Resultados de la encuesta de seguridad de la información 2011 en las instituciones de educación superior

Documento de trabajo

Rubén Aquino Luna
Carmen Díaz Novelo
Patricia Muñoz Romero
José Luis Ponce López

Colección **Documentos**

ANUIES
Al servicio y fortalecimiento de la educación superior

ASOCIACIÓN NACIONAL DE UNIVERSIDADES
E INSTITUCIONES DE EDUCACIÓN SUPERIOR

Dr. en Quím. Rafael López Castañares
Secretario General Ejecutivo

Mtra. Luz Ma. Solís Segura
Directora General Académica

Dr. Fernando de Jesús Bilbao Marcos
Director General de Relaciones Interinstitucionales

Mtro. Javier Mendoza Rojas
Director General de Información y Planeación

L.A.E. Teresa Sánchez Becerril
Directora General de Administración

La ANUIES

La Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES) es una asociación civil mexicana constituida por 174 instituciones de educación superior, en las que se atiende a la mayoría de los estudiantes de este nivel y trabaja el 86.4% de los integrantes del Sistema Nacional de Investigadores.

La asociación tiene entre sus objetivos realizar estudios estratégicos sobre temas de la educación superior, diseñar políticas, anticipar, planear y promover los cambios que éstas requieren y sustentar la toma de decisiones; participar en las instancias nacionales, estatales y regionales de coordinación y planeación de la educación superior, así como sugerir opciones para un desarrollo de calidad en los ámbitos nacional, regional y estatal, especialmente en lo que concierne a modelos, métodos y procedimientos para su planeación y evaluación.

Resultados de la encuesta de seguridad de la información 2011 en las instituciones de educación superior

Documento de trabajo

Rubén Aquino Luna
Carmen Díaz Novelo
Patricia Muñoz Romero
José Luis Ponce López

Red Nacional de Seguridad en Cómputo (RENASEC)

Asociación Nacional de Universidades e Instituciones de Educación Superior

378.19580972 LB1028.43
R47 R47

Resultados de la encuesta de seguridad de la información 2011 en las instituciones de educación superior : documento de trabajo Red Nacional de Seguridad en Cómputo (RENASEC) / equipo de trabajo Rubén Aquino Luna… [et al.] – México, D.F. : ANUIES, Dirección de Medios Editoriales : UNAM, 2013.
58 p. – (Colección documentos)

ISBN 978-607-451-061-4

1. Universidades-México-Procesamiento de datos-Medidas de seguridad. 2. Universidades-México-Sistemas de seguridad. 3. Protección de datos. 4. Seguridad informática. 5. Tecnología de la información. I. Aquino Luna, Rubén. II. Red Nacional de Seguridad de Cómputo (México) II. t. III. Ser.

Resultados de la encuesta de seguridad de la información 2011 en las instituciones de educación superior

Rubén Aquino Luna
Carmen Díaz Novelo
Patricia Muñoz Romero
José Luis Ponce López

Coordinación editorial
Rolando Emilio Maggi Yáñez

Diseño gráfico de la colección
Estudio Sagahón /Leonel Sagahón, Susana Vargas y Jazbeck Gámez

Ilustración de portada
Reveca E. Rivera Galicia

Imagen
© Kheng Guan Toh / 123RF.COM

Formación de este título
Juan Carlos Rosas Ramírez

El cuidado de edición estuvo a cargo de
Michel Torres Gutiérrez

Primera edición, 2013

Tenayuca 200
Col. Santa Cruz Atoyac
México, D. F.

ISBN: 978-607-451-061-4

Impreso en México

CONTENIDO

AGRADECIMIENTOS 7

A las instituciones de educación superior por el tiempo dedicado para el registro de la encuesta, cuya colaboración permite documentar el impacto y perspectivas de la seguridad en tecnologías de información de las instituciones de educación superior.

A los rectores, directores y representantes de las instituciones de educación superior por su compromiso con el proyecto de seguridad informática nacional que ha contribuido a la protección de unos de los activos más preciados en nuestras Instituciones, la información.

A la Universidad Nacional Autónoma de México por su contribución a la seguridad de la información, a nivel nacional e internacional, quien mediante su Equipo de Respuesta a Incidentes de Seguridad en Cómputo (UNAM-CERT), colabora y da el soporte a las instituciones de educación superior del país a través de la Red Nacional de Seguridad en Cómputo de la ANUIES.

A la Secretaría General de la ANUIES por su gran apoyo y entusiasmo hacia el proyecto de la Red Nacional de Seguridad en Cómputo.

INTRODUCCIÓN 9

La Asociación Nacional de Universidades e Instituciones de Educación Superior (ANUIES) es una asociación no gubernamental de carácter plural que agrupa a las principales Instituciones de Educación Superior (IES) de México, promoviendo su mejoramiento integral y el de la educación superior en los campos de la docencia, la investigación y la extensión de la cultura y los servicios.

En el marco de las tecnologías de información, y en específico de la seguridad de la información de las IES, la ANUIES y sus redes regionales en este campo, en conjunto con la Universidad Nacional Autónoma de México (UNAM) y su Equipo de Respuesta a Incidentes de Seguridad en Cómputo (UNAM-CERT), conformaron la Red Nacional de Seguridad en Cómputo (RENASEC). La Red Nacional de Seguridad en Cómputo (RENASEC) es reconocida oficialmente desde octubre de 2003 por la Asamblea General de rectores y directivos representantes de las IES como una de sus redes estratégicas.

La RENASEC, con la coordinación técnica de UNAM-CERT y el apoyo constante de las Redes Regionales de Seguridad en Cómputo de la ANUIES, ha promovido acciones de trabajo conjunto entre las IES, de donde surgió el requerimiento de contar con indicadores que permitan identificar sus necesidades en este ámbito, por lo que desde el año 2002 se elaboró una encuesta cuyos resultados serían la base de un diagnóstico sobre el estado de la Seguridad en Cómputo de las IES del país. Este diagnóstico funcionó como la primera "radiografía" de la situación de las IES en México y fue un factor determinante para el desarrollo de significativas propuestas y acciones.

Es importante hacer notar que la participación de las IES en la encuesta en 2002 -la primera en su tipo entre las IES en México- fue de 51%, lo cual refleja una respuesta positiva a la convocatoria.

Para el año 2006 se formuló una segunda encuesta de seguridad en cómputo de las IES, que tuvo una participación del 70% de ellas. Dicha encuesta se encaminó a determinar el nivel de seguridad con que contaban las IES afiliadas a la ANUIES, además de conocer con detalle su entorno tecnológico. El resultado del diagnóstico 2006 fue la base para formular propuestas de la ANUIES orientadas al desarrollo de la seguridad en cómputo, entre las que destacan dos Diplomados en Tecnologías de Seguridad de la Información (Fideicomiso SEP-UNAM), la creación del sitio web de la RENASEC, el intercambio de experiencias entre las IES durante las reuniones de la redes regionales y la reunión nacional de la RENASEC, promoción de la normatividad mediante políticas regionales de seguridad en cómputo de las IES y, formación de capital humano en atención a incidentes de seguridad en cómputo en las IES mediante TRANSITS (*Training of Network Security Incident Teams Staff*).

Para 2011, la Dirección de Cómputo y Sistemas de la ANUIES, en coordinación con el UNAM-CERT de la UNAM elaboraron un modelo inicial de reactivos. El modelo fue revisado y enriquecido con la aportación de otras IES para diseñar una nueva encuesta con el objetivo de desarrollar indicadores de seguridad en TI que permitieran identificar el estado actual de seguridad, así como necesidades y áreas de oportunidad. Las instituciones afiliadas que con la coordinación de la ANUIES participaron en el diseño enriquecido de la encuesta 2011 fueron la Universidad Autónoma de Yucatán (UADY), el Instituto Tecnológico de Sonora (ITSON), la Universidad Autónoma de Querétaro (UAQ), y la Universidad Nacional Autónoma de México (UNAM-CERT).

La implementación tecnológica del sistema de información para el registro en línea se realizó en la ANUIES, en tanto el procesamiento de los datos y la conformación del documento con la interpretación de resultados, conclusiones y recomendaciones la efectuaron los responsables de seguridad en TI de la UNAM-CERT, la UADY, la UAA y la ANUIES.

Este documento es un reflejo de las necesidades que las IES plasmaron en la encuesta de seguridad 2011 de la RENASEC. Incluye un resumen ejecutivo, el desglose de los resultados en las distintas categorías de nivel de participación de las IES, información sobre su infraestructura tecnológica general, necesidades de formación y capacitación y los estándares de seguridad o buenas prácticas que actualmente aplican en sus instituciones. Asimismo se incorpora información de resultados en cuanto al manejo de emergencias ante incidentes de seguridad en tecnologías de información y se hace mención de las medidas de prevención que se aplican en la disminución de la inseguridad en las IES.

De manera complementaria, se formula una serie de conclusiones sobre los resultados captados en la Encuesta de Seguridad en TI, y se agregan recomendaciones basadas en la experiencia técnica en seguridad de TI del Equipo de Respuesta a Incidentes de la UNAM (UNAM-CERT), de la Universidad Autónoma de Yucatán, de la Universidad Autónoma de Aguascalientes y de la ANUIES.

El impacto de este documento plasmará de manera formal los principales indicadores de seguridad en tecnologías de información, y ayudará en una detección de necesidades que nos permita definir las áreas de oportunidad, lo cual fundamentará la generación de recomendaciones técnicas y estratégicas con un enfoque de trabajo colaborativo entre las IES de las distintas regiones que conforman la ANUIES.

RESUMEN EJECUTIVO

13

INTRODUCCIÓN

La Red Nacional de Seguridad en Cómputo (RENASEC), como parte de sus actividades fundamentales, en 2003 elaboró la primera encuesta nacional de seguridad en cómputo en las instituciones de educación superior mexicanas, cuyos resultados bosquejaron la primera "radiografía" de la situación en ese ámbito en el país, que fue un factor determinante para la elaboración de importantes propuestas y acciones en este campo. En 2006 se formuló una segunda encuesta de seguridad en cómputo, con una participación muy significativa de las universidades e instituciones de educación superior del país. En los resultados del diagnóstico 2006 se identificaron áreas de oportunidad orientadas al fortalecimiento de aspectos relacionados con la cooperación, el capital humano, la infraestructura tecnológica, la normatividad en seguridad, los esquemas de seguridad y el manejo de incidentes de seguridad en TI de las IES.

En 2011 la RENASEC elaboró una nueva encuesta con el objeto de desarrollar los indicadores generales de seguridad en TI, con el sustento de los requerimientos identificados en las encuestas anteriores (2003 y 2006), y que permitiera detectar nuevas necesidades y áreas de oportunidad y finalmente, generar recomendaciones y líneas de acción con un enfoque de trabajo colaborativo entre las IES de las distintas regiones que conforman la ANUIES.

Los reactivos de la encuesta 2011 se orientaron a los siguientes temas: información general, infraestructura tecnológica, capital humano, esquemas de seguridad, estándares y buenas prácticas de seguridad de la información, manejo de incidentes y prevención.

RESULTADOS CLAVE

- De las 159 instituciones que se convocaron entre septiembre y noviembre de 2011 a nivel nacional, se recuperaron 119 encuestas (74.8%) atendidas puntualmente.
- En cuanto a los enlaces de telecomunicaciones de banda ancha, es importante hacer notar que para las necesidades de las IES del país son insuficientes, no obstante, desde la perspectiva académica, la tendencia de las IES que más se acerca a satisfacer estas necesidades es la incorporación al proyecto "Internet 2" que coordina la Corporación Universitaria para el Desarrollo de Internet (CUDI).
- En cuanto a equipamiento de cómputo a nivel de usuario final y con acceso a Internet, algunas IES cuentan con grandes cantidades de equipamientos, predominando los rangos desde 100 a 500 equipos (20% del total), hasta 1000 a 2500 equipos (24% del total). Esto denota una tendencia muy fuerte hacia un gran alcance de equipos conectados a Internet, lo cual potencializa los posibles aumentos en vulnerabilidades, amenazas y riesgos. Es muy importante hacer notar que no se incluyeron los dispositivos móviles que son una cifra significativa en la utilización de recursos de red de las IES.
- Sólo el 18% (21 IES) tienen implementado el protocolo IPv6, lo cual denota retos tecnológicos de las IES para evolucionar hacia la conectividad mundial y la seguridad de las redes. De las pocas IES que han implementado el protocolo IPv6, sólo destacan las aplicaciones de tipo experimental.
- En relación a necesidades de concientización y formación en seguridad de TI a nivel de usuario final en las IES, prevalecieron los temas de las "buenas prácticas en el uso de Internet", el "antimalware", las "redes sociales", el "uso seguro de aplicaciones de Internet", entre otros.
- Acorde con las necesidades de formación de personal especializado en seguridad de TI en las IES, éstas se orientaron hacia la formación en tópicos como "el monitoreo y seguridad de las redes", "la seguridad en el desarrollo de sistemas"; "el manejo adecuado de incidentes" y "los estándares de seguridad", entre otras.

- El 86% de las IES cuenta con responsables de seguridad en TI. No obstante, en muchos de los casos, dichos responsables de seguridad en TI, al mismo tiempo, también son los encargados de otras actividades afines a la tecnología, a la docencia, o cargos diversos. De las IES que respondieron la encuesta, sólo 19 (18.6) cuentan con el cargo de "Oficial de Seguridad de la Información".
- De las IES que respondieron a la encuesta en línea, 102 cuentan con un área dedicada a la Seguridad en TI. La ubicación de éstas áreas es muy variable, predominando como responsables las áreas de TI y Auditoría.
- Solo el 39% de las IES ha establecido algún plan de seguridad en TI.
- Entre las IES participantes, el 87% cuenta con mecanismos de protección física. Uno de los retos de la seguridad física, es la convergencia con la seguridad lógica (Seguridad convergente).
- El 47% de las instituciones participantes cuentan con certificaciones en estándares de TI o estándares de seguridad en TI.
- El 86% de las IES cuenta con lineamientos, políticas, reglamentos o normatividad general, apoyados en estándares de operación o aspectos legales.
- El 56% de las IES aplica cláusulas de confidencialidad en los documentos legales.
- El 35.29% de las IES participantes aplican procedimientos de control de cambios en sus sistemas de información e infraestructura tecnológica.
- El 97% de las instituciones que respondieron reportan sus incidentes de seguridad en TI hacia el interior y ante organizaciones de apoyo como los centros o equipos de atención a incidentes.
- De las IES participantes en la encuesta, el 93% responde inmediatamente a sus incidentes de seguridad en TI.
- El 76% además de dar respuesta inmediata a sus incidentes de seguridad en TI, también da continuidad al seguimiento posterior de los mismos para detectar las causas que los originan y evitar que se repitan.
- El 73% de las IES participantes aplican ciertas medidas preventivas con el objetivo de disminuir la inseguridad tecnológica.

CONCLUSIONES

- El nivel de participación de las IES fue muy satisfactorio, (74% de las IES que conforman a la ANUIES). Sin embargo, el reto futuro deberá implicar a una mayor cantidad de IES interesadas en participar en el proyecto de diagnóstico.
- La infraestructura tecnológica ha evolucionado en las IES, no obstante, la seguridad sigue siendo un gran reto que implica aspectos que van desde el robustecimiento de equipamientos y las telecomunicaciones hasta la formación de especialistas para la operación segura. El incremento de los dispositivos móviles debe ser atendido adecuadamente para evitar consecuencias negativas.
- El capital humano es un factor determinante para la seguridad en todos los niveles de usuarios, tanto de las aplicaciones básicas, hasta los especialistas que operan las infraestructuras tecnológicas de las IES. La concientización en todos los niveles de usuarios de tecnologías de información es esencial para conformar una cultura de la seguridad en las IES.
- La definición y aplicación adecuada de esquemas de seguridad en las IES es crucial para contrarrestar los riegos que éstos conllevan.
- Pese a que gran cantidad de IES están conscientes de la importancia de los estándares y buenas prácticas de seguridad de la información, habrá que hacer extensiva su promoción en todas las IES.
- Pese a que la mayoría de las IES afirma que da atención de sus incidentes de seguridad en TI (97%), es muy importante concientizar y actualizar constantemente a sus responsables de seguridad y administradores de TI en la aplicación de procedimientos y documentación para su óptimo seguimiento.
- Un buen porcentaje de IES (73 %) aplican medidas preventivas para contrarrestar las amenazas de seguridad en TI, sin embargo, dichas medidas se orientan en su mayoría hacia el personal técnico, lo cual hace mandatorio considerar acciones preventivas para usuarios finales de las tecnologías de información.

RECOMENDACIONES

- Mantener la realización anual del diagnóstico nacional entre las IES afiliadas a la ANUIES, con el fin de gene-

rar estrategias colaborativas de seguridad en TI más efectivas en su ejecución.

- Establecer los esquemas de administración para equipos de cómputo y para dispositivos móviles que consideren la generación y aplicación de políticas de uso, y el establecimiento de mecanismos de seguridad reductores de los riesgos que presentan estos dispositivos.
- Se requiere capacitación especializada, formación con experiencia técnica y la actualización constante del capital humano hacia el interior de las IES, y personal formado por las propias IES.
- Es importante contar con recursos propios hacia el interior de las IES (Infraestructura de *hardware* y *software*), promoviendo la autodeterminación tecnológica a nivel institucional y evitando con esto ser clientes cautivos para los proveedores comerciales de tecnología.
- Uno de los retos de la seguridad física, es la convergencia con la seguridad lógica. Se debe trabajar en una cultura de la seguridad convergente en las IES.
- Es importante alinearse con estándares de seguridad de todos los servicios tecnológicos que las IES demandan con la idea de impulsar las buenas prácticas de seguridad en TI.
- Las buenas prácticas en el uso de sistemas operativos conllevarán a resolver problemáticas que están bajo el alcance de los administradores de TI, y la forma de solucionarlo es la actualización de los sistemas, y el buen uso de éstos mediante las políticas y la formación de capital humano especializado.
- El papel del responsable de seguridad en TI es fundamental en cualquier organización y la capacitación y actualización constantes deben ser una de las principales líneas de acción a seguir. Es importante contar con un responsable de seguridad en TI con "perfil de puesto dedicado" en cada IES, con una visión integral de la seguridad de la información alineada con los objetivos estratégicos institucionales. En el perfil del responsable debe enfatizarse un nivel que le permita tomar decisiones hacia el interior de la institución.
- Es fundamental para los responsables de seguridad de las IES contar con los conocimientos teóricos y prácticos de los estándares de seguridad en TI, además de la generación de normatividad y documentación de buenas prácticas orientadas hacia el buen uso de los recursos tecnológicos y de la información para ser aplicados hacia el interior de las instituciones.
- Es muy importante para las IES contar con la documentación de sus procedimientos de control de cambios de sus sistemas de información e infraestructuras tecnológicas, facilitando la identificación, almacenamiento y protección de la información.
- Es importante establecer la formación en cuanto al seguimiento de incidentes de seguridad en TI en las IES, generando beneficios orientados a las buenas prácticas para la adecuada coordinación de respuesta a los mismos.
- Es fundamental la conformación de programas de concientización orientados hacia la difusión de una cultura de la seguridad en TI que permita fortalecer el eslabón más débil de la seguridad: el usuario final.
- Es importante que la IES considere un presupuesto anual para la adquisición, actualización y mantenimiento de sus esquemas de seguridad que involucra estándares, políticas, personal y tecnología entre los elementos más importantes.

METODOLOGÍA

17

La encuesta de Seguridad en Tecnologías de Información 2011 fue dirigida a los responsables, institucional y técnico, designados o ratificados por las autoridades de las 159 IES afiliadas a la ANUIES entre septiembre y noviembre de 2011.

El registro de datos en la encuesta se llevó a cabo mediante un sistema en línea con distribución de claves de acceso para cada institución. En cuanto a la elaboración de reactivos, se conformó un breve cuestionario de 24 preguntas distribuidas en las siguientes categorías de información, las cuales se conformaron teniendo como base la experiencia de encuestas anteriores:

Información general

En esta categoría se contemplaron datos generales como el nivel de participación, el nombre de la IES, la región de la ANUIES a la que pertenece la IES y el tipo de IES, además de los datos de contacto de los responsables de responder la encuesta.

Infraestructura tecnológica

Registro de información sobre la capacidad instalada en las IES en cuanto a las infraestructuras de telecomunicaciones y las capacidades de cómputo de usuario final y equipos servidores conectados a Internet. Se contemplaron los tipos de servicios de red que prestan las IES a su comunidad académica y se recopiló información general sobre la implantación de tecnologías de red avanzadas, como el protocolo IP versión 6 (IPv6) e Internet 2. Finalmente, se consideraron los tipos de sistemas operativos con que las IES cuentan, con el objetivo de detectar su frecuencia de uso en las IES y problemáticas de seguridad asociadas a los mismos.

Capital humano

Identificación de las necesidades de concientización y capacitación en seguridad, tanto a nivel de usuarios finales como a nivel de administradores de TI. Además, se contempla el puesto que tienen los responsables de seguridad en TI de las IES y la ubicación de su área de adscripción en la estructura organizacional.

Esquemas de seguridad

Identificación de esquemas de seguridad en TI para la protección de los sistemas de información, así como los planes de aseguramiento de la infraestructura tecnológica de las IES. También se incluyeron aspectos relacionados con la protección de los bienes e instalaciones físicas de la institución (seguridad física).

Estándares y buenas prácticas de seguridad de la información

Información sobre certificaciones y capacitación en buenas prácticas de seguridad en TI de las IES. Adicionalmente, se incluyó información relativa a disposiciones de tipo normativo que las IES han incorporado, complementando con información de cláusulas que se apliquen en convenios o contratos. Asimismo, se recopiló información sobre la gestión del cambio en la infraestructura de TI en las IES.

Manejo de incidentes

Incidentes de seguridad en TI que las IES reportaron en los 12 meses anteriores a la aplicación de la encuesta (septiembre-noviembre de 2011). Se complementó con información sobre los tipos de acciones de respuesta inmediata

ante incidentes, así como las actividades de seguimiento a medidas preventivas y correctivas derivadas de los mismos.

Prevención

Finalmente, se contempló el registro de las medidas de prevención que las IES aplican para evitar incidentes, así como la identificación de los incidentes más frecuentes desde la perspectiva de usuario final que se reportaron durante el último semestre (antes de septiembre-noviembre de 2011).

El uso de la información de esta encuesta está orientado a fines académicos y sin fines de lucro, lo cual permitirá utilizar la encuesta libremente entre las IES afiliadas a la ANUIES haciendo la respectiva referencia a la misma.

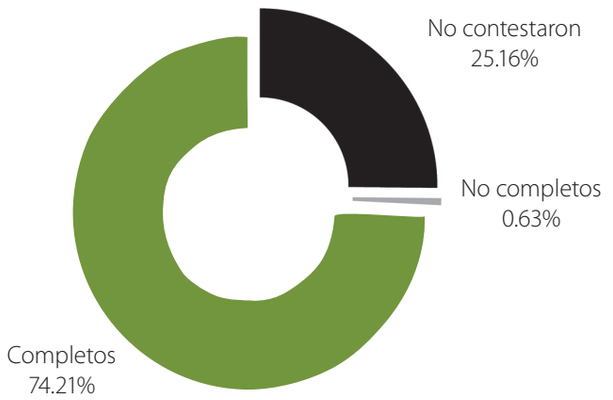
RESULTADOS GENERALES

INFORMACIÓN GENERAL

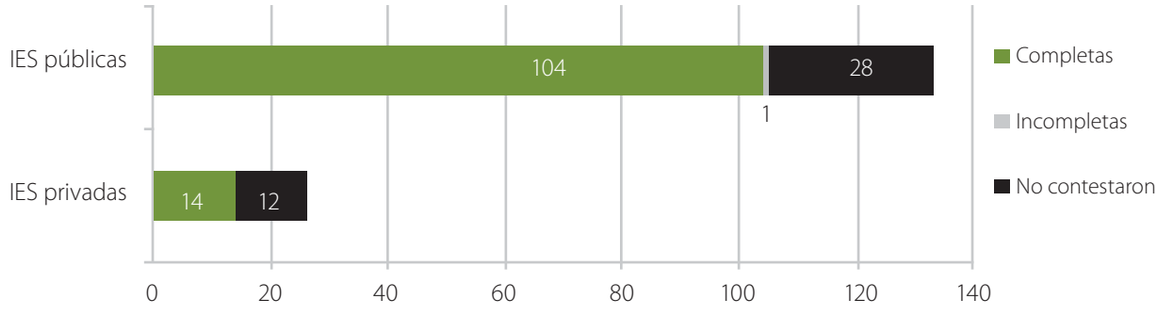
Nivel de participación de las IES

Entre septiembre y noviembre de 2011 se convocó a 159 instituciones de educación superior a nivel nacional, de las cuales 119 atendieron la encuesta, lo que significa una participación del 74.8% (gráfica 1).

Gráfica 1 Porcentaje de participación en la encuesta



Gráfica 2 Participación por tipo de institución



De las 119 instituciones participantes, 105 son públicas y 14 son privadas (gráfica 2).

La distribución de la participación por regiones de la ANUIES se muestra en la gráfica 3. Es destacable el nivel de participación de las IES de las regiones Centro-Sur, Sur-Sureste y Noroeste.

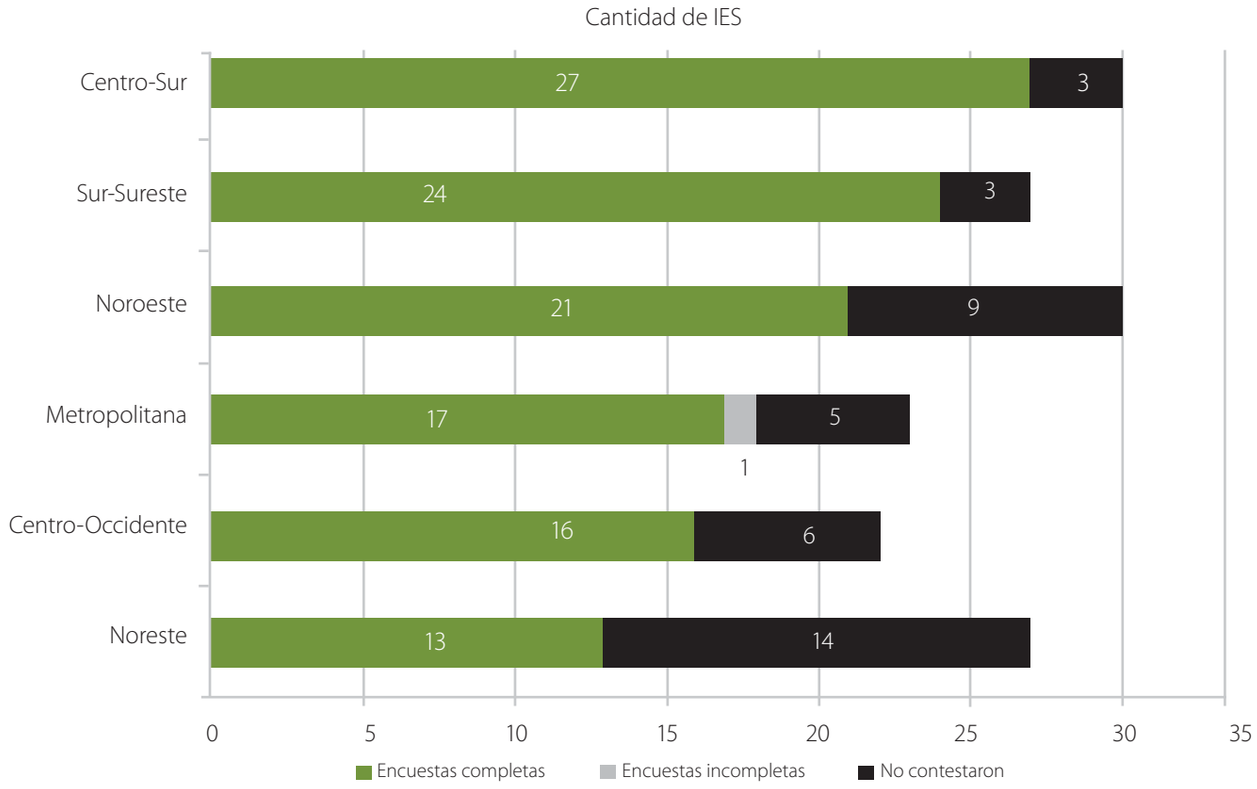
No obstante cabe destacar la amplia convocatoria que han tenido algunas regiones de la ANUIES en cuanto a proyectos de la Red Nacional de Seguridad en Cómputo (RENASEC), lo cual, con la constancia de sus coordinadores regionales, reflejó muy buen nivel de participación de la encuesta 2011.

INFRAESTRUCTURA TECNOLÓGICA

Enlaces de telecomunicaciones

Actualmente, para las IES al igual que para muchas organizaciones, la conexión a Internet es un elemento crítico de la infraestructura tecnológica necesaria para desarrollar sus actividades fundamentales: docencia, investigación, vinculación, difusión de la cultura. Servicios tales como el

Gráfica 3 Nivel de participación por regiones de las 159 IES convocadas a nivel nacional



correo electrónico, portales web, foros interactivos, y demás aplicaciones en la red son un pilar del funcionamiento operativo, académico y administrativo de una institución de educación superior en nuestro país.

De acuerdo con la gráfica 4, ha habido una gran evolución desde que se implementaron los primeros enlaces de telecomunicaciones en las IES de nuestro país. La oferta de telecomunicaciones se ha incrementado y diversificado, en tecnología y proveedores, lo que sin duda ha facilitado el acceso a mejor tecnología de conectividad para las IES (gráfica 4), aunque de forma general el ancho de banda con que las universidades se conectan a Internet está lejos incluso del que países como Estados Unidos tenía en 2008[1]. Las instituciones requieren todavía de una mayor capacidad de transmisión de datos ante una inminente evolución de las aplicaciones, las cuales tienden a ser cada vez más robustas y demandantes.

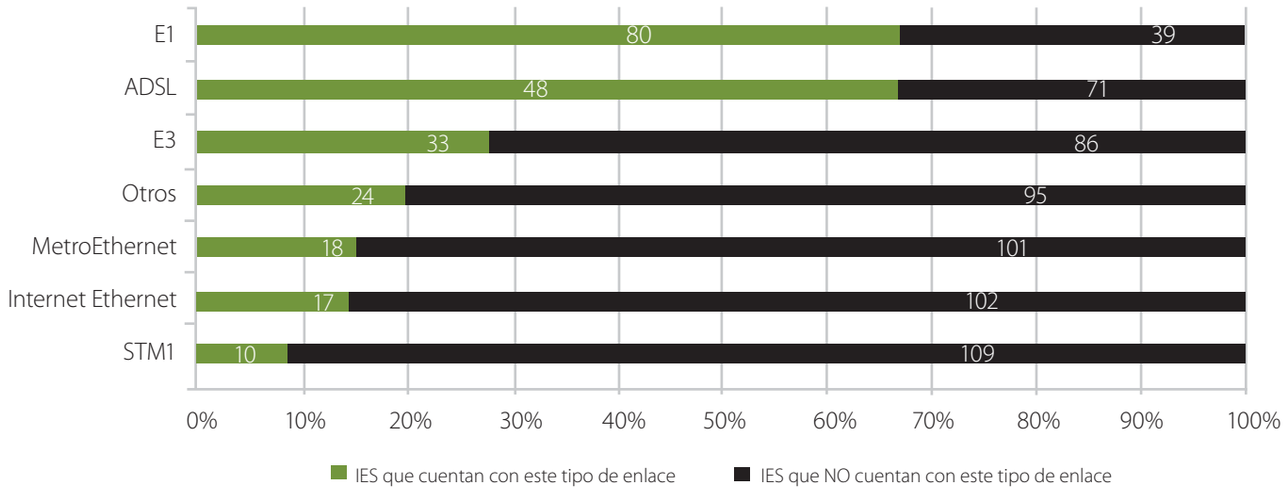
Equipos de cómputo a nivel de usuario final con acceso a Internet

Respecto de la cantidad de equipos de cómputo fijo que se utilizan al interior de las instituciones en áreas como los centros de cómputo, los laboratorios, oficinas administrativas, entre otros, que son fundamentales para el desarrollo de las actividades de estudiantes, académicos, y personal administrativo de cualquier IES, los resultados indican que las instituciones de educación superior en México, por la población de cada una, están en rangos muy diversos. De acuerdo con la encuesta, el 20% de las IES cuenta con más de 5,000 equipos, el mismo porcentaje representa a instituciones que tienen entre 100 y 500 (gráfica 5). En todos los casos, hay una gran cantidad de equipos conectados a Internet, lo que representa un reto importante para la gestión y optimización de los mismos y de la infraestructura de conectividad asociada.

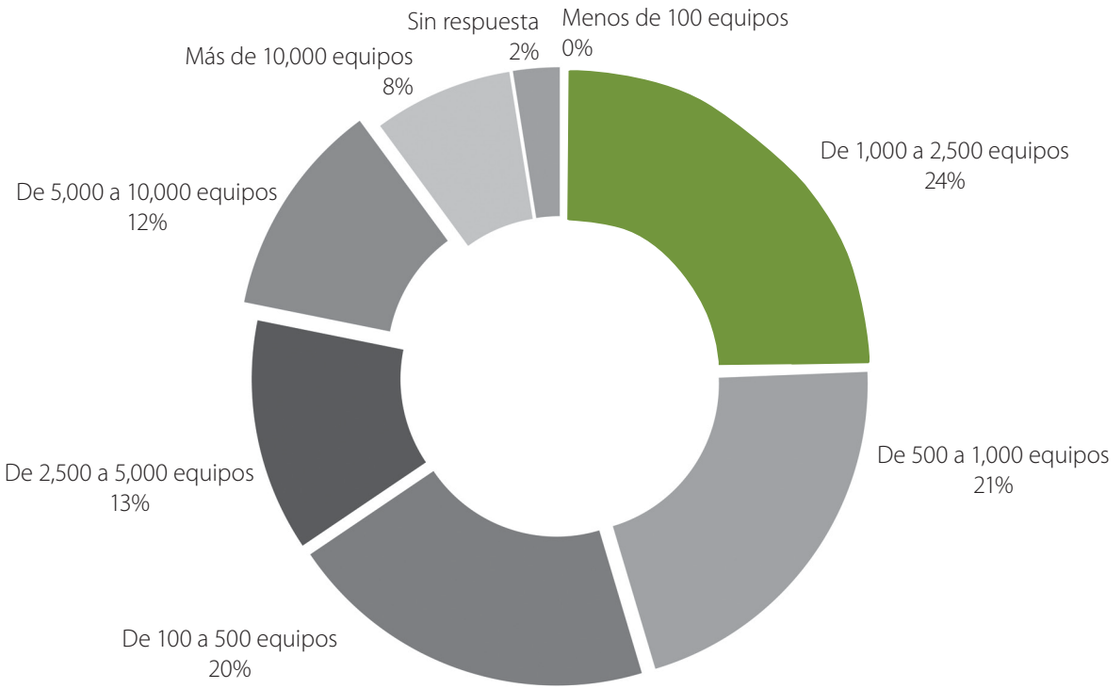
Es importante hacer notar que no se incluyeron los equipos o dispositivos móviles que son una cifra importante y en crecimiento en la utilización de recursos de red de las IES. La masificación del uso de dispositivos móviles

1 http://www.nsf.gov/statistics/infbrief/nsf10328/

Gráfica 4 Enlaces de telecomunicaciones



Gráfica 5 Porcentaje de equipos de cómputo con acceso a servicios Internet a nivel de usuario final



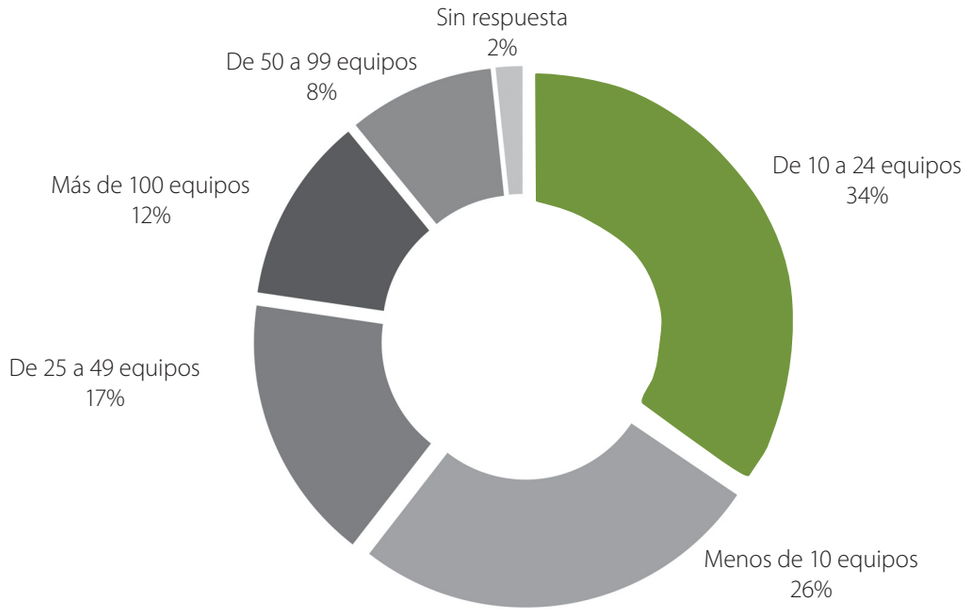
representa uno de los principales retos en cuanto a requerimientos de conectividad y seguridad de la información.

Equipos servidores con que cuentan las IES

El incremento en la cantidad y alcance de los servicios de TI que requieren las IES ha implicado una mayor inversión en infraestructura de equipos servidores, los cuales se han especializado en función de las necesidades académicas y administrativas de las instituciones.

Todas las IES que respondieron a la encuesta cuentan con al menos una decena de equipos servidores y, en algunos casos, hasta con más de 100 (gráfica 6). La especialización de los servicios que se proporcionan a través de esta

Gráfica 6 Porcentaje de equipos servidores con que cuentan las IES



infraestructura implica también la identificación y satisfacción de necesidades asociadas a la operación de la misma, como aplicación de mejores prácticas y capacitación de los responsables de administrar los sistemas y la seguridad informática para los diversos tipos de sistemas.

Tipos de servicios que brindan los equipos servidores

Entre los servicios y aplicaciones que las IES soportan con su infraestructura de TI destacan las páginas web, el correo electrónico y las redes sociales. Asimismo, destacan las aplicaciones de gestión interna de una IES, como los sistemas administrativos, de control escolar, bibliotecas, información sobre ingreso, entre otros.

Es importante destacar la operación de servicios de TI para educación a distancia, infraestructura de llave pública y la virtualización de muchos de estos servicios (gráfica 7), ya que son tendencias globales que se han incorporado para resolver necesidades en servicios de las IES.

Entre los otros sistemas que albergan los servidores se encuentran los sistemas estatales de hacienda, y la venta de libros en línea. Y en cuanto a otros servicios técnicos, se cuenta con servidores para tareas específicas tales como: DHCP, RADIUS, FTP, Acceso Remoto VPN, servicios de almacenamiento, SSO, Videoconferencia, podcast, video-streaming, y sistemas de video-vigilancia (CCTV).

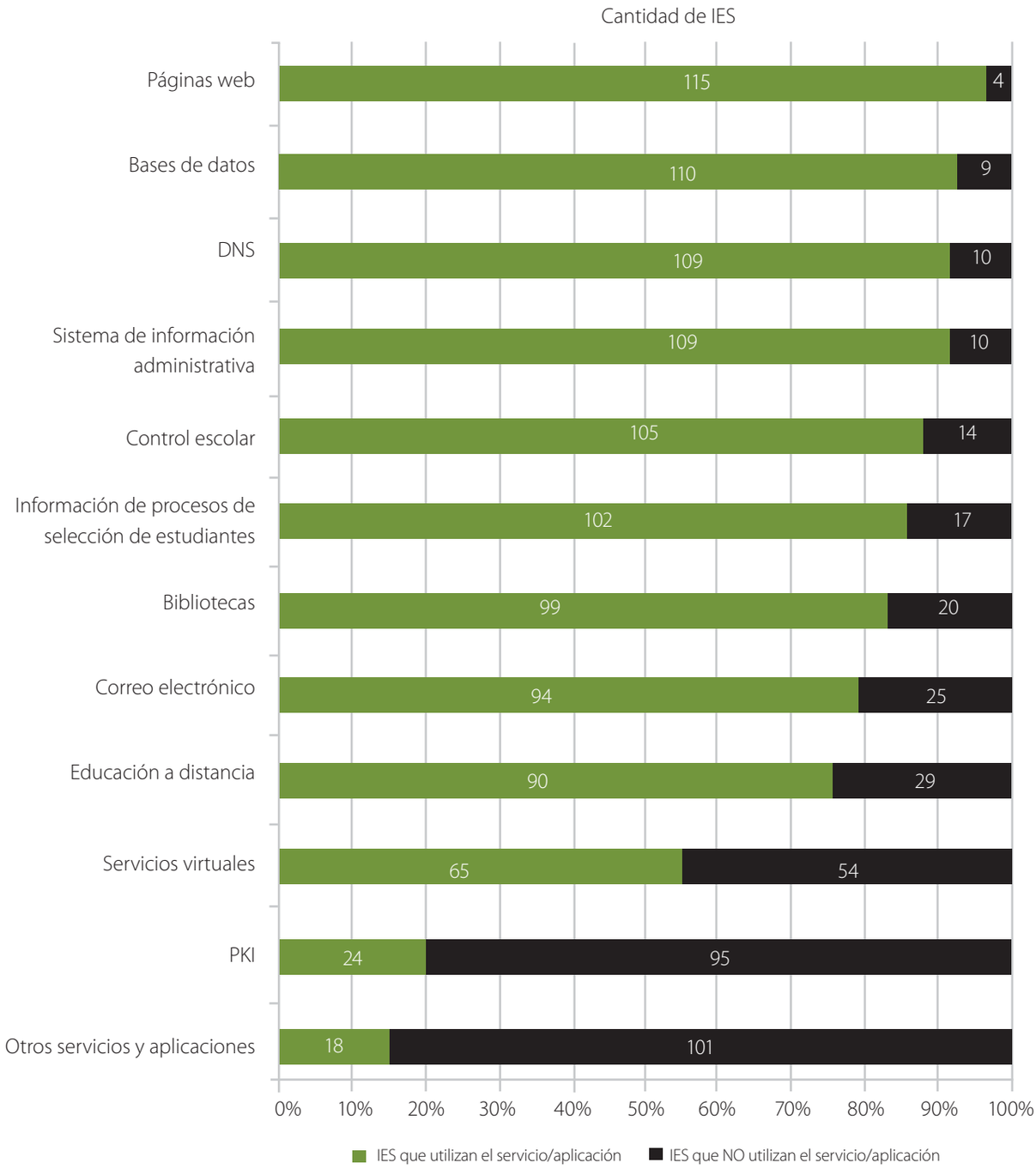
IMPLANTACIÓN DEL PROTOCOLO IPV6 EN LAS IES

La implantación del protocolo IPv6 (*Internet Protocol version 6*) para el soporte de las comunicaciones en Internet es una realidad a nivel mundial. Los países más avanzados tecnológicamente (y económicamente) llevan la vanguardia. Sin embargo, más allá de la gran ventaja tecnológica que esto implica por la capacidad de gestión de direcciones IP actualmente, así como el contraste en el rezago de los países menos implicados en ese sentido, como el nuestro, el protocolo ofrece nuevos retos de seguridad por descubrir y explorar, lo que indica que tarde o temprano será un problema por enfrentar en el cual las IES juegan un papel protagónico por su naturaleza académica y de investigación en los ámbitos tecnológicos.

La encuesta muestra que de las 119 IES que respondieron, sólo el 18% (21 IES) tienen implementado el protocolo IPv6, lo cual denota el gran reto tecnológico de las IES para adecuarse al cambio global inminente hacia esta tecnología (gráfica 8).

En cuanto al tipo de aplicaciones, en las 21 instituciones que han implementado esta tecnología, predominan los proyectos experimentales y con un mínimo de aplicaciones de tipo crítico para las instituciones académicas (gráfica 9).

Gráfica 7 Servidores en las IES

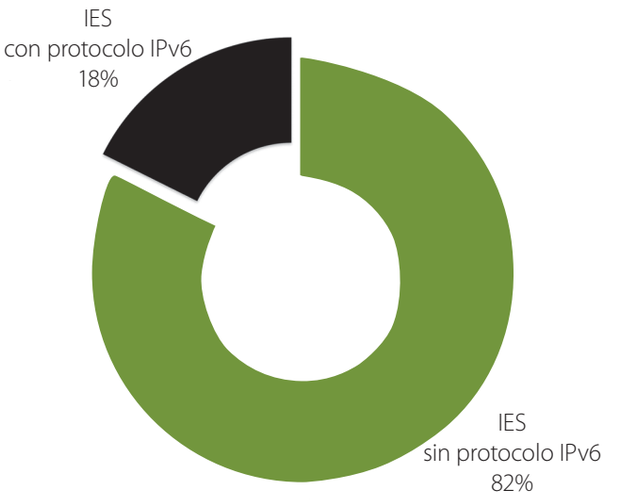


Instituciones de educación superior con aplicaciones bajo Internet 2

La necesidad de trabajar con una red Internet dedicada exclusivamente a la investigación y el ámbito académico llevó al surgimiento de la Internet 2, la cual es coordinada para el caso de México desde abril de 1999 por el Consorcio Universitario para el Desarrollo Internet (CUDI).

Cerca del 20 por ciento de las IES utilizan Internet 2, independientemente del nivel de desarrollo que cada ins-

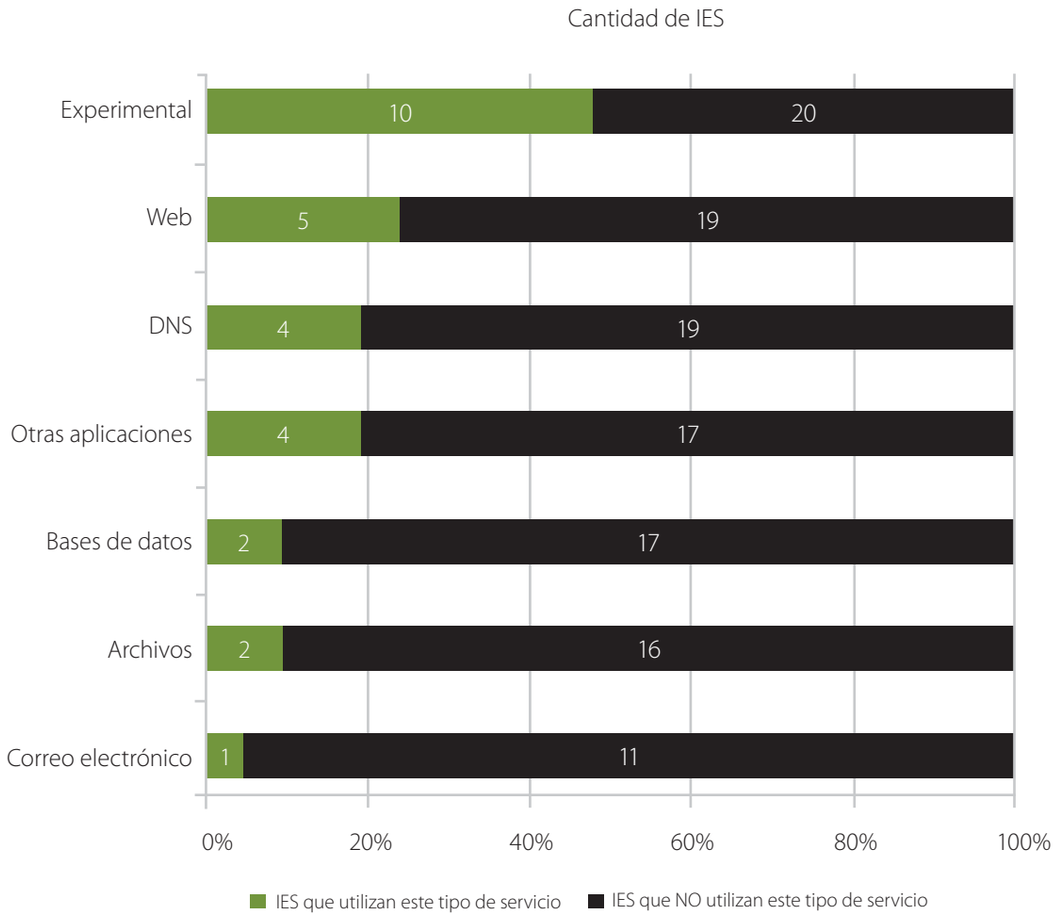
Gráfica 8 Porcentaje de IES con el Protocolo IPv6



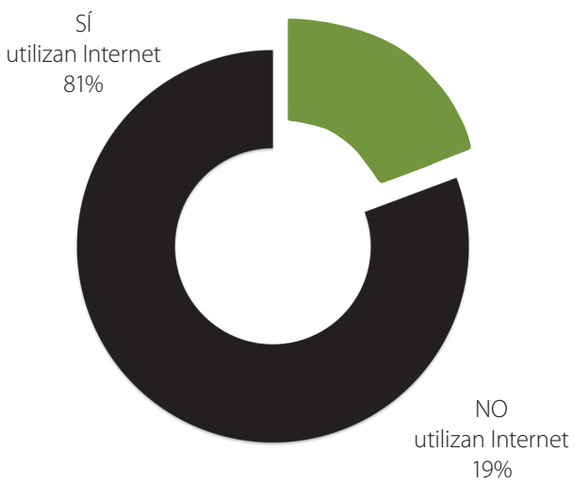
titución haya logrado en su aprovechamiento. Existen dificultades tecnológicas y económicas que las instituciones han experimentado en el desarrollo de la misma. Muchos de los retos en la gestión y uso de Internet comercial aplican también para el ámbito de las redes académicas, por lo que la seguridad de la información es un aspecto que CUDI puede impulsar en el desarrollo de este tipo de redes.

De las 119 IES que respondieron a la encuesta, el 81% (96 IES) implementaron la Internet2 (gráfica 10). Y de las 96 IES que han cambiado a la Internet2, destacan las aplicaciones en educación de diversa índole, las bibliotecas digitales, la divulgación de la ciencia, entre otras. No obstante, son pocas las IES que se orientan al desarrollo de proyectos de investigación y el desarrollo avanzado en ciencia y tecnología. Otras aplicaciones que predominan son la videoconferencia y algunos servicios de voz sobre IP (VoIP) y redes privadas virtuales (gráfica 11).

Gráfica 9 Protocolo IPv6 en las IES



Gráfica 10 Porcentaje de IES que ejecutan aplicaciones bajo Internet 2

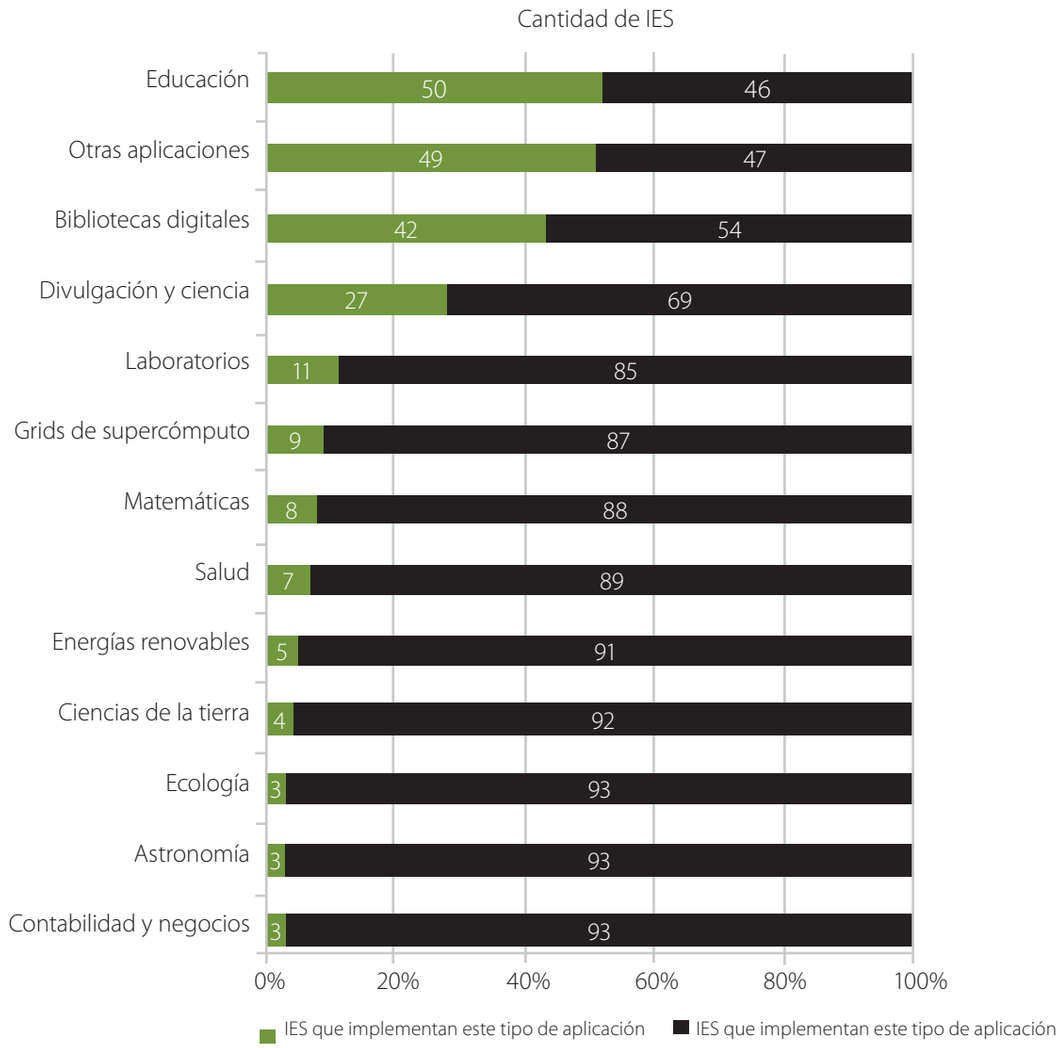


Sistemas operativos utilizados en las IES

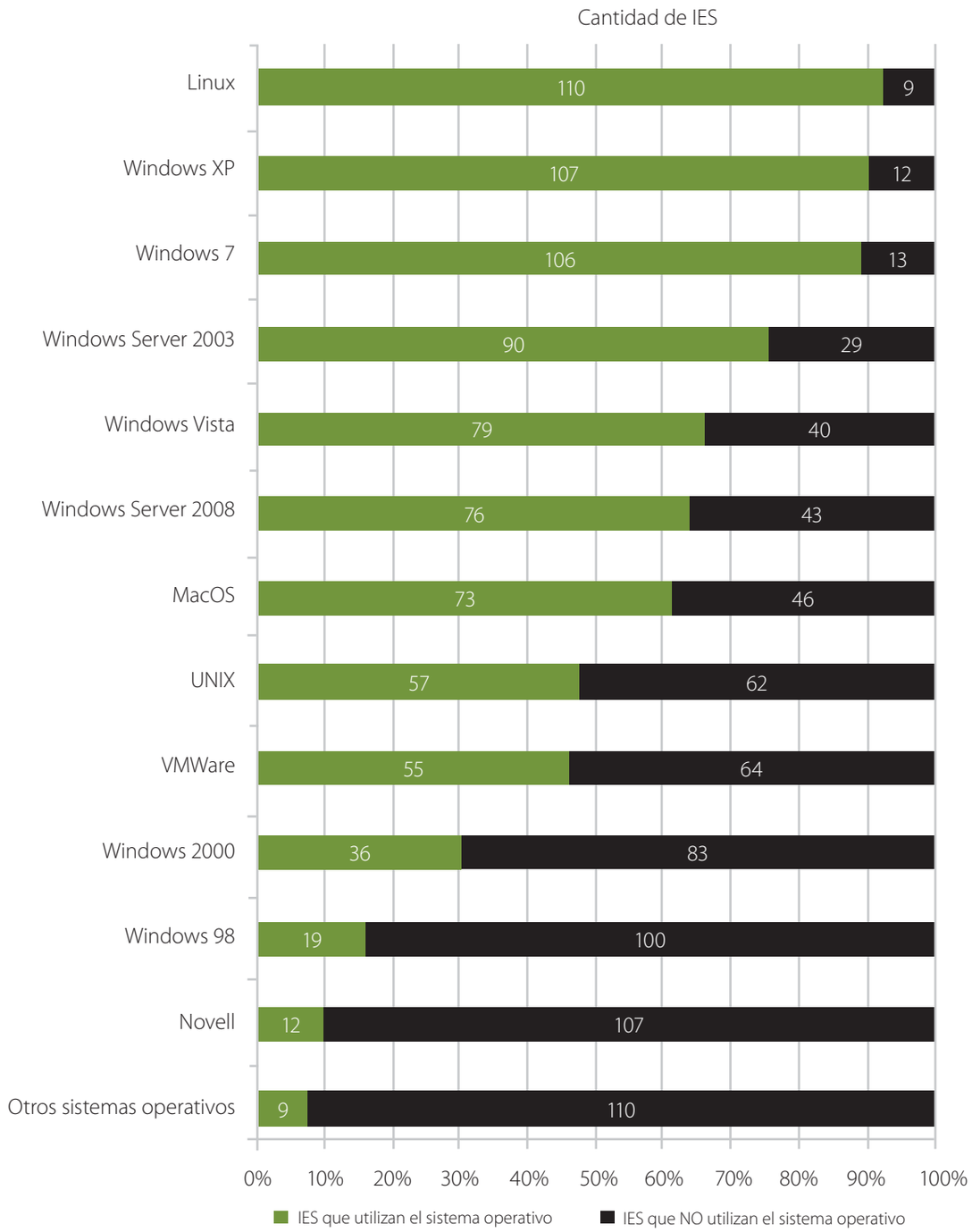
En las encuestas anteriores (años 2003 y 2005) se marcaba una fuerte tendencia hacia el uso de sistemas operativos como Microsoft Windows, y una incorporación paulatina de otros. En la actualidad, el uso de sistemas operativos se ha diversificado. Se ha incrementado el uso de sistemas operativos como Linux, MacOS y otros además de contar con una presencia relevante de los ambientes operativos basados en la virtualización (VMWare y Citrix), lo cual presenta otros retos en cuanto a la seguridad de los mismos.

Por otra parte, acorde al diagnóstico, es importante hacer énfasis en que muchas IES todavía utilizan sistemas operativos que ya son obsoletos, lo cual representa riesgos importantes de seguridad, debido a que estos sistemas ya no cuentan con mantenimiento ni actualizaciones de seguridad del fabricante (gráfica 12).

Gráfica 11 Tipo de aplicaciones bajo Internet 2



Gráfica 12 Sistemas operativos utilizados en las IES



CAPITAL HUMANO

Necesidades de concientización y formación en seguridad de TI a nivel de usuario final en las IES

La seguridad de la información es un proceso permanente en el que participan diversos elementos como tecnología (hardware y software), mejores prácticas, planes de contingencia, pero sobre todo, es un proceso en el que las personas juegan un papel fundamental. Son ellas las que conocen la información, quienes pueden clasificarla, determinar los riesgos a los que está expuesta, las medidas que deben tomarse para mitigar esos riesgos, las que administran la infraestructura tecnológica y las que hacen

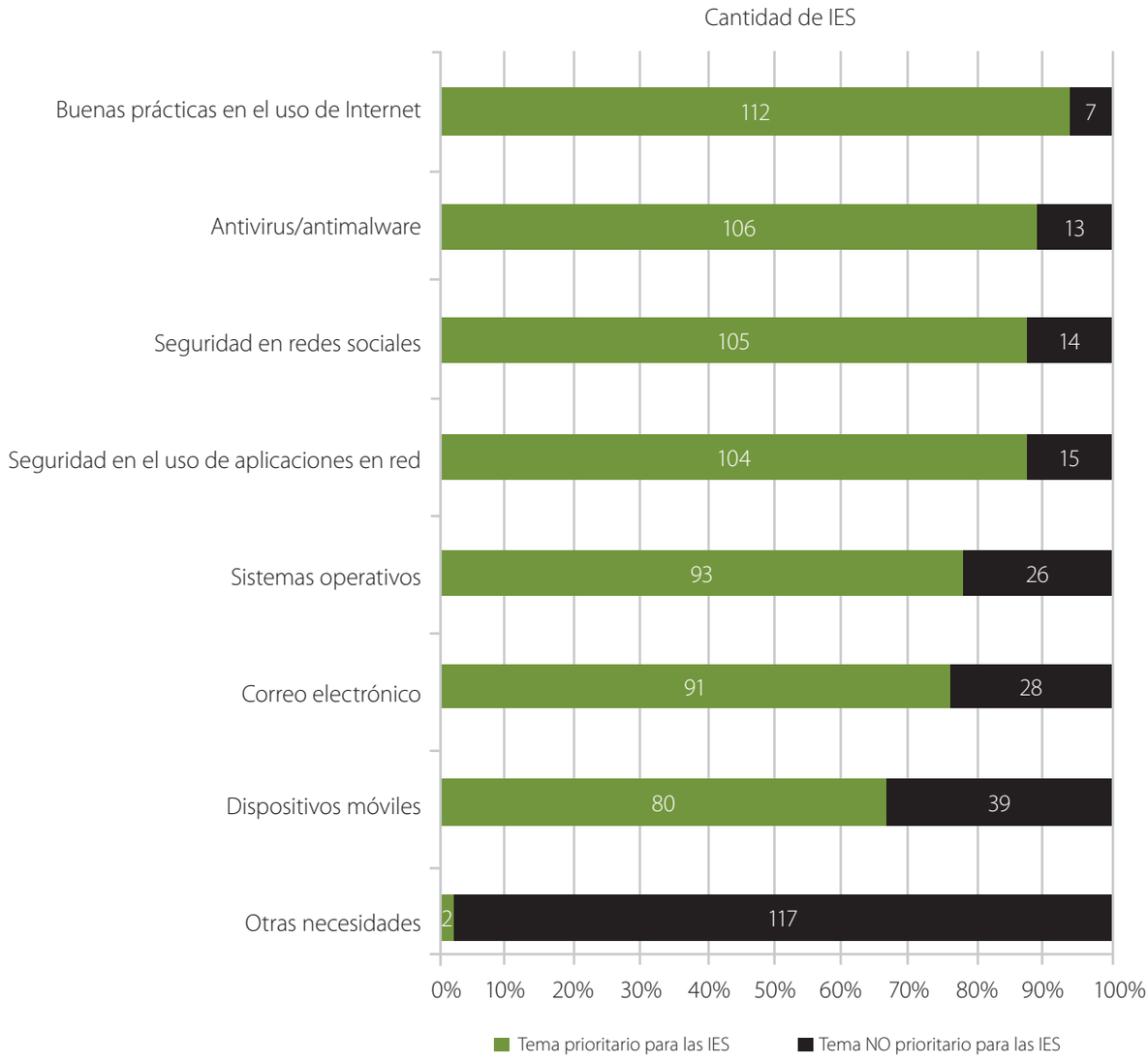
uso de la misma para el procesamiento, almacenamiento y transferencia de la información.

Es entonces que el factor humano juega un papel fundamental en el proceso de la seguridad pues las personas son quienes desarrollan la tecnología y al mismo tiempo son quienes buscan la forma de vulnerarla. Todo esto puede implicar desde la aplicación de acciones sofisticadas con un alto nivel tecnológico, hasta la utilización de la simple persuasión para obtener información crítica de las personas o de las organizaciones.

Una de las principales prioridades para la prevención y protección de los activos de información y de las propias personas es el fortalecimiento del capital humano en las IES, en donde la concientización, capacitación, formación y actualización constante de estudiantes, profesores, investigadores, personal administrativo y funcionarios, todos en general, debe ser un punto de atención prioritaria para el fortalecimiento de la seguridad de la información y servicios institucionales.

En relación al diagnóstico, de las 119 instituciones que reportaron sus necesidades de capacitación a nivel de usuario final, prevalecieron los temas de las buenas prácticas en el uso de Internet, el antimalware, las redes sociales, el uso seguro de aplicaciones de Internet. Aunque no menos importantes, también se encuentran el uso del correo electrónico de forma segura y el uso de los dispositivos móviles, los cuales son muy concurridos entre los usuarios finales (gráfica 13).

Gráfica 13 Necesidades de capacitación de seguridad en TIC a nivel de usuario final



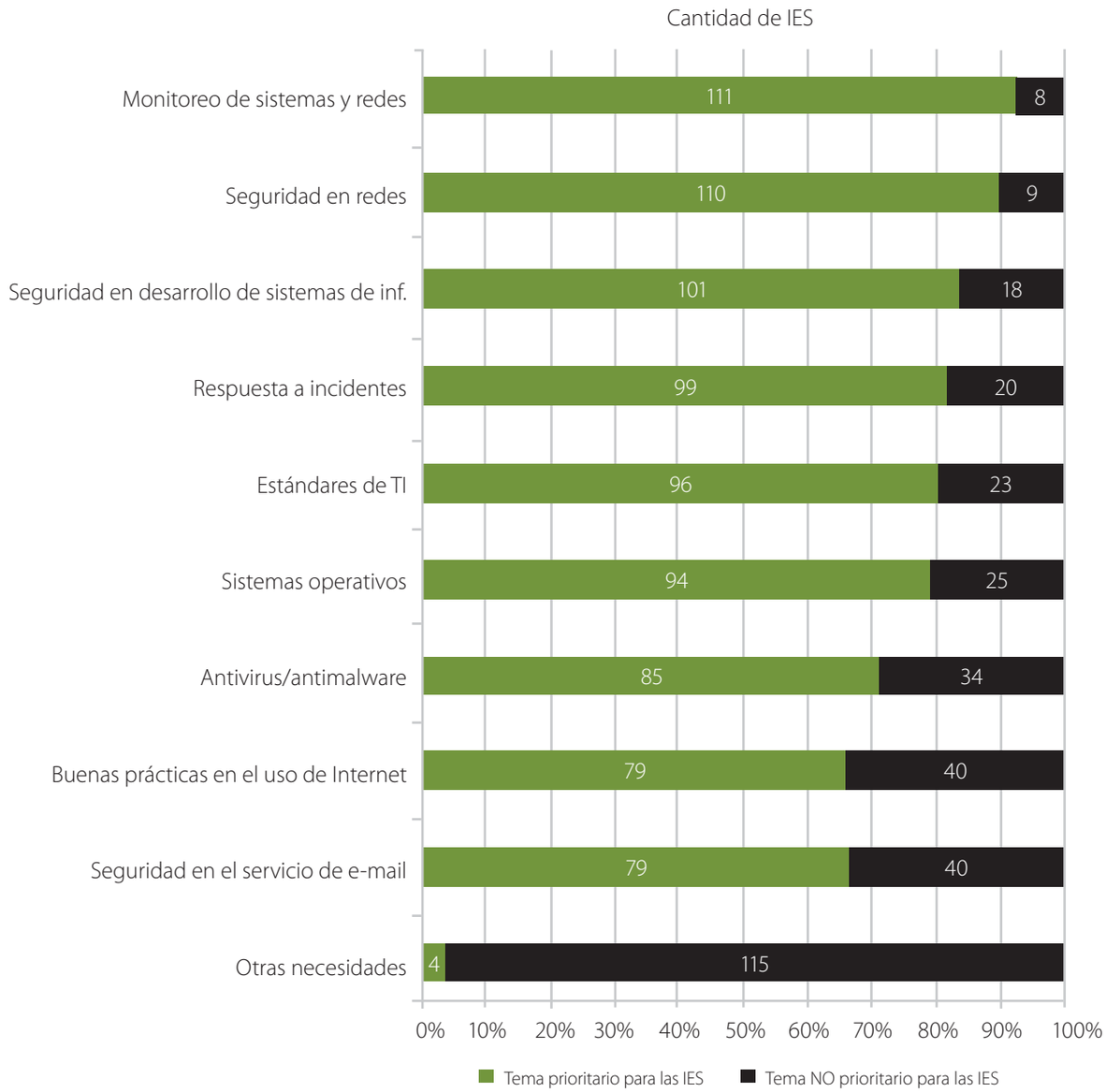
Necesidades de formación de personal especializado en seguridad de TI en las IES

El papel del responsable de gestionar la seguridad de la información, así como de los administradores de tecnologías de información y comunicación en las IES es fundamental para la óptima operación de los servicios y procesos que se apoyan en la tecnología y que incluyen lo académico y lo administrativo.

De las 119 instituciones que respondieron a la encuesta, en cuanto a requerimientos de capacitación en seguridad de la información destacan los temas orientados a administración de sistemas y tópicos de seguridad de TI. La gráfica 14 muestra que el monitoreo y seguridad de las redes es uno de los temas más presentes entre los responsables de TI de las IES.

La seguridad en el desarrollo de sistemas es también una preocupación entre los responsables de TI. Este tema es relevante ya que en las IES se desarrollan sistemas propios, a la medida, y es importante considerar la seguridad como parte fundamental del ciclo de desarrollo. Sin embargo, otros temas específicos requeridos por los administradores de TI y que no se muestran en la gráfica son los siguientes: análisis forense, análisis de riesgos, *hacking* ético, seguridad en bases de datos, seguridad en sistemas de virtualización, esquemas de respaldos y políticas de seguridad.

Gráfica 14 Necesidades de capacitación a nivel de administradores de TI

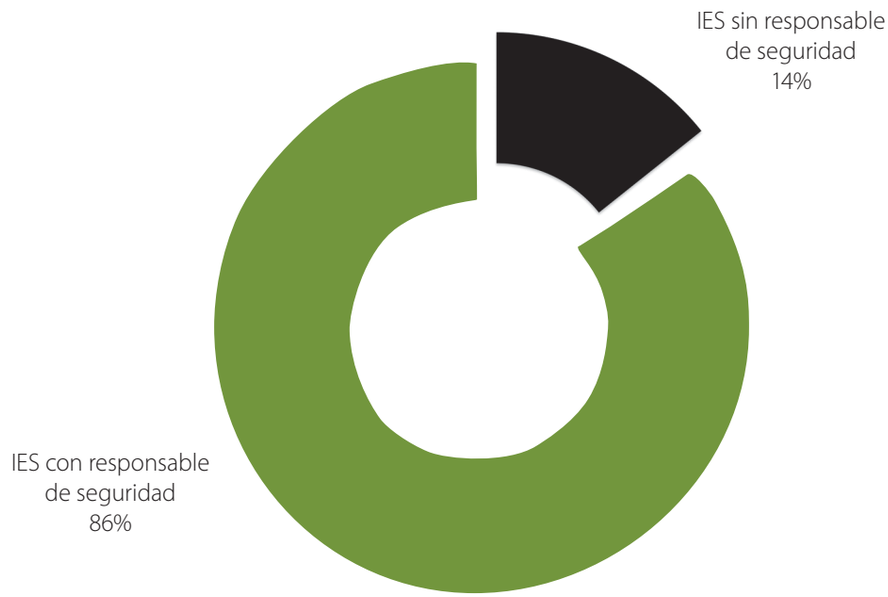


Cargo de los responsables de seguridad en TI de las IES

En organizaciones con procesos soportados en la operación de TI, como las IES, es cada vez más necesario y frecuente que exista un responsable de seguridad en TI para diseñar e implantar soluciones que permitan proteger la infraestructura tecnológica y la información.

Los resultados de la encuesta indican que de las 119 IES que respondieron, el 86% cuenta con responsables de seguridad en TI (gráfica 15). En muchos casos, los responsables de seguridad en TI también son los encargados de otras actividades de TI, docencia, administración de redes, de servidores, de centros de cómputo, de soporte técnico, de tecnologías web, profesores de tecnología y responsables de desarrollo de sistemas entre otras responsabilidades (gráfica 16).

Gráfica 15 Porcentaje de IES con personal responsable de seguridad en TI

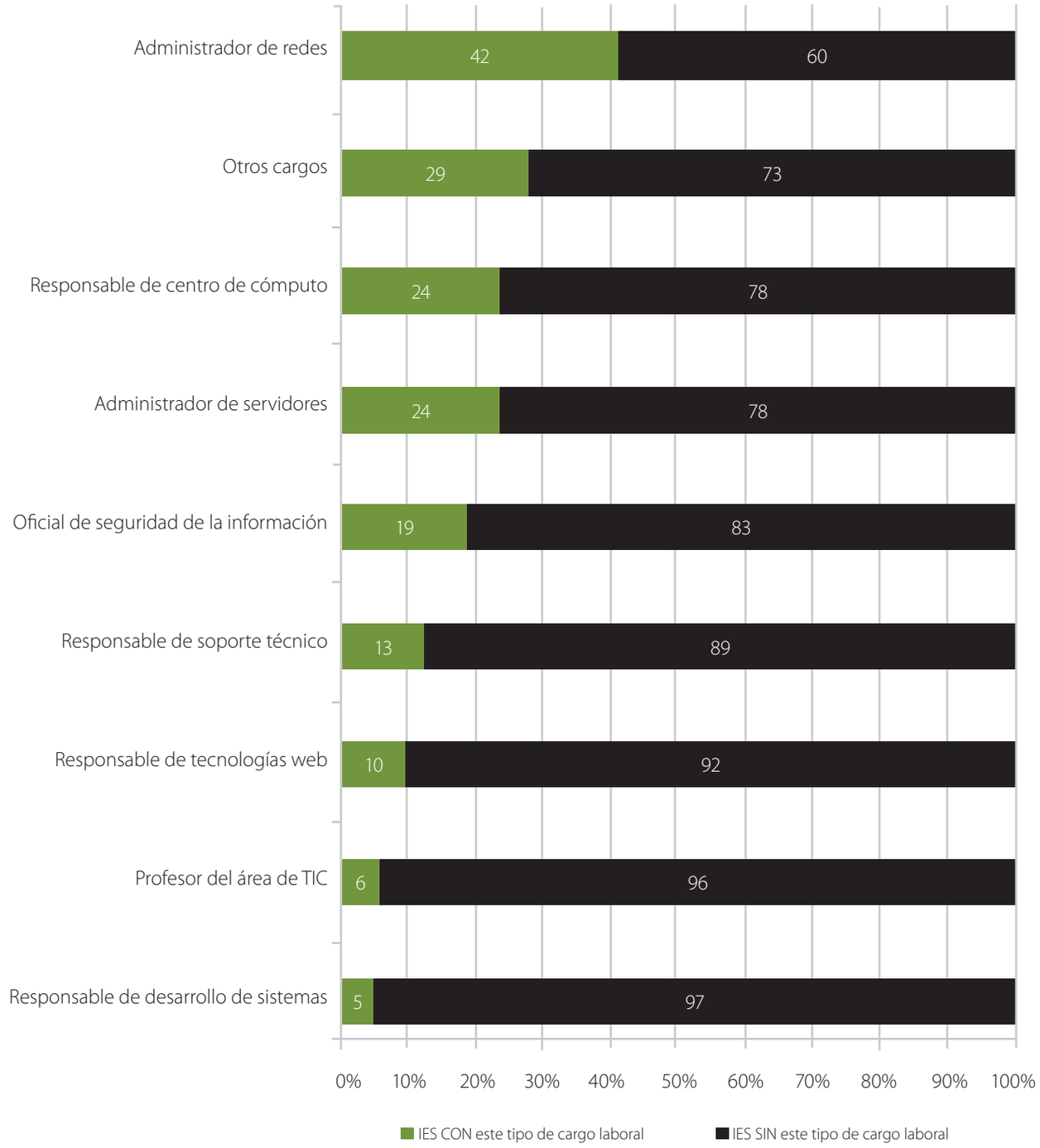


Por otra parte, es importante mencionar que de las 119 IES que respondieron la encuesta, sólo 19 cuentan con el cargo de Oficial (responsable) de Seguridad de la Información (gráfica 15). Asimismo, en el caso de otros tipos de cargo de los responsables de seguridad de TI en algunas IES, predomina que la implementación de la seguridad está a cargo de todas las áreas o sub-áreas de TI. Es importante hacer mención que en diversas IES el responsable de seguridad puede ocupar más de un tipo de cargo o función al mismo tiempo, por lo cual dicho responsable, en esos casos, no está dedicado exclusivamente a la seguridad de TI en su institución (gráfica 16).

De las IES que sí cuentan con responsable de seguridad en TI, el 73% se dedica a una sola función técnica; y en contraparte, el otro 27% de los responsables llega a tener desde 2 hasta 5 funciones técnicas, académicas o administrativas dentro de su IES (gráfica 17).

Adicionalmente, de las 102 IES que cuentan con personal de seguridad en TI, sólo el 18.6% (19 responsables) cuenta con el nombramiento de "Oficial de Seguridad de la Información". De los cuales, sólo 12 IES dedica a un responsable de forma exclusiva a dicho cargo o nombramiento (tabla 1).

Gráfica 16 Tipo de cargo de los responsables de seguridad en las IES



Gráfica 17 Porcentaje de responsables de seguridad en TI dedicados a una o varias funciones hacia el interior de las IES

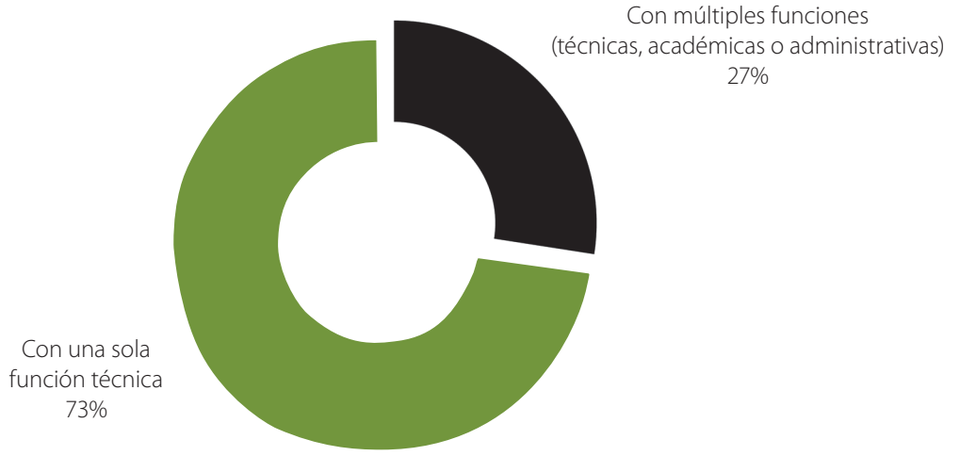


Tabla 1 IES con responsables de seguridad con nombramiento de "Oficial de Seguridad de la Información"

Funciones	Total de responsables de seguridad	Subtotal con nombramiento oficial	% subtotal de responsables con nombramiento oficial
Con múltiples funciones (técnicas, académicas o administrativas)	28	7	6.9%
Con una sola función técnica	74	12	11.8%
Total	102	19	18.6%

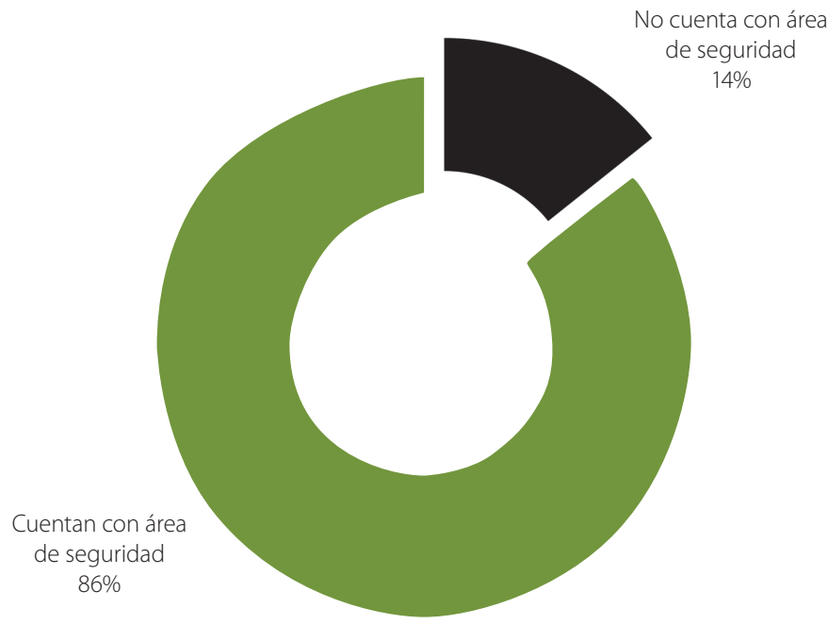
Ubicación del área de seguridad en TI de las IES

En lo que se refiere a la conformación de áreas de seguridad en TI en las IES, de las 119 que respondieron a la encuesta en línea, 102 de ellas respondieron que cuentan con un área dedicada (gráfica 18).

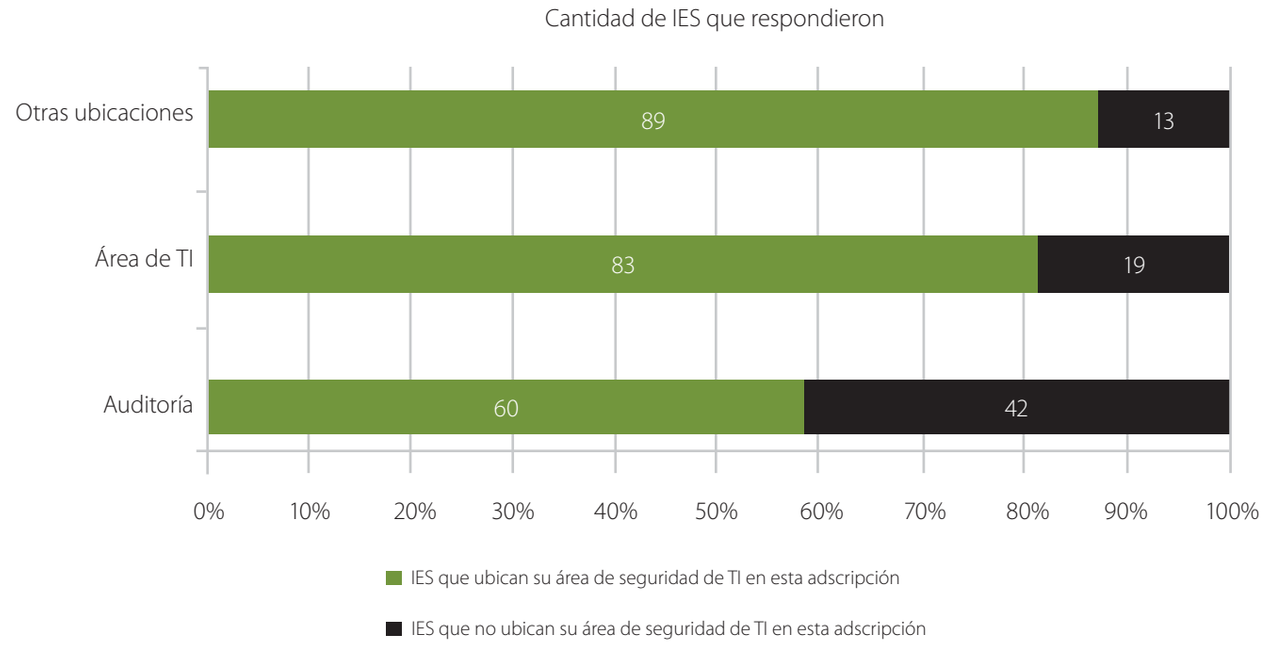
La ubicación de estas áreas en la estructura organizacional es muy variable. Es notable que en muchos casos no dependan de las áreas de TI o Auditoría, como ocurre en otras organizaciones.

Es importante hacer mención que en muchos casos, algunas áreas de seguridad en las IES, no dependen exclusivamente de una sola área de adscripción dentro de la organización, por lo cual existe redundancia de ubicaciones para esta función en las IES. Por otra parte, en el caso de otras ubicaciones del área de seguridad, en éstas predominan las adscripciones de TI que dependen directamente de áreas administrativas, rectorías o direcciones generales de las IES (gráfica 19).

Gráfica 18 Porcentaje de IES que cuentan con área de seguridad en TI



Gráfica 19 Ubicación del Área de Seguridad de TI en las IES

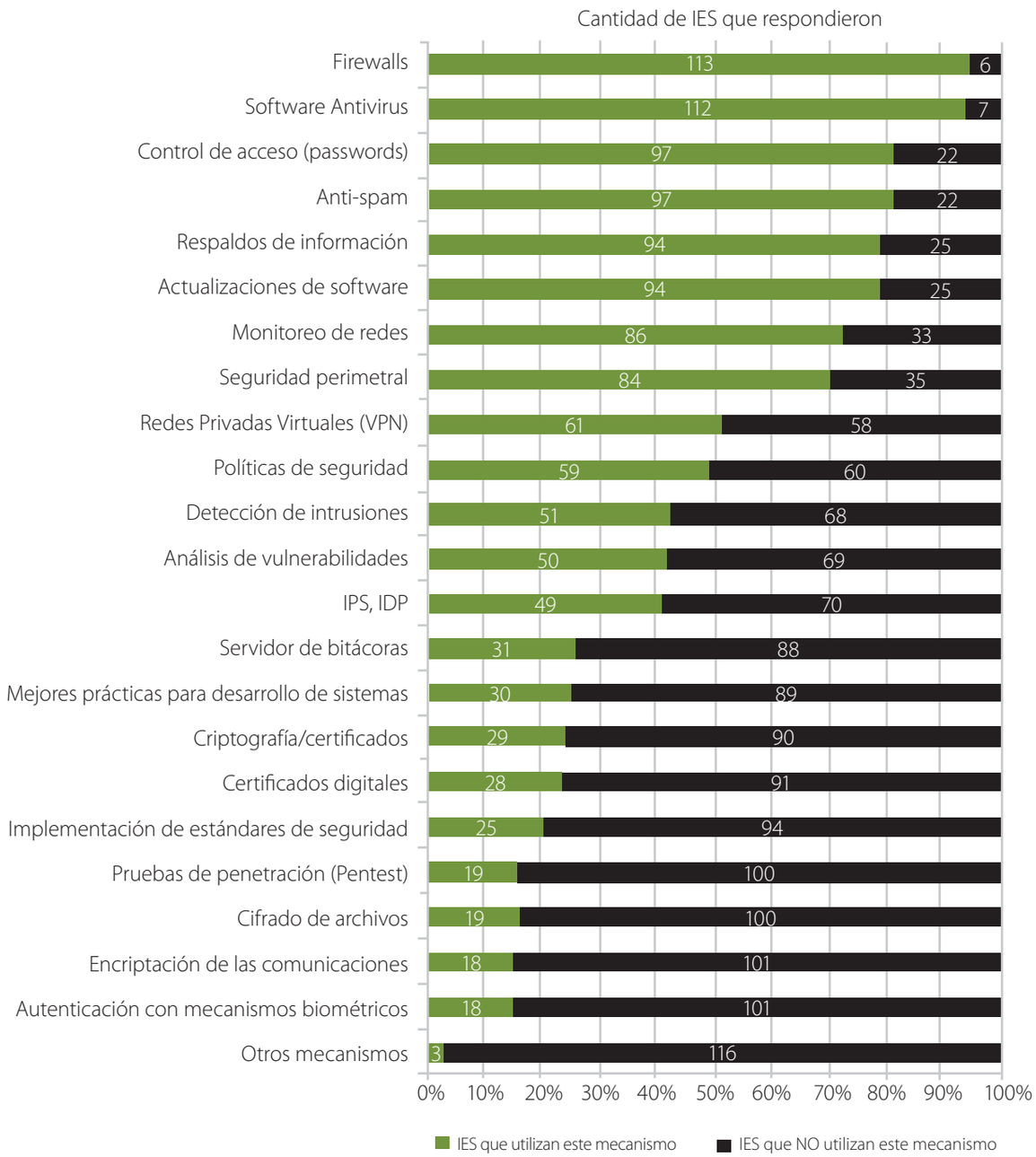


ESQUEMAS DE SEGURIDAD

Mecanismos utilizados para la protección de sistemas de información en las IES

Los mecanismos de seguridad que las IES aplican para la protección de sus sistemas de información apuntan primordialmente a la seguridad de las redes con mecanismos como firewalls, monitoreo, redes privadas virtuales, entre otros. También el software antimalware, anti-spam, así como la actualización de programas y el respaldo de la información están entre las principales soluciones que se utilizan. Es importante indicar que las IES aplican de forma paralela una gran variedad de mecanismos de seguridad en TI, acorde a la redundancia de opciones de la gráfica 20.

Gráfica 20 Mecanismos utilizados para proteger sus sistemas e información en las IES



Planes de seguridad empleados para la protección de infraestructuras de TIC en las IES

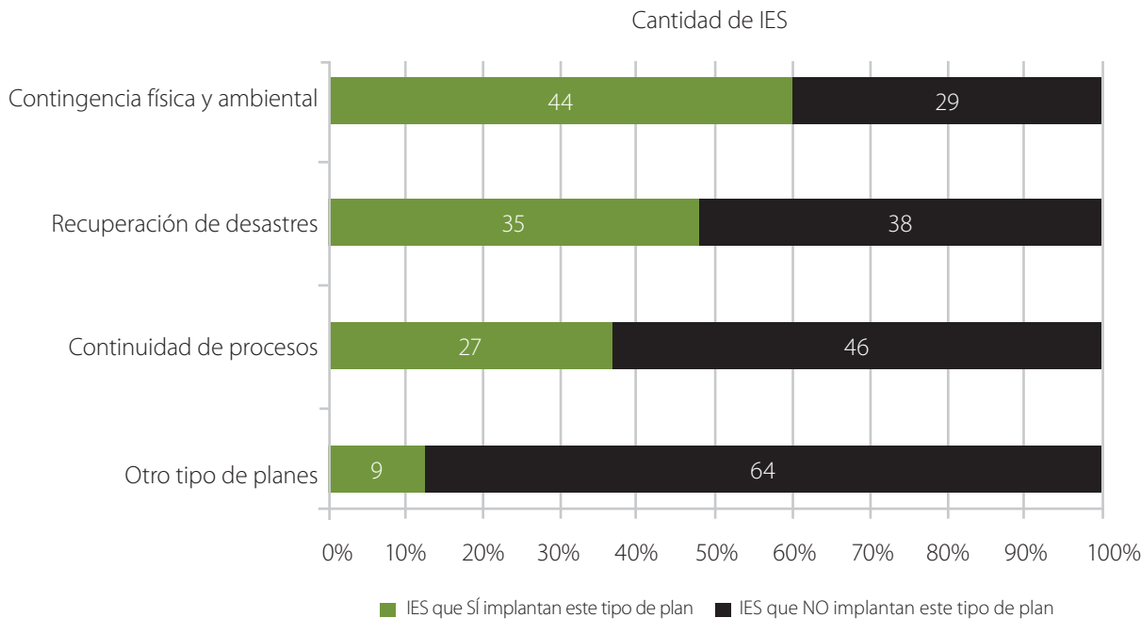
En cuanto al establecimiento de planes de seguridad en TI de las IES, de las 119 instituciones participantes en la encuesta, el 61% no cuenta con ellos y el 39% ha establecido algún plan de seguridad (gráfica 21).

Por otra parte, del 39% de las IES (gráfica 22) que sí cuentan con planes de seguridad en TI, estos están orientados a:

1. Contingencia física.
2. Recuperación de desastres.
3. Continuidad de procesos.
4. Otros.

Gráfica 21 Porcentaje de IES que cuentan con planes de seguridad en TI

Gráfica 22 Tipo de planes de seguridad que aplican las IES

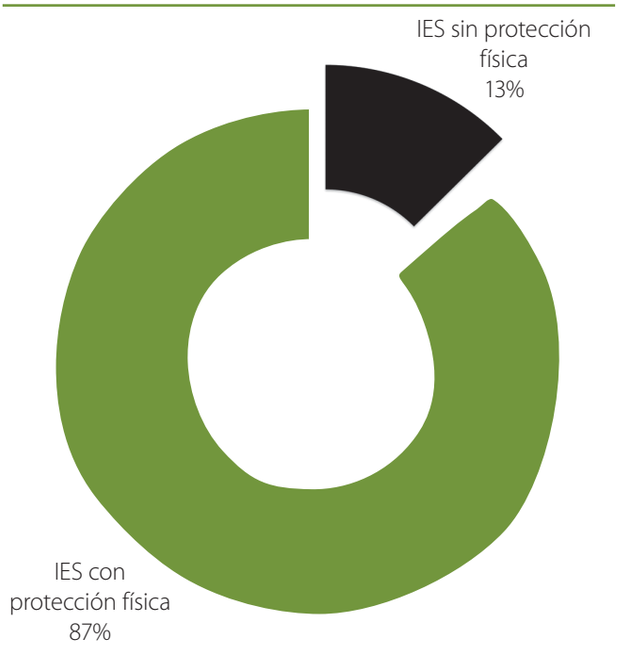


Es de considerar que la información de la gráfica anterior muestra los temas que predominan en los planes de seguridad en TI de las IES, considerando que dichos temas no son exclusivos, por lo que pueden estar implícitos múltiples temas de forma paralela en un solo plan institucional.

Mecanismos de seguridad física empleados por las IES

Entre las IES participantes, el 87% de las mismas cuenta con mecanismos de protección física y sólo 13% no los ha considerado (gráfica 23).

Gráfica 23 IES que aplican mecanismos de protección física



Por otra parte, los temas que destacan en orden de prioridad en cuanto a las IES que aplican mecanismos de seguridad física se muestran en la gráfica 24.

