*Visión Antataura*
Vol.2, No.1: 1-15
Junio-Noviembre, 2018
Panamá
ISSN 2520-9892

# Nivel de seguridad de las redes de área local en algunas instituciones públicas que funcionan en la ciudad de Santiago, provincia de Veraguas.

## Security level of local area networks in some public institutions operating in the Head District of Santiago, province of Veraguas.

*Oscar E. Rodríguez C.[1], Raúl E. Dutari D.[2], Edwin J. Cedeño H.[3] y Norberto A. Delgado R.[4]*

[1]Magister en Sistemas Computacionales; Docente del Centro Regional Universitario de Veraguas, Universidad de Panamá; oseroca.rodriguez@up.ac.pa
[2]Magister Scientiae en Computación; Docente del Centro Regional Universitario de Veraguas, Universidad de Panamá; raul.dutari@up.ac.pa
[3]Dr. en Ingeniería en Sistemas Telemáticos; Docente del Centro Regional Universitario de Veraguas, Universidad de Panamá; edwin.cedenoh@up.ac.pa
[4]Licenciatura en Ingeniería en Informática; Facultad de Informática, Electrónica y Comunicación, Centro Regional Universitario de Veraguas, Universidad de Panamá; norberto.d07@gmail.com

**Resumen:** Con la finalidad de determinar el nivel de seguridad en las redes de área local en algunas instituciones públicas en Santiago de Veraguas, se aplicó a los administradores de las redes de 15 entidades gubernamentales, entre los meses de junio a julio de 2016, una encuesta que contiene 16 ítems, de los cuales el 37,5% fueron preguntas cerradas y el 62,5% abiertas. El 93,33% de las instituciones cumplieron con criterios técnicos como: el conjunto de funciones y procesos administrativos que se desarrollan sobre la red, la cantidad de colaboradores-usuarios y las tecnologías existentes; juicios que fueron propuestos y validados como referentes de los resultados. Como aspecto concluyente, se determinó que las instituciones objeto de estudio, cuentan con un deficiente nivel de seguridad en sus redes de área local establecido por el orden del 40,31%; asociado a su poca capacidad de protección y condición de funcionamiento de la red; lo que requiere de un mejor desempeño de la administración de la seguridad.

**Palabras clave:** Seguridad, niveles de seguridad, redes de área local.

**Abstract:** In order to determine the level of security in the local area networks in some public institutions in Santiago, Veraguas, a survey was applied to the network administrators of 15 government entities between the months of June and July 2016; this survey contains 16 items, of which 37,5% were closed questions and 62,5% were open questions. 93,33% of the institutions met technical criteria such as the set of functions and administrative processes, that were developed on the network, the number of collaborators-users, and the existing technologies; judgments that were proposed and validated as references of the results. As a conclusive aspect, it was determined that the institutions under study have a deficient level of Security in their Local Area Networks established by the order of 40,31%; associated with its low protection capacity and network operating condition which requires a better performance of the security administration.

**Key words:** Security, level of security, local area networks.

*Fecha de recepción: 10 de abril de 2018* *Fecha de aceptación: 15 de mayo de 2018*

## 1. Introducción

Las condiciones actuales de desarrollo en materia de redes de computadoras, en nuestro país están marcadas fuertemente por la evolución dinámica de las diversas tecnologías aplicadas al proceso de transmisión de datos, las que han avanzado de manera acelerada y arrolladora; convirtiéndonos en dependientes de casi todos los servicios y beneficios que ofrecen. Sin embargo, ligado a estas bondades, no es indiferente la presencia de los problemas de seguridad, ausencia de políticas y con ella la necesidad puntual de la protección y salvaguarda de los equipos, componentes y, sobre todo, de los datos e información que fluyen a través de éstas (Aguilera, 2010).

Un aspecto fundamental que presenta un claro referente investigativo y técnico como antecedente al estudio, es el propuesto por la empresa de Consultoría RISCCO y que, en conjunto con la Universidad Tecnológica de Panamá, señalan un sinnúmero de condiciones muy importantes en materia de seguridad de la información (RISCCO, 2010), (RISCCO, 2011), (RISCCO, 2012). Estos documentos recabaron información relevante y muy significativa en materia de seguridad, demostrando que la situación de los activos informáticos en las empresas en Panamá están en riesgo debido, entre otros aspectos, a la ausencia de políticas y a la poca implantación de estrategias de seguridad para reducir los riesgos, amenazas y las vulnerabilidades asociadas al caso (Gómez, 2014).

En Panamá, se nota con mucha frecuencia que las empresas, instituciones y entidades públicas y privadas en su contexto general son cada vez más dependientes de sus redes de área local y de los sistemas informáticos que utilizan; en consecuencia, por mínimo que sea el problema de seguridad que las afecte, puede llegar a comprometer parcial o totalmente la continuidad de las operaciones (Williams, 2013). Es aquí donde se evidencia la presencia de un problema que cada vez, toma más fuerza y del cual poco se habla al respecto.

El término Red de Área Local (Local Area Network-LAN, por sus siglas en inglés), incluye tanto los equipos y componentes informáticos físicos, reconocidos por el término técnico de Hardware como a los componentes lógicos determinados como el Software; ambos son necesarios para la interconexión de los distintos dispositivos y del tratamiento y

flujo de la información (Abad, 2012). Tanto es así, que desde los albores del presente siglo se ha destacado que las redes de área local son generalmente propiedