Published on *Revista .Seguridad* (https://revista.seguridad.unam.mx)

EVOLUCIÓN EN EL USO DE HERRAMIENTAS DE SEGURIDAD INFORMÁTICA EN INSTITUCIONES DE EDUCACIÓN SUPERIOR DE MÉXICO

Carmen Humberta de Jesús Díaz Novelo

IES

numero-29

INTRODUCCIÓN

Las amenazas de seguridad están continuamente evolucionando, por lo tanto las herramientas y tecnologías de seguridad para las redes no pueden quedarse estáticas, especialmente si su objetivo es analizar el *payload* o "contenido" de los paquetes de información y no el medio en que son transportados, considerando la existencia de amenazas como *bots*, *ramsomware*, *APTs* (*Advanced persistent Threats*), *malware* o *spam* (Kennet T., 2013).

Las herramientas de seguridad informática tienen como principal objetivo controlar los accesos a la red, proteger el flujo de información sensible y prevenir los ataques maliciosos dirigidos a sistemas de telecomunicaciones, de transporte de información y del "contenido" de las comunicaciones; algunas herramientas de seguridad conocidas son los *firewalls*, sistemas de detección de intrusos (*IPS*), sistemas antivirus, *antimalware* y servicios de autenticación, entre otros.

En este contexto, analizaremos la información reportada por Instituciones de Educación Superior (IES), miembros de la Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES), entre los años 2005 al 2016, acerca del uso de herramientas de seguridad informática. Actualmente la ANUIES cuenta con 187 asociados y para el seguimiento de sus iniciativas ha dividido los trabajos en regiones. La región sur-sureste, que es el objeto de estudio de este artículo, está conformada por los Estados de Veracruz, Oaxaca, Chiapas, Campeche, Quintana Roo y Yucatán.

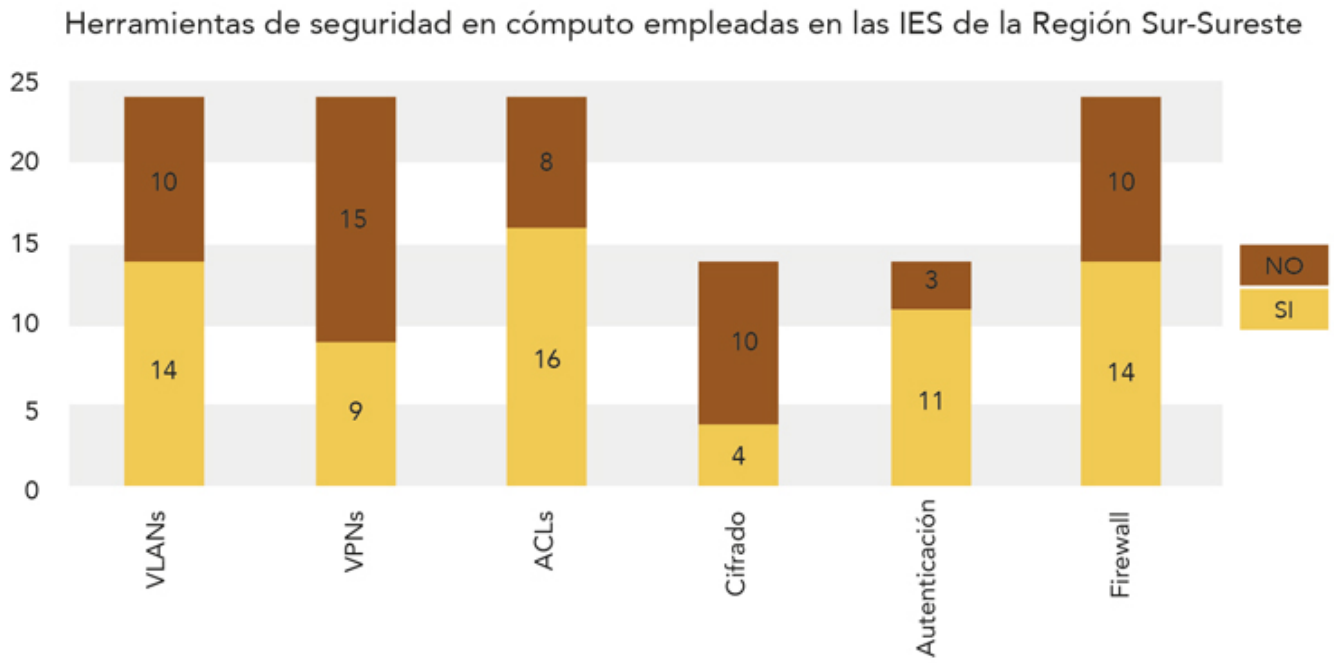
RESULTADOS SOBRE HERRAMIENTAS DE SEGURIDAD

INFORMÁTICA EN INSTITUCIONES DE EDUCACIÓN SUPERIOR

RESULTADOS EN LA REGIÓN SUR-SURESTE DE MÉXICO

En una encuesta de ANUIES aplicada a 24 instituciones de la zona sur-sureste del país, cuyo objetivo era conocer el estado de las Tecnologías de Información en la Región en el año 2005, se encontró que todas utilizaban alguna solución antivirus.

Se pudo observar que "la seguridad de las IES está basada principalmente en las listas de acceso (ACL) y la autenticación" (ANUIES; 2005; p-13); así mismo, 14 de 24 instituciones reportaron contar con firewalls, pero solo 4 contaban con herramientas de cifrado de datos, redes privadas virtuales y calidad de servicio (QoS). La gráfica 1 nos muestra el resultado sobre el uso de las herramientas de seguridad en las IES.



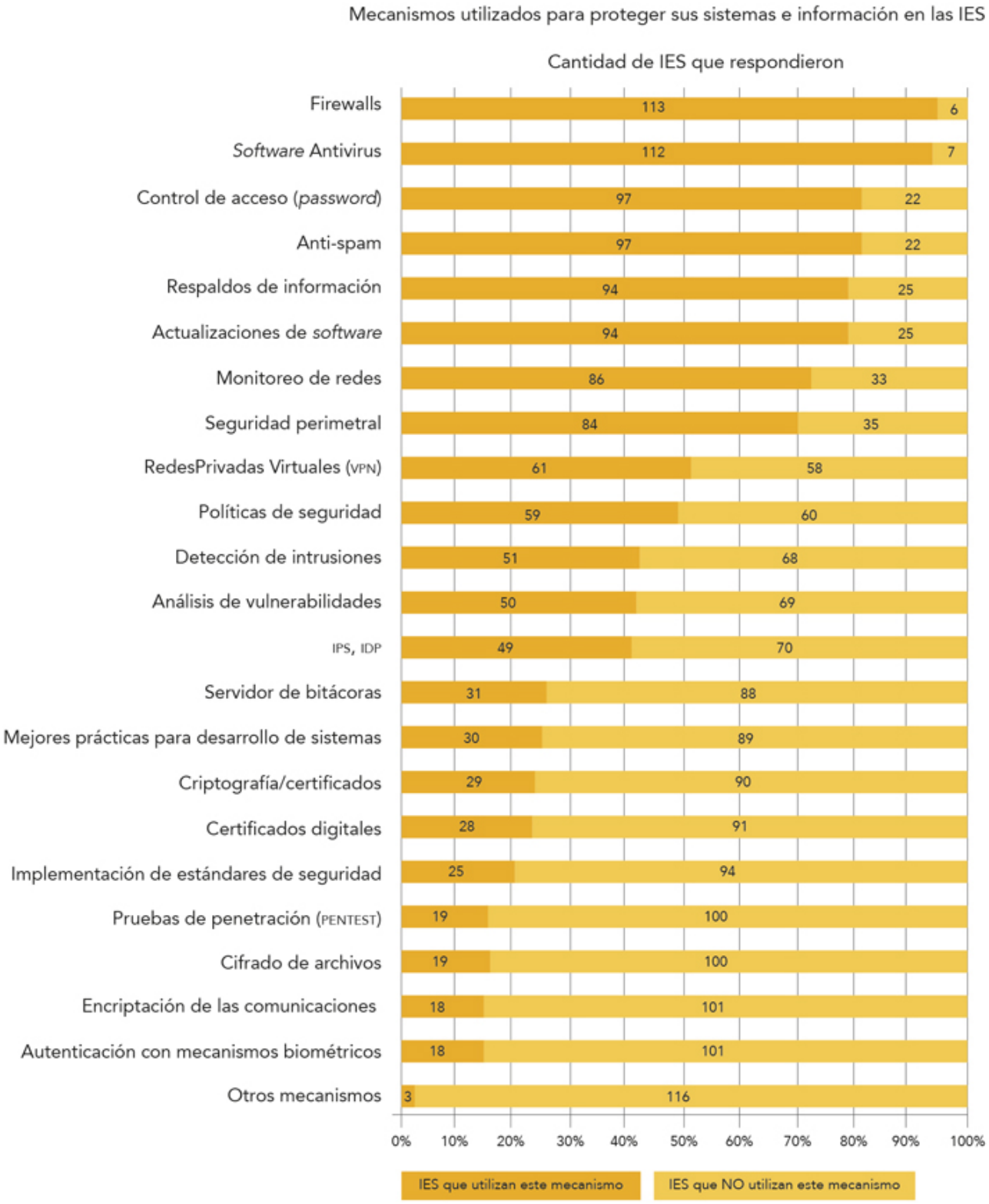
Gráfica 1. Herramientas de seguridad en Cómputo empleadas en la Región sur-sureste. Fuente: Asociación Nacional de Universidades e Instituciones de Educación Superior; 2005; p-13

ENCUESTA DE SEGURIDAD INFORMÁTICA

En el año 2011, la ANUIES en coordinación con UNAM-CERT, la Universidad Autónoma de Yucatán, el Instituto Tecnológico de Sonora y la Universidad Autónoma de Querétaro elaboraron una encuesta para conocer el estado de la seguridad, las necesidades y áreas de oportunidad de IES miembros de la ANUIES.

Los resultados que se obtuvieron apuntan primordialmente a la seguridad de las redes con mecanismos como firewalls, Sistema de Prevención de Intrusos (*IPS*) y redes privadas virtuales. Las IES indicaron que utilizan principalmente *software anti-malware*, *anti-spam*, además de actualizar sus programas y realizar respaldos. De 119 IES, 61 utilizan redes privadas virtuales, y 113 cuentan con firewalls (Aquino R., 2013).

En la gráfica 2, se puede apreciar que es menor el uso de herramientas criptográficas y certificados, así como de autenticación con mecanismos biométricos.

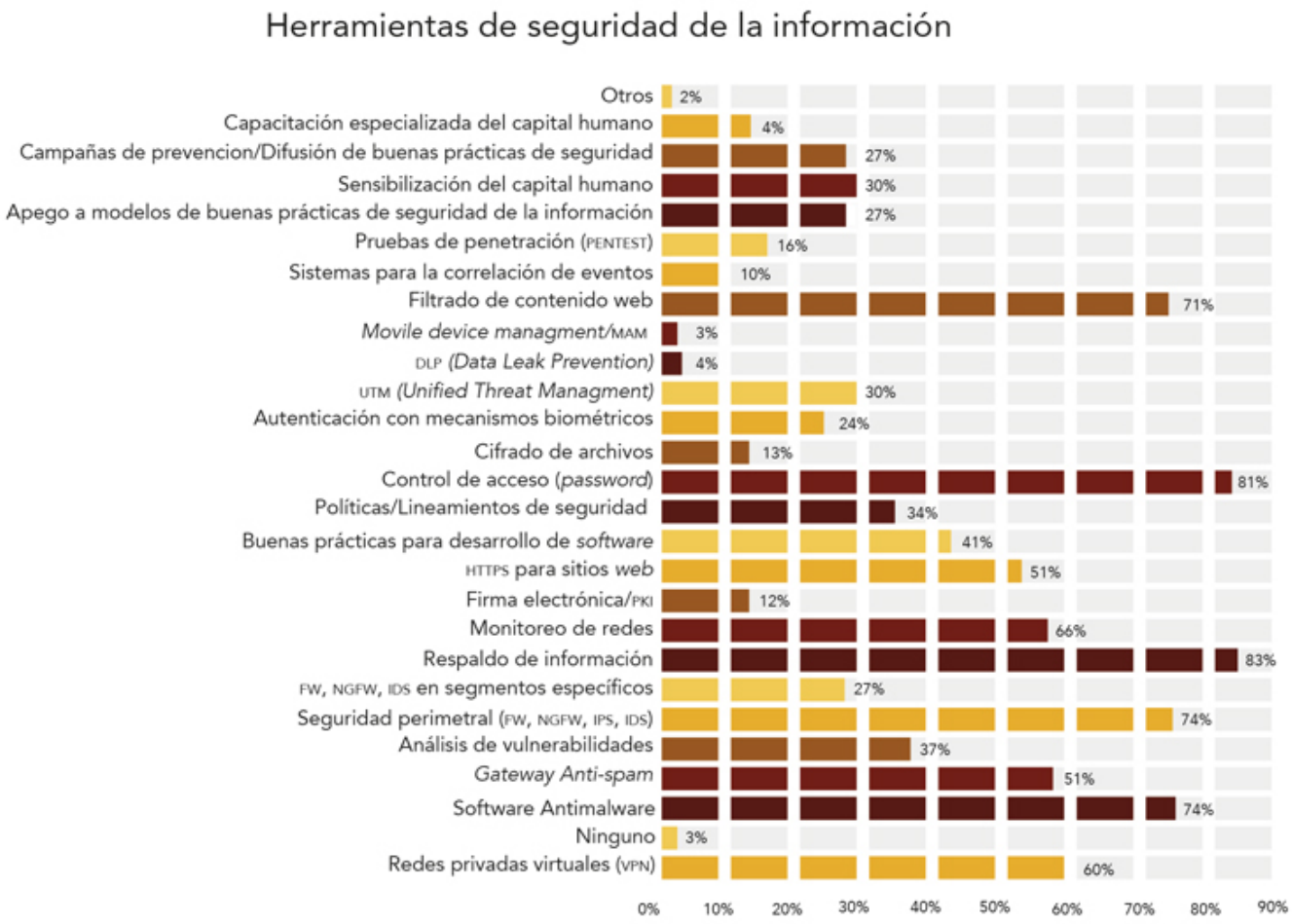


Gráfica 2. Mecanismos utilizados para proteger sistemas e información en las IES.
Fuente: Aquino; et al.; 2013; p-35

RESULTADOS SOBRE EL ESTADO DE LAS TIC

La ANUIES diseñó en el año 2016 un diagnóstico para detectar el estado de las TIC en las 140 IES de todo el país; dicha encuesta también abordó temas de seguridad de la información.

Se muestra en la gráfica 3 que “las IES seleccionan las diversas herramientas de seguridad informática que utilizan para la prevención y contención de amenazas y ataques de seguridad informática; entre las más utilizadas destacan el filtrado de contenido *web* (71%), el control de acceso mediante la utilización de *passwords* (81%), los respaldos de información (83%), la seguridad perimetral utilizando tecnologías de firewall, prevención y detección de intrusos (74%) y software *antimalware* (74%)” (ANUIES; 2016; p-51).



Gráfica 3. Herramientas de seguridad de la información
Fuente: Asociación Nacional de Universidades e Instituciones de Educación Superior; 2016; p-51