La gráfica anterior destaca la frecuencia de tipos de mecanismos de protección física que predominan en las IES, no obstante, una vez más cabe aclarar que las instituciones aplican de forma múltiple más de un mecanismo.

ESTÁNDARES Y BUENAS PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN

Tipo de certificación, capacitación o seguimiento de buenas prácticas de seguridad en TI de las IES

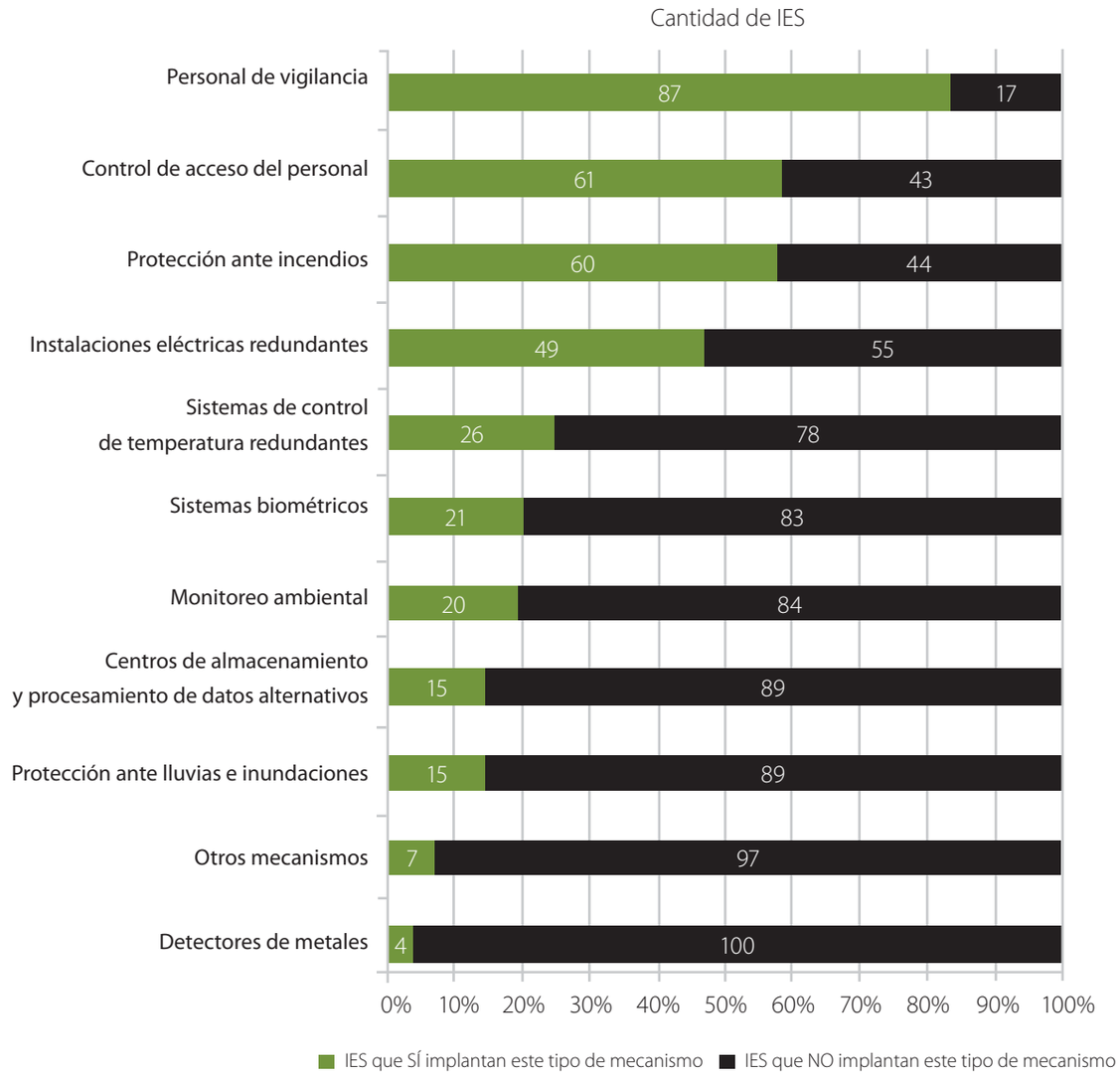
Los estándares y buenas prácticas de seguridad en TI han tenido gran difusión con respecto de su implementación en las IES, teniendo una respuesta del 47% de las 119 instituciones participantes, las cuales cuentan con certificaciones en estándares de TI o estándares de seguridad en TI (gráfica 25).

No todas las instituciones que respondieron positivamente cuentan con certificaciones sobre estándares internacionales de seguridad, pero cuentan con la "aplicación de mejores prácticas" basadas en estándares y marcos de referencia internacionales.

De las IES que aplican buenas prácticas, o que están certificadas en los estándares de TI, cabe mencionar que destaca la implantación de estándares internacionales como ISO9000/9001, ITIL (*Information Technology – Security Techniques – Information Security Management Systems – Requirements*), CoBit (*Control Objectives for Information and Related Techologies*), CISSP (*Certified Information Systems Security Profesional*), CISA (*Certified Information Systems Auditor*), CISM (*Certified Information Systems Management*), CEN (*Certified Ethical Harker*) CompTIA *Security* y otras (gráfica 26).

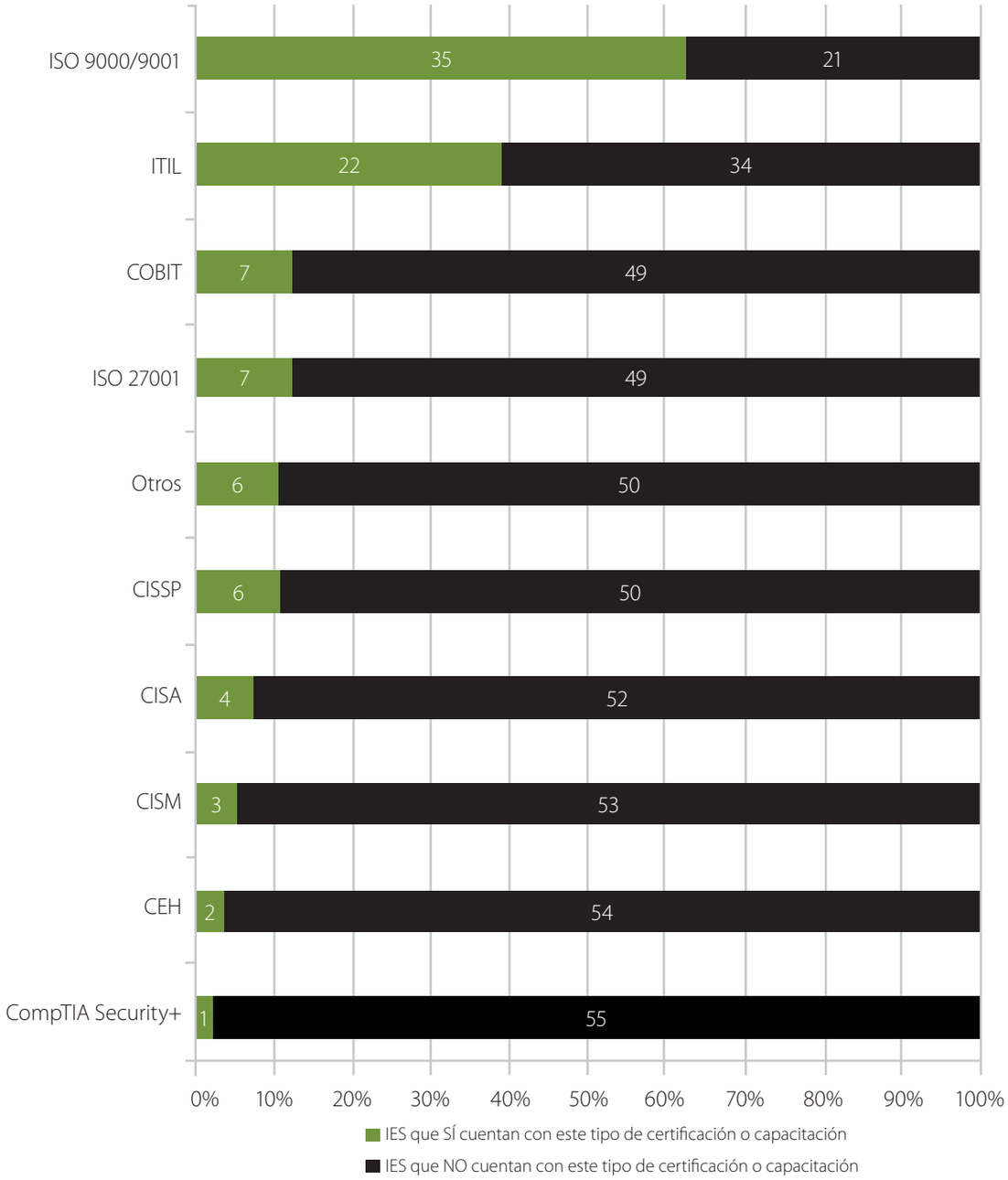
La gráfica muestra la frecuencia de estándares de seguridad de la información más aplicados, siendo múltiples las opciones que las IES pudieron seleccionar.

Gráfica 24 Tipos de mecanismos de protección física empleados en las IES



Gráfica 25 Porcentaje de IES que cuentan con alguna certificación o capacitación sobre buenas prácticas en seguridad de la información

Gráfica 26 Tipo de certificación/capacitación sobre seguridad de la información en las IES

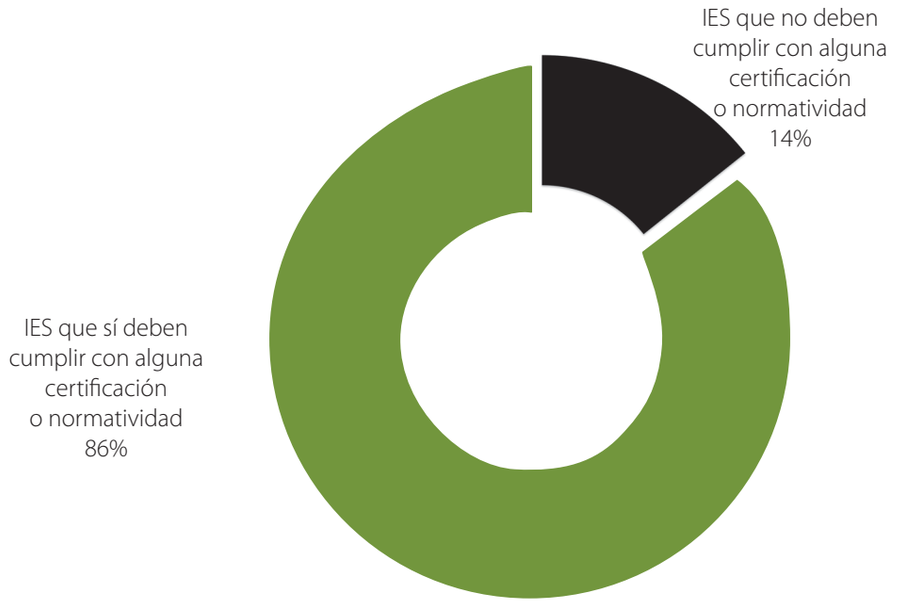


Disposiciones de cumplimiento interno en cuanto a certificación, normatividad o legislación en las IES

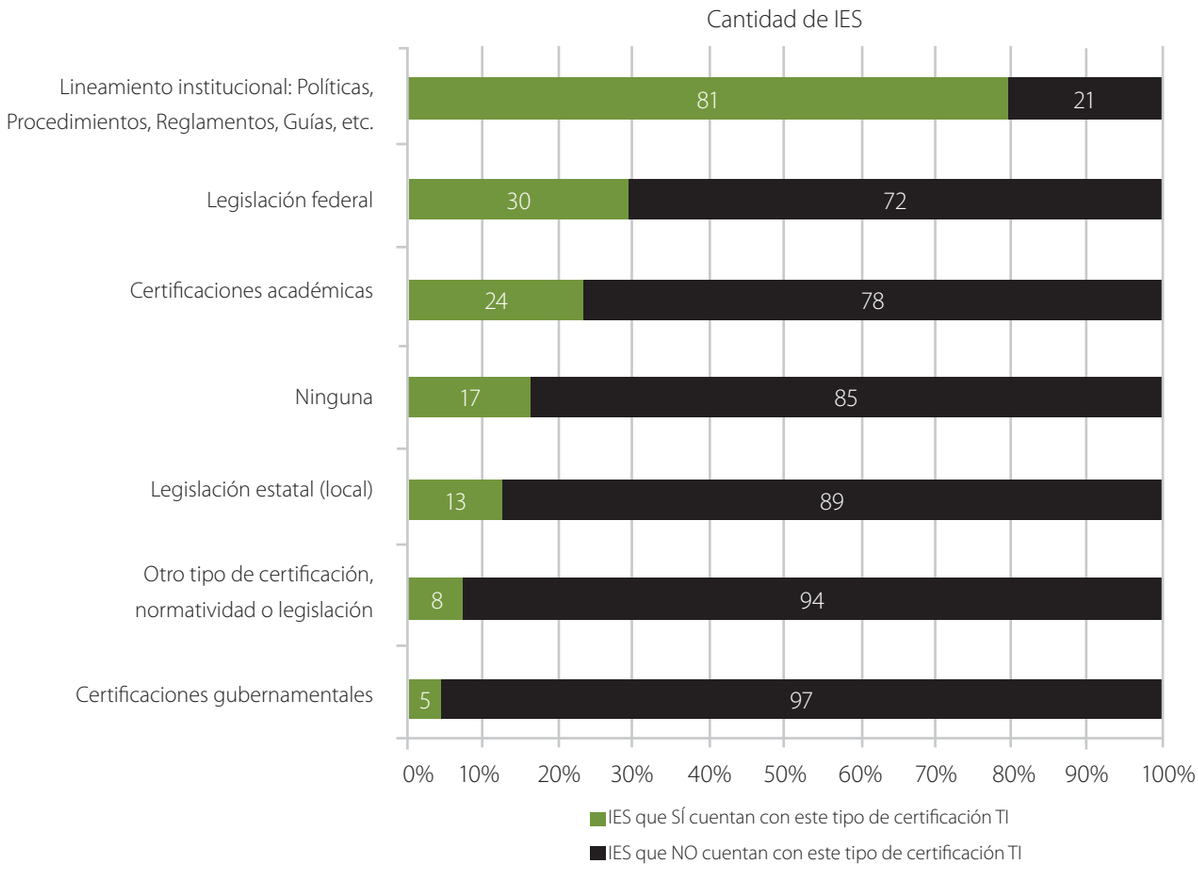
Una gran mayoría de IES (85 %) debe apegarse a normas específicas en la operación de TI, que incluyen políticas, reglamentos, certificaciones, leyes, etcétera (gráfica 27).

Por otra parte, el tipo de certificación, normatividad o legislación para las IES que sí cuentan con una disposición interna, se muestran en la gráfica 28. De igual manera, la gráfica muestra la frecuencia por tipo de certificación, normatividad o legislación que se debe cumplir, siendo múltiples las opciones que las IES pudieron seleccionar.

Gráfica 27 Porcentaje de IES que deben cumplir con alguna certificación o normatividad interna de seguridad de la información



Gráfica 28 Tipo de certificación, normatividad interna o legislación en TI que las IES deben cumplir



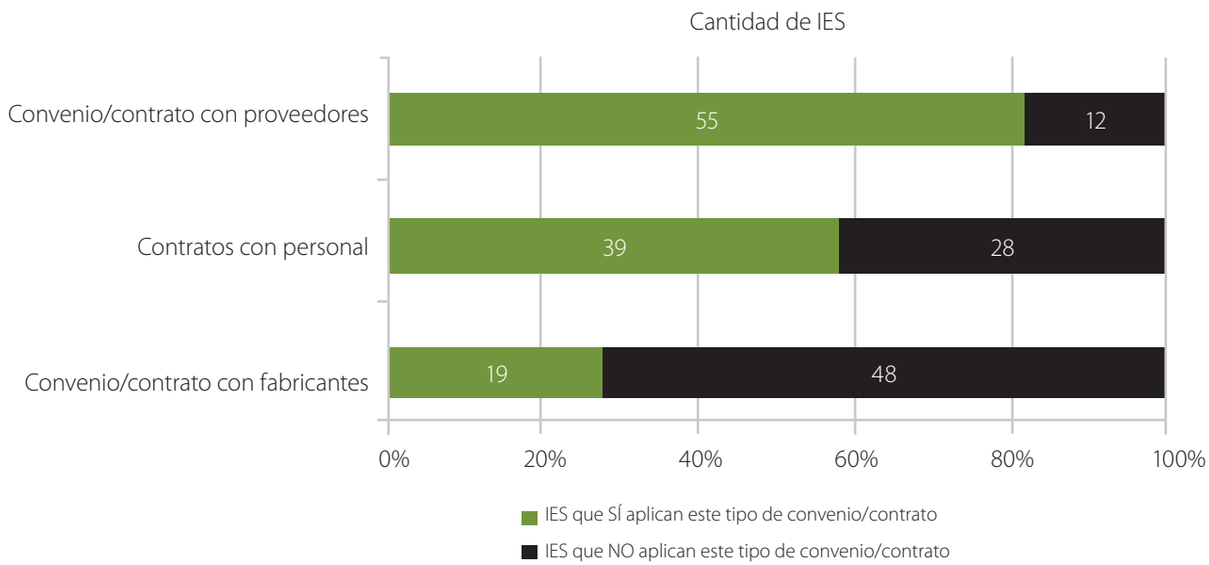
Aplicación de cláusulas de confidencialidad en los documentos legales de las IES

En la encuesta de seguridad en TI de las IES 2011; de las 119 instituciones participantes, el 56% cuenta con este tipo de disposiciones. Sin embargo, casi la mitad de las mismas (44%) lo omiten (gráfica 29).

Y en relación con las IES que cuentan con cláusulas en sus convenios y contratos, éstos aparecen aplicados en el orden de prioridad de la gráfica 30. Se considera que la gráfica muestra la frecuencia de cláusulas más utilizadas en convenios y contratos, siendo múltiples las opciones que las IES pudieron seleccionar.

