la información.
6. Y, solo el 7% de las instituciones cuentan con certificación ISO/IEC 27001 vigente.
7. Sin embargo, casi el 70% de las IES encuestadas cuenta con acuerdos de confidencialidad como estrategia de seguridad.
8. En cuanto a la responsabilidad de las acciones de seguridad, refiere que el 88% de lasa IES cuentan con personal de TI en las áreas de redes y telecomunicaciones que adicionalmente se desempeñan en seguridad de la información.
9. Adicional a ello, refieren que solo el 7% de las IES tienen personal certificado en ISO/IEC 27001.
10. En lo referente a si existe un plan de tratamiento de riesgo de seguridad de la información el 54 de las IES encuestadas cuentan con un plan de tratamiento de riesgos de seguridad de la información.
11. Finalmente, el 51% de las IES refieren tener materias obligatorias en sus programas académicos en seguridad de la información y el 16% materias optativas.
12. Además, el 77% de ellas no cuenta con investigadores en seguridad de la información.

CONCLUSIONES

El estado actual de los indicadores nacionales presentados, se muestran con la finalidad de promover la planeación, implementación y puesta en marcha de un *Plan de Gestión de la Seguridad de la Información*, en cada institución, mismo que se propone sea implementado e impulsado para el Tecnológico Nacional de México campus Ciudad Valles, considerando los siguientes aspectos:

La concientización del establecimiento de metodologías estructuradas para la mejora continua, en cuanto a la gestión de la seguridad de la información. La reducción del riesgo ante pérdida, robo o corrupción de la información. La promoción del establecimiento de una política institucional, planes de la continuidad y disponibilidad de los servicios de TI. La reducción de los costos vinculados a los incidentes de seguridad. El incremento de los niveles de confianza de los usuarios de la comunidad tecnológica. El mejoramiento de la imagen institucional.

El cumplimiento de las legislaciones vigentes, como la protección de datos personales en posesión de sujetos obligados y de particulares, transparencia y acceso a la información pública, ley general de archivo, y todas aquellas relacionadas con la seguridad de la información institucional. Apoyo en procesos de certificación, acreditación e investigación en materia de seguridad informática y estándares para ello.

Igualmente, importante se propone solicitar ante la Academia del TecNM - Campus de Ciudad Valles la consideración para agregar una asignatura/curso/capacitación en todas las carreras de Fundamentos de la Ciberseguridad y, como segundo punto, se proponga una especialidad de Administración de Redes y Ciberseguridad, esta para la carrera de Ingeniería de Sistemas Computacionales.

BIBLIOGRAFÍA

ANFEI. (2021). *Asociación Nacional de Facultades y Escuelas de Ingeniería*. Obtenido de https://www.anfei.mx/miembros/

ANUIES. (2020). *Plataforma y recursos digitales ante la contingencia de la COVID-19.* Obtenido de https://recursosdigitales.anuies.mx/ciberseguridad-para-educacion-en-linea/

CICE. (2021). *El Centro Mundial de Seguridad Cibernética y Educación*. Obtenido de https://www.cice.es/blog/articulos/necesidad-trabajadores-en-ciberseguridad/#inicio_contenido

Galiana, P. (3 de Marzo de 2021). IEBS. Obtenido de *Qué es la Ciberseguridad, por qué es importante y como convertirte en experto*: https://www.iebschool.com/blog/que-es-ciberseguridad-tecnologia/

Holloway, C. (8 de octubre de 2020). ITMaster Mag. Obtenido de El estado de la seguridad *IT en 2020: Las superficies de ataque se amplían y las personas nunca fueron tan importantes para la defensa*: https://www.itmastersmag.com/informes-whitepapers/el-estado-de-la-seguridad-it-en-2020-las-superficies-de-ataque-se-amplian-y-las-personas-nunca-fueron-tan-importantes-para-la-defensa/

IBM. (2021). Ciberseguridad con IBM Security. Obtenido de *Security Summit México* 2021.: https://www.ibm.com/mx-es/security?p1=Search&p4=43700057927479626&p5=e&gclid=Cj0KCQjwqKuKBhCxARIsACf4XuHijL4OXKlBtdhmkwh0xqW9q7bNeWjXNyG-j30o3iXDID-AV3Yic5QaAtvOEALw_wcB&gclsrc=aw.ds

Inoguchi Rojas, A., & Macha Moreno, E. (2017). *Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las pymes del Perú* 2016. Lim, Perú: Universidad San Ignacio de Loyola.

Lucie Reynaud, Y. (5 de octubre de 2020). *ICES España Exportación e Inversiones. Obtenido de Ciberseguridad en México*: ttps://www.ivace.es/Internacional_Informes-Publicaciones/Pa%C3%ADses/M%C3%A9xico/M%C3%A9xicociberseguridadicex2020.pdf

Planas, J. (2014). Publicaciones ANUIES. Obtenido de *Adecuar la oferta de educación a la demanda de trabajo. ¿Es posible? Una crítica a los análisis "adecuacionistas" de relación entre formación y empleo*: http://publicaciones.anuies.mx/colecciones/temas-de-hoy-en-la-educacion-superior/202/adecuar-la-oferta-de-educacion-a-la-demanda-de-trabajo-es-posible-una