HERRAMIENTAS DE SEGURIDAD INFORMÁTICA

Las amenazas que han enfrentado las IES van desde el gusano informático Slammer, que afectó las redes en el año 2003, *botnets*, e incluso el reciente ransomware WannaCry; en el mismo sentido, el uso de las herramientas de seguridad informática ha evolucionado e incrementado.

En la tabla 1 podemos apreciar que inicialmente las IES contaban con herramientas antivirus y posteriormente antimalware. En un principio solo contaban con firewalls y más adelante, con equipos perimetrales como el *UTM (Unified Treath Management)*. Continúa el uso de herramientas con el control de acceso, cifrado de datos y redes privadas virtuales y otro tipo de herramientas se reportaron en años posteriores, por ejemplo los respaldos de información, *IPS* y filtrado de contenido.

	Año		
Herramientas	**2005** **(25 IES)**	**2011** **(119 IES)**	**2016** **(140 IES)**
Antivirus / antimalware	100%	95%	74%
Firewall / equipo perimetral	58%	94%	74%
Control de acceso	66%	81%	81%
Cifrado de datos	16%	15%	13%
Redes privadas virtuales	37%	51%	60%

Respaldos de información	No considerada	79%	83%
IPS	No considerada	41%	74%
Filtrado de contenido	No considerada	No considerada	71%

Tabla 1. Índice de uso de herramientas de seguridad informática en Instituciones de Educación Superior de México en once años. (Carmen Díaz Novelo, 2017)

Las tendencias mundiales revelan el crecimiento de la demanda de servicios a las Instituciones de Educación Superior, como conexión inalámbrica Wi-Fi, el uso de tabletas electrónicas, *smartphones* y otros tipos de dispositivos móviles, por lo que se debe considerar la incorporación de otros tipos de mecanismos como *IPS* para entornos inalámbricos y *Mobile Device Management* (MDM). Así mismo, los sistemas de correlación de eventos comienzan a figurar en el lenguaje de las Instituciones ante redes cada vez más complejas de administrar y analizar debido a la cantidad de “contenido”.