Gráfica 29 Porcentaje de IES que aplican cláusulas de seguridad en sus convenios o contratos

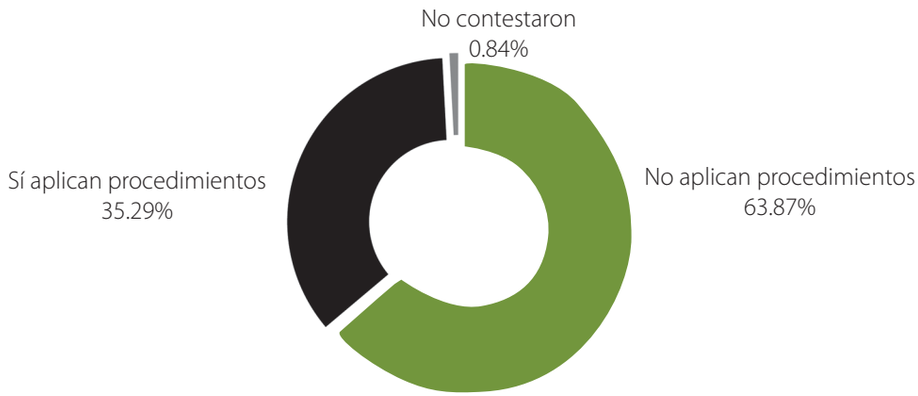
Gráfica 30 Tipo de convenios o contratos que aplican las IES con cláusulas de seguridad



Cumplimiento en cuanto a procedimientos de control de cambios en los sistemas de información, e infraestructuras tecnológicas de las IES

El cumplimiento de procedimientos de control de cambios es sólo un aspecto importante de un sistema de gestión de la seguridad de la información (SGSI) en las IES; sólo el 35.29% de las IES participantes en la encuesta aplican este tipo de procedimientos, mientras que el 63.87% no aplica algún procedimiento que permita el control de cambios en sus sistemas de información (gráfica 31).

Gráfica 31 Porcentaje de aplicación de procedimientos de control de cambios a los sistemas de información y a la infraestructura de TI en las IES



MANEJO DE INCIDENTES

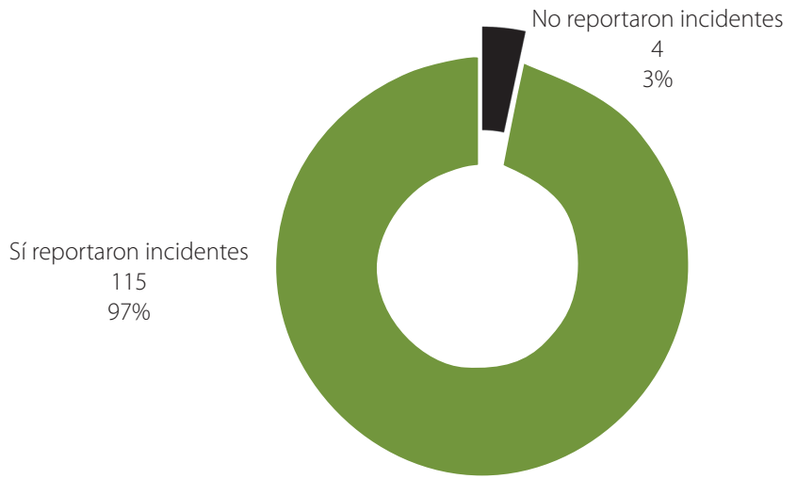
Incidentes de seguridad en TI reportados por las IES en los últimos 12 meses

Para la encuesta de seguridad en TI de las IES 2011, el 97% de las instituciones participantes respondieron que sí reportan sus incidentes hacia el interior y ante organizaciones de apoyo como los centros o equipos de atención a incidentes (gráfica 32).

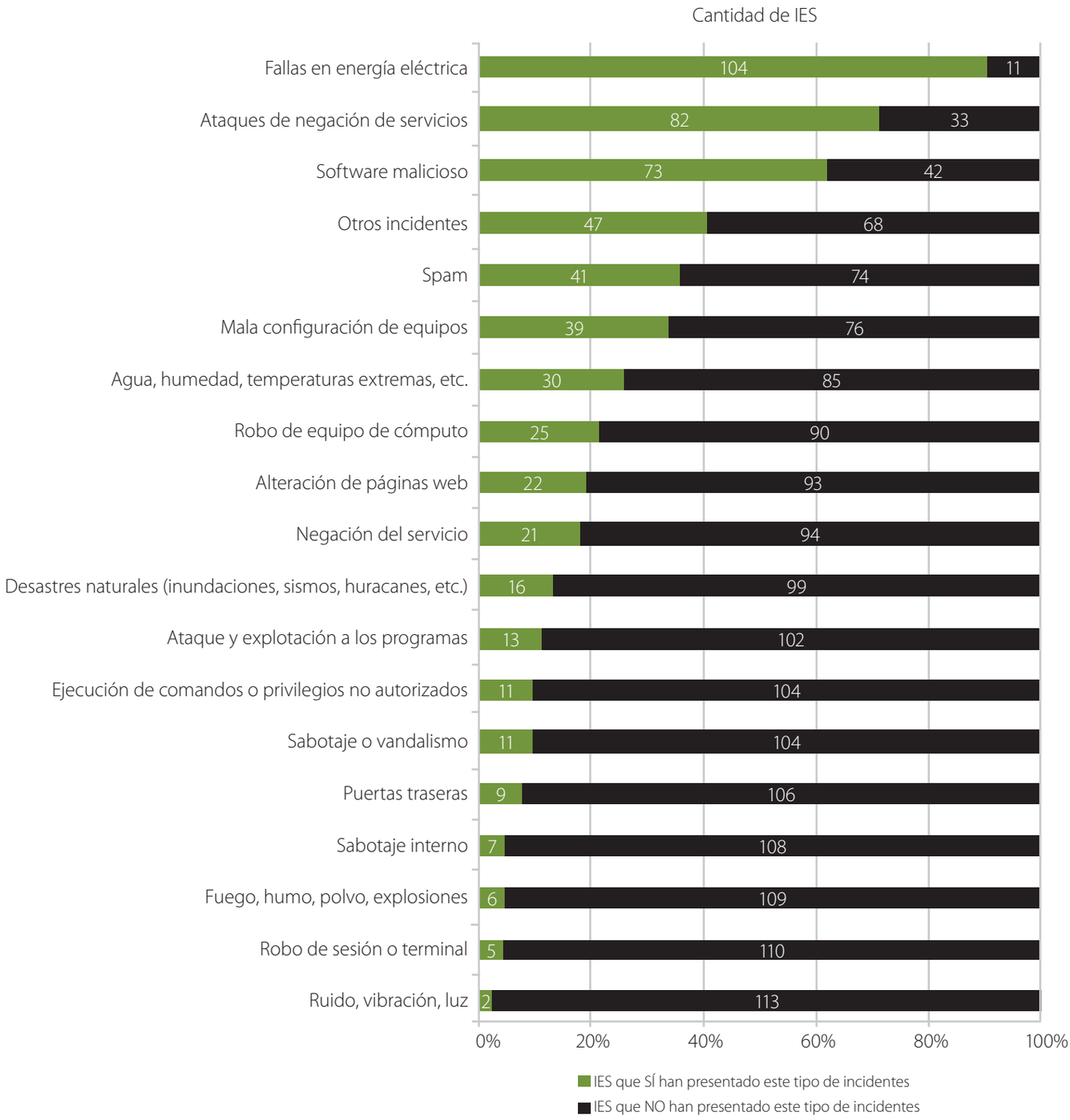
Por lo que respecta a las IES que sí reportan sus incidentes de seguridad en TI, la gráfica 33 nos muestra los diez incidentes más frecuentes en orden de prioridad durante los últimos 12 meses.

Además, otro tipo de incidentes de seguridad en las IES incluye el robo de cableado, tanto de red como eléctrico, así como las fallas de hardware, la inyección de código malicioso, los ataques de fuerza bruta, las vulnerabilidades en sistemas *open source* y la difamación y amenazas a personal de la IES mediante las redes sociales.

Gráfica 32 Porcentaje de IES que reportaron incidentes de seguridad en los últimos 12 meses



Gráfica 33 Tipo de incidentes de seguridad en TI que se han presentado en los últimos 12 meses

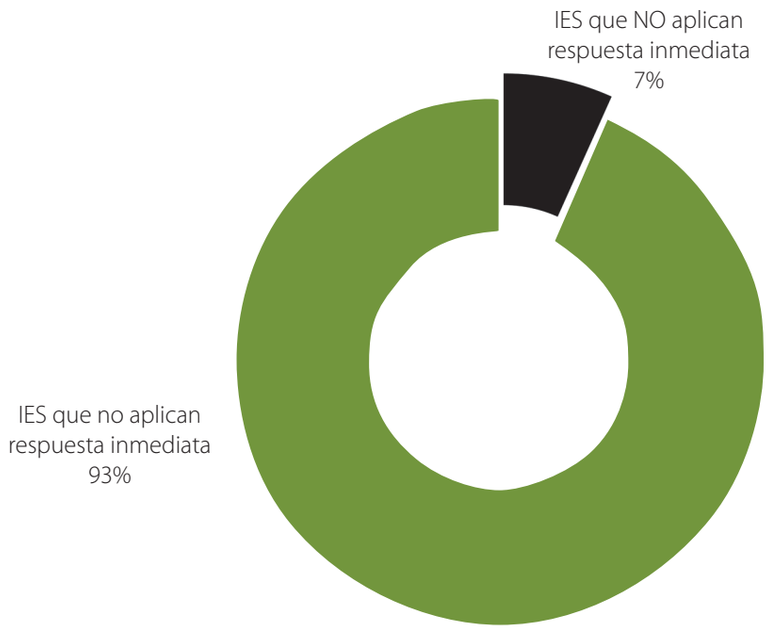


Respuesta inmediata ante incidentes de seguridad en TI de las IES

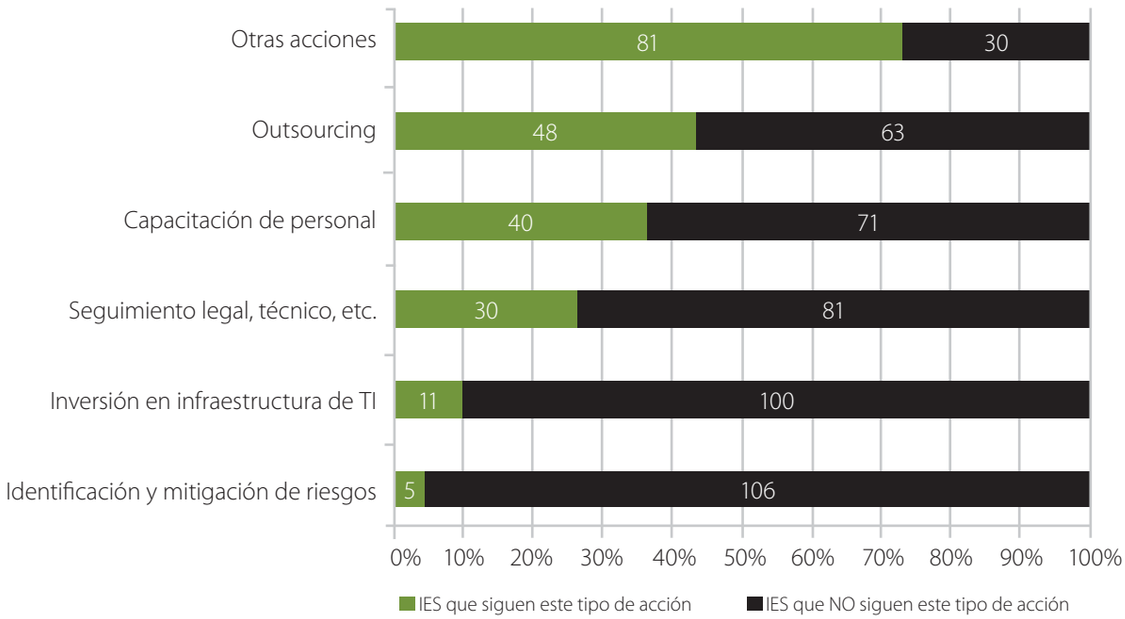
La respuesta inmediata a los incidentes de seguridad es un factor fundamental para la oportuna atención y control de las problemáticas consecuentes en las organizaciones.

De las IES participantes 119 en la encuesta, el 93% responde inmediatamente a sus incidentes (gráfica 34), se tienen distintos tipos de respuesta en orden de frecuencia que aparecen en la gráfica 35, siendo múltiples las opciones que las IES pudieron seleccionar.

Gráfica 34 Porcentaje de IES que generan respuesta inmediata ante incidentes de seguridad



Gráfica 35 Tipo de acciones de respuesta inmediata ante incidentes de seguridad



Acciones de seguimiento continuo a incidentes de las IES

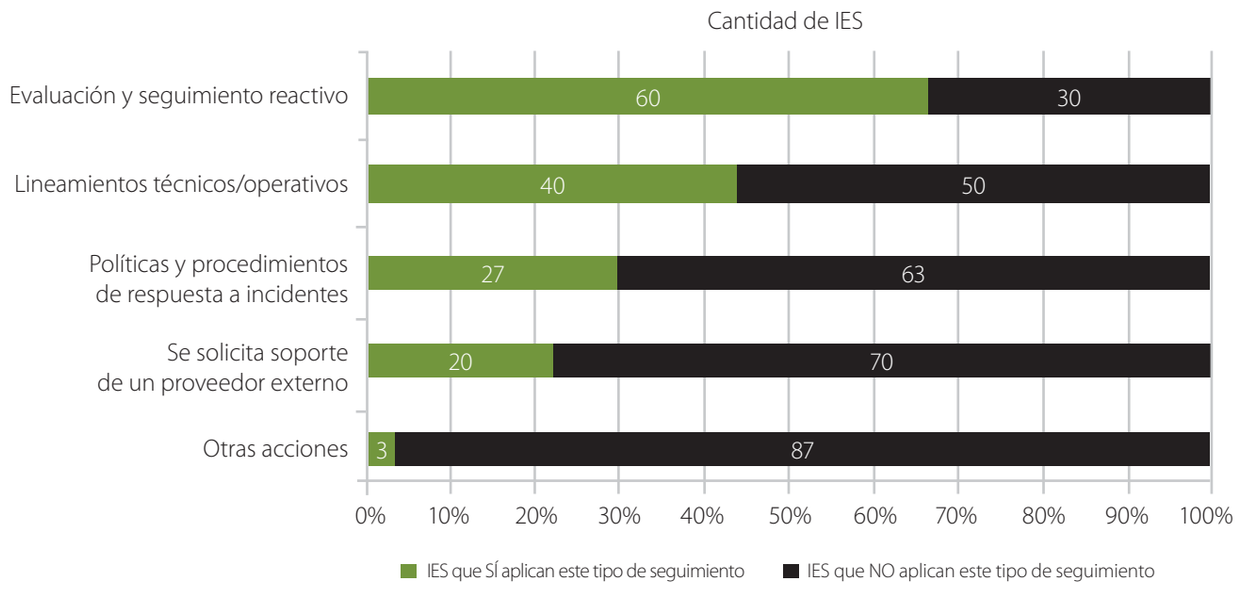
Después que se presenta algún incidente de seguridad y se responde oportunamente, se generan acciones de continuidad para solucionar y mitigar, en la medida de lo posible, los riesgos que generan determinadas problemáticas.

La encuesta dio como resultado que el 76% de las IES participantes (119), además de dar respuesta inmediata a sus incidentes de seguridad en TI, también da continuidad al seguimiento posterior de los mismos, para detectar las causas que los originan y dar resolución completa, para evitar que se repitan nuevamente (gráfica 36).

Se destacan en la gráfica 37 las acciones de seguimiento continuo hacia los incidentes de las IES, en donde se aplican distintas medidas de acuerdo al tipo de incidente que se presente. También es de considerar que fueron múltiples las opciones que las IES pudieron seleccionar, por lo que se destacan los tipos de acciones de seguimiento continuo que predominan en las IES ante incidentes de seguridad en TI.

Gráfica 36 Porcentaje de IES que dan continuidad a mayor plazo a los incidentes de seguridad, una vez que ya han sido atendidos de forma inmediata

Gráfica 37 Tipo de incidentes de seguimiento a mayor plazo de tiempo, una vez que ya han sido atendidos de forma inmediata



Otras acciones de seguimiento continuo que sólo se mencionan en la gráfica anterior, implican la aplicación de políticas y procedimientos acordes al Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones (MAAGTIC), para IES públicas, así como la aplicación de prácticas no formales.

PREVENCIÓN

Medidas de prevención en seguridad de TI aplicadas por las IES

La idea de generar una cultura de la seguridad en TI de las IES se orienta hacia la prevención de cualquier tipo de incidentes, lo cual constituye niveles de concientización y formación entre los responsables de administrar las TI y los usuarios de las mismas.

Con la intención de contar con un mejor control en los impactos que los riesgos pueden representar para las organizaciones, se pueden aplicar distintos mecanismos que permitirán la protección ante los incidentes de seguridad en TI, o al menos, se procurará contrarrestar los impactos de los mismos en caso de que éstos ocurran.

En relación con lo anterior, la encuesta de seguridad en TI de las IES 2011 muestra que de las instituciones participantes, el 73% aplican ciertas medidas preventivas con el objetivo de disminuir la inseguridad tecnológica (gráfica 38).

La gráfica 39 muestra la frecuencia de las medidas preventivas que aplican las IES para prevenir las incidencias de seguridad. Las opciones que las IES pudieron seleccionar fueron de tipo múltiple.

Entre otras medidas de seguridad en TI preventivas, destacan el despliegue de consejos de seguridad en las pantallas en los relojes de registro de asistencia de los empleados administrativos y académicos, los oficios informativos, y los eventos hacia el interior de la IES sobre seguridad informática.

Incidentes más frecuentes que se han presentado en los últimos 6 meses en las IES

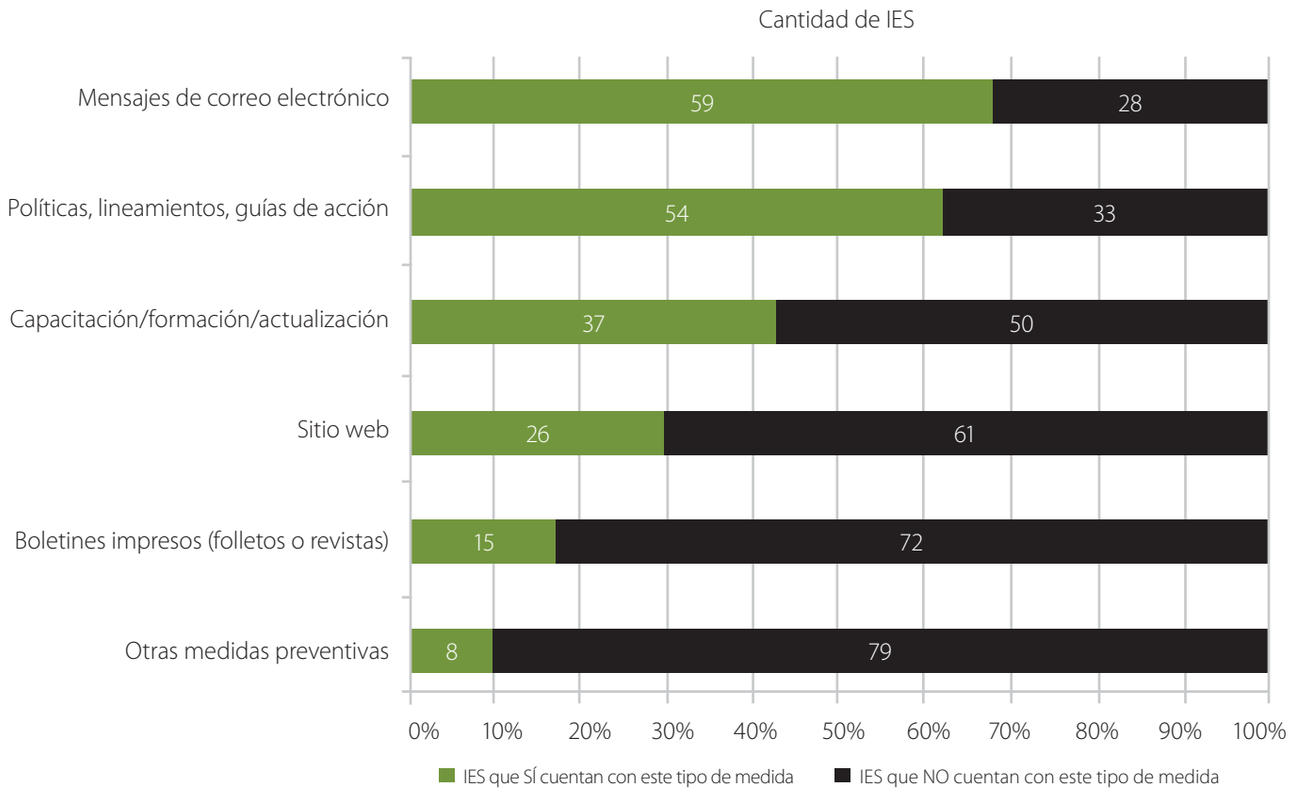
Como se comentó anteriormente, los usuarios finales de las tecnologías de información en las IES son un factor crítico en cuanto al uso adecuado de los recursos informáticos, y en el uso de la información.

Esto representa la conjunción de esfuerzos entre administradores de TI y usuarios finales para atraer resultados positivos en el uso óptimo de las tecnologías, y el aseguramiento de la información y sus infraestructuras físicas y lógicas.

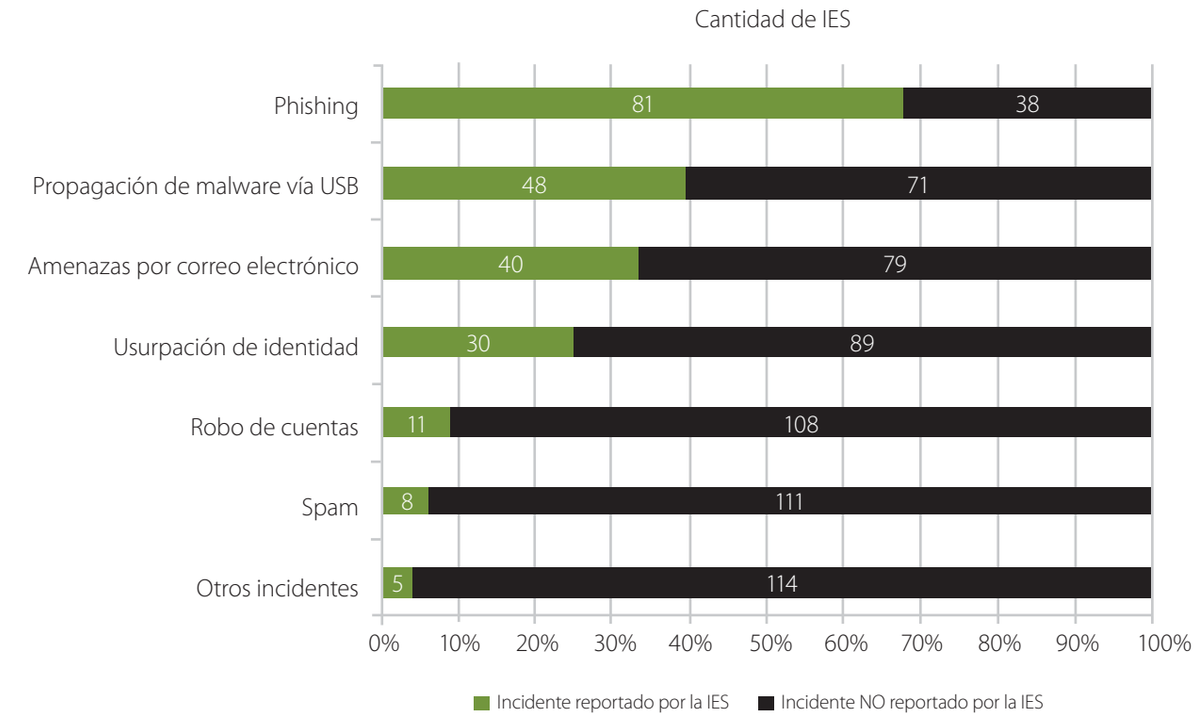
En este sentido, la encuesta de seguridad en TI de las IES 2011 consideró los incidentes más frecuentes que habían sido reportados por los usuarios finales en los últimos meses (gráfica 40). La gráfica indica la frecuencia de los variados incidentes que las IES reportaron, siendo múltiples las opciones que las IES pudieron responder.

Gráfica 38 Porcentaje de IES que aplican medidas preventivas hacia la cultura de seguridad en TI

Gráfica 39 Tipo de medidas preventivas de seguridad en TI aplicadas por las IES



Gráfica 40 Tipo de incidentes más frecuentes reportados por los usuarios finales en los últimos seis meses



CONCLUSIONES

- El nivel de participación de las IES fue muy satisfactorio, (74% de las IES que conformaban a la ANUIES en el periodo de aplicación). Sin embargo, el reto futuro deberá implicar a una mayor cantidad de IES interesadas en participar en el proyecto de diagnóstico.
- La infraestructura tecnológica ha evolucionado en las IES, no obstante, la seguridad sigue siendo un gran reto que implica aspectos que van desde el robustecimiento de equipamientos, y las telecomunicaciones, hasta la formación de especialistas para la operación segura.
- Por otra parte, a pesar de que las instituciones han mejorado en sus enlaces de telecomunicaciones, éstas requieren todavía de una mayor capacidad de transmisión de datos ante una inminente evolución sobre el tipo de aplicaciones, las cuales tienden a ser cada vez más robustas y demandantes.
- En cuanto a la banda ancha en México, es importante hacer notar que para las IES son insuficientes los niveles de servicio, no obstante, desde la perspectiva académica la tendencia de las IES que más se le acerca debe ser la incorporación y madurez del proyecto "Internet 2", que coordina la Corporación Universitaria para el Desarrollo de Internet (CUDI). El reto en este ámbito es muy importante, puesto que al momento no se ha considerado lo suficiente el tema de la seguridad en TI para el Internet 2 desde la perspectiva de las IES en la RENASEC.
- En relación con los equipos a nivel de usuarios finales, la encuesta denota una tendencia muy fuerte hacia un gran alcance de equipos conectados a Internet, lo cual podría implicar posibles aumentos en vulnerabilidades, amenazas y riesgos. El incremento de los dispositivos móviles debe ser atendido adecuadamente para evitar consecuencias negativas.
- Es notable la creciente utilización de servicios que son hospedados en equipos servidores propios, lo cual, anteriormente era de uso exclusivo de IES con recursos amplios.
- La importancia de la seguridad en sistemas operativos es fundamental para la adecuada operación de equipos de telecomunicaciones, servidores de cómputo, equipos de escritorio, portátiles, móviles, etc.
- El capital humano es un factor determinante para la seguridad en todos los niveles de usuarios, tanto usuarios de las aplicaciones básicas, hasta los especialistas que operan las infraestructuras tecnológicas de las IES. La concientización en todos los niveles de usuarios de tecnologías de información es esencial para conformar una cultura de la seguridad en las IES. Por tal razón, una de las mayores prioridades para la prevención y protección de los activos de información y de las propias personas, es el fortalecimiento del capital humano en las IES, en donde la concientización, la capacitación, la formación y la actualización constante de estudiantes, profesores, investigadores, personal administrativo y funcionarios, todos en general, deben ser un punto de atención prioritaria para el aseguramiento institucional.
- Un responsable de seguridad en TI en una IES, no necesariamente está dedicado a la seguridad de tiempo completo, lo cual contrarresta sus alcances y rendimiento, asumiendo que además de que su enfoque sobre la seguridad puede ser parcial, el poder de toma de decisiones en la institución también puede ser muy limitado.
- Cabe destacar que la ubicación de las áreas de seguridad en TI de las IES, cuando éstas existen, es muy variable en su gran mayoría, teniendo también como adscripciones a las áreas de TI y Auditoría en gran medida.

Es importante hacer mención que en muchos casos algunas áreas de seguridad no dependen de una sola área de adscripción dentro de la organización.

- La definición y aplicación de forma adecuada de esquemas de seguridad en las IES es crucial para contrarrestar los riegos que éstos conllevan.
- La gran variedad de mecanismos que aplican las IES para su protección es diversa, no obstante, existen alternativas de seguridad que todavía no son muy utilizadas y que deben representar soluciones apropiadas para ciertas amenazas; tal es el ejemplo de las tecnologías de cifrado (criptografía) y sus aplicaciones derivadas.
- Uno de los retos de la seguridad física es la convergencia con la seguridad lógica. Esto se refiere a la convergencia de la seguridad física y la seguridad lógica.
- Pese a que gran cantidad de IES están conscientes de la importancia de los estándares y buenas prácticas de seguridad de la información, habrá que hacer extensiva su promoción en todas las IES desde la perspectiva de las llamadas buenas prácticas. Es importante hacer mención que no necesariamente todas las instituciones que respondieron positivamente cuentan con certificaciones sobre estándares internacionales de seguridad; pero de manera fundamental sí cuentan con la "aplicación de buenas prácticas" basadas en éstos; lo que promueve una eficiente cultura en el uso de las tecnologías de información en las IES.
- En cuanto a los aspectos de seguridad de la información, muchas IES aplican cláusulas en su documentación oficial que se relaciona con convenios y contratos que protegen la confidencialidad de la información; sin embargo, en algunas instituciones no se considera ese cuidado esencial para su propia seguridad; lo que puede provocar problemas relacionados a la fuga de información u omisiones en el tratamiento de información personal o institucional que a futuro puede generar problemas difíciles de resolver.
- Pese a que la mayoría de las IES afirma que da atención de sus incidentes de seguridad en TI (97%), es muy importante concientizar y actualizar constantemente a sus responsables de seguridad y administradores de TI en la aplicación de procedimientos y documentación para su óptimo seguimiento. La respuesta inmediata a los incidentes de seguridad es fundamental para la oportuna atención y control de las problemáticas consecuentes en las organizaciones.
- Un buen porcentaje de IES (73 %) aplican medidas preventivas para contrarrestar las amenazas de seguridad en TI, sin embargo, éstas se orientan en gran medida hacia personal técnico; lo cual hace mandatorio considerar acciones preventivas para usuarios finales de las tecnologías de información.

RECOMENDACIONES

53

- Mantener de forma anual el diagnóstico nacional que permita para generar estrategias colaborativas de seguridad en TI, más efectivas en su ejecución, entre las IES afiliadas a la ANUIES.
- Establecer los esquemas de administración para equipos de cómputo y dispositivos móviles que consideren la generación y aplicación de políticas de uso y mecanismos de seguridad que mitiguen los posibles riesgos que presentan. Los dispositivos móviles que van desde celulares hasta tabletas electrónicas, suelen ser personales y por tanto, responsabilidad del usuario final (estudiantes, profesores, investigadores, empleados administrativos, visitantes); no obstante, pueden llegar a afectar el desempeño de las redes institucionales si no se toman las medidas adecuadas para su control. En resumen, cada vez son más los equipos fijos y móviles conectados a la red internet, por lo que la adecuada administración de estos genera retos de consolidación de la seguridad en ámbitos técnicos y de la normatividad de uso en las IES.
- Las buenas prácticas en el uso de sistemas operativos ayudarán a mitigar problemáticas que están bajo el alcance de los administradores de TI, y la forma de solucionarlo es la actualización de los sistemas, y el buen uso de éstos mediante políticas y formación de capital humano especializado.
- Es importante contar con recursos propios hacia el interior de las IES (Infraestructura de hardware y software), promoviendo la autodeterminación tecnológica a nivel institucional y evitando con esto ser clientes cautivos para los proveedores comerciales de tecnología.
- El personal encargado de las infraestructuras de servidores de cómputo y telecomunicaciones debe estar consciente del alto nivel de responsabilidad que implica la formación técnica en administración de sistemas, y la aplicación de las buenas prácticas de seguridad en las infraestructuras tecnológicas en las instituciones de educación superior. Ante esta circunstancia se recomienda que la administración de los servicios esté basada en las buenas prácticas, y con un alto nivel técnico de quienes se encargan de ésta labor, lo cual implica la creación de políticas, la capacitación especializada y aseguramiento integral desde la administración de las redes, servidores y procesos de desarrollo e implantación de sistemas de información; entre otros tópicos complementarios de la seguridad de la información.
- Se requiere capacitación especializada, formación con experiencia técnica, y la actualización constante del capital humano hacia el interior, y el personal formado por las propias IES.
- Es recomendable para las IES contar con un responsable con un "perfil de puesto dedicado" que permita tener una "visión integral de la seguridad de la información" que esté alineada a los objetivos estratégicos institucionales.
- Uno de los retos de la seguridad física es la convergencia con la seguridad lógica. Se debe trabajar en una cultura de la "seguridad convergente en las IES". Las instituciones de educación superior que aplican mecanismos de seguridad física, deben evolucionar a las tecnologías que convergen con la seguridad lógica, conjuntando tecnologías más avanzadas que permitan potencializar la seguridad de las personas y de sus infraestructuras de información y tecnológicas.
- Es importante alinearse con estándares de seguridad de todos los servicios tecnológicos que las IES demandan con la idea de impulsar las buenas prácticas de seguridad en TI de las IES. Debe privilegiarse el cumplimiento de estándares de seguridad de todos los servicios tecnológicos que las IES demandan, por tratarse de servicios tanto de uso diario como de misión crítica para el funcionamiento adecuado de las funciones,

tanto sustantivas como adjetivas. Por ejemplo, para el ámbito de desarrollo de sistemas seguros, se recomienda la aplicación del Proyecto OWASP (*Open Web Application Security Project*), el cual incorpora las buenas prácticas para el desarrollo de sistemas de información, entre otros mecanismos, tales como los estándares de seguridad de la información como ISO IEC 27000.

- Las buenas prácticas en el uso de sistemas operativos ayudarán a disminuir problemáticas que están bajo nuestro alcance, y la forma de solucionarlo es la actualización de los sistemas y su buen uso, mediante las políticas y la formación de capital humano especializado.
- El papel del responsable de seguridad en TI es fundamental en cualquier organización, en donde la capacitación y la actualización constantes deben ser una de las principales líneas de acción a seguir. Es importante contar con un responsable de seguridad en TI con "perfil de puesto dedicado" en cada IES, y con una "visión integral de la seguridad de la información. El perfil del responsable debe contar con suficiente nivel de toma de decisiones hacia el interior de la institución.
- Es fundamental para los responsables de seguridad de las IES contar con los conocimientos teóricos y prácticos de los estándares de seguridad en TI, además de la "generación de normatividad y documentación de buenas prácticas" orientadas hacia el buen uso de los recursos tecnológicos y de la información" para ser aplicados hacia el interior de las instituciones.
- Es muy importante para las IES contar con la documentación de sus procedimientos de control de cambios de sus sistemas de información e infraestructuras, facilitando la identificación, almacenamiento y protección de la información. Sin embargo, esto conllevaría a los responsables de seguridad de TI en las IES a tener los conocimientos teóricos y prácticos para conformar a futuro un SGSI de forma institucional que consolidará el proceso integral de la seguridad, y no sólo del control de cambios de sus procesos.
- Es importante establecer la formación en cuanto a seguimiento de incidentes de seguridad en TI en las IES, generando beneficios orientados a las buenas y mejores prácticas para la adecuada coordinación de respuesta a los mismos. El manejo de incidentes de seguridad en TI es un aspecto que debe ser documentado para su mejor seguimiento en las organizaciones.
- Es recomendable establecer la formación especializada de personal en cuanto a seguimiento de incidentes de seguridad en TI en las IES, generando beneficios orientados a las buenas y mejores prácticas para la adecuada coordinación de respuesta a los mismos. Es este sentido, las acciones de las IES pueden abarcar desde la concientización del manejo de incidentes entre sus responsables de TI, hasta la conformación de equipos de respuesta a incidentes que formarán el punto de contacto y seguimiento, así como la prevención ante las vulnerabilidades y sus respectivas recomendaciones hacia el interior de las IES.
- Es muy importante la conformación de programas de concientización orientados hacia la difusión de una "Cultura de la Seguridad en TI" que permita robustecer el eslabón más débil de la seguridad: "El usuario final". De acuerdo con los resultados reportados por las IES en la encuesta, se detecta que es evidente la necesidad de concientización de los usuarios mediante la difusión de información oportuna y en lenguaje directo, lo que permitirá entender los riesgos que puede implicar el uso indebido de las TI en la vida cotidiana de las personas, tanto de forma individual como institucional (laboral). Esto implica la recomendación hacia la concientización de los usuarios de TI, desde los niveles directivos y administrativos hasta los estudiantes y académicos en las IES.
- Es importante que la IES considere un presupuesto anual para la adquisición, actualización y mantenimiento de sus esquemas de seguridad que involucre estándares, políticas, personal y tecnología entre los elementos más importantes.

BIBLIOGRAFÍA

Contos Bryan T. *et. al.* (2010). *Physical and logical security convergence*, Syngress Publishing Inc.
Encuesta de Seguridad en TI de las Instituciones de Educación Superior 2011. [https://diagnostico.renasec.mx/]
Herbert Mattord, Michael Whitman (2004). *Management of information security*. Estados Unidos, Ed. Thompson.
McCarthy Linda (2003). *IT Security: Risking the Corporation*, Estados Unidos Prentice Hall.

Redes de Colaboración de ANUIES:

http://redes.anuies.mx/paginas.php?page=documentos

Documentos estratégicos:

Políticas de Seguridad Informática para Instituciones de Educación Superior. México: Red de Seguridad en Cómputo Sur-Sureste de ANUIES.
Plan de Contingencias para Instituciones de Educación Superior. México: Red de Seguridad en Cómputo Sur-Sureste de ANUIES.
Red Nacional de Seguridad en Cómputo ANUIES-UNAM [http://renasec.anuies.mx/]
Wil Allsopp (2009). *Unauthorized Access*, Ltd, Estados Unidos, John Wiley & Son.

Resultados de la encuesta
de seguridad de la información 2011
en las instituciones
de educación superior
se terminó de imprimir en enero de 2013 en
GRUPO H IMPRESORES
El tiraje fue de 500 ejemplares

Impreso en papel Bond
de 90 g y couché de 300g.

La composición tipográfica se
realizó con tipografía Myriad Pro