RETOS PARA LAS INSTITUCIONES DE EDUCACIÓN SUPERIOR

En un mundo en que las tecnologías evolucionan constantemente, los modelos de seguridad informática regulares pueden quedar rebasados, por ello las Instituciones de Educación Superior requieren una continua y ágil actualización de sus herramientas de seguridad informática, y deben contar con especialistas para la configuración y operación segura de estas.

A pesar de la evolución de amenazas (cada vez más sofisticadas para eludir los sistemas de defensa), las IES pueden ser eficaces en resguardo y manejo de la información adaptando los modelos de seguridad a la nueva realidad: es necesario proteger el acceso al contenido sin importar el dispositivo empleado, el usuario, el momento o lugar (Zurier S., 2017). Los privilegios de acceso deben determinarse en función de varios atributos que establecen a la vez el contexto del usuario y la solicitud. Estos modelos deben además detectar y corregir las amenazas en evolución, desde el malware común al *ransomware*, pasando por los ataques de tipo *zero-day* y las campañas avanzadas que emplean herramientas técnicas y planificación sofisticada (Intel Security, 2017).

Las herramientas y tecnologías de seguridad son parte de un modelo integral, donde las políticas de seguridad informática deben guiar el mejor uso y aprovechamiento de las herramientas con que cuentan las IES. La ausencia de este tipo de políticas en las instituciones pone en riesgo el

establecimiento de estándares, reglamentos y herramientas de seguridad (Almeida F., 2015)

Contar con información sobre las herramientas de seguridad informática más utilizadas en las IES se convierte, para las instituciones del país, en un factor importante para la toma de decisiones al enfrentar las amenazas de manera más eficaz. Las amenazas cibernéticas emergentes obligan a que tanto directivos como administradores de seguridad informática presten mayor atención a la evolución y adopción de las herramientas de seguridad en entornos académicos, y a encontrar en estas un soporte que contribuya a proporcionar servicios de TI confiables a sus usuarios.

REFERENCIAS

- Almeida, F. a., Monteiro, J. j., & Peixe, J. i. (2015). ICT Security Review: Perceptions at Portuguese High Schools. Journal Of Systems Integration (1804-2724), 6(3), 15-24. Recuperado el 27 de abril de 2017 de: http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=3&sid=746ee544-41f8-4eca-838f-e98a6471d134%40sessionmgr120
- Aquino R., Díaz C., Muñoz P. y Ponce J. (2013). Resultados de la encuesta de seguridad de la información 2011 en las Instituciones de Educación Superior. México. Asociación Nacional de Universidades e Instituciones de Educación Superior.
- Asociación Nacional de Universidades e Instituciones de Educación Superior. (2016). Estado actual de las Tecnologías de Información y las comunicaciones en las Instituciones de Educación Superior en México. Estudio Ejecutivo 2016. México.
- Asociación Nacional de Universidades e Instituciones de Educación Superior. (2005). Tecnologías de Información y comunicaciones en Instituciones de Educación Superior del Sur-Sureste de México. Recuperado el 25 de abril de 2017, de: http://www.anuies.mx/media/docs/89_2_1_1103091247Articulo_Tecnologias_de_la_Informacion.pdf
- Intel Security. (2017). McAfee *Labs*. Informe sobre amenazas. Abril 2017. Recuperado el 25 de abril de 2017, de: https://www.mcafee.com/es/resources/reports/rp-quarterly-threats-mar-2017.pdf
- Prudente L., Sánchez G. y Vázquez J. (2015). Gestión de la seguridad de la información basado en le MAAGTICSI para programas académicos en Instituciones de Educación Superior. Recuperado el 26 de abril de https://revista.seguridad.unam.mx/node/2218
- Tam Kenneth. Hoz Martín. Mcalpine Ken. Basile Rick. Matsugu Bruce. More Josh. (2013) UTM Security with Fortinet. United Satates of America. Syngress.
- Zurier, S. (2017). MOBILE DEFENSE. SC Magazine: For IT Security Professionals (15476693), 28(1), 16-19. Recuperado el 27 de abril de 2017 de: http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=5&sid=df4033a3-a1a9-4794-8851-756e42366ef9%40sessionmgr4006&hid=4001

SI QUIERES SABER MÁS, CONSULTA:

- Seguridad en la nube para una IES
- Normatividad en las organizaciones: Políticas de seguridad de la Información – Parte I
- Gestión de seguridad de la información basado en el MAAGTICSI para programas académicos en Instituciones de Educación Superior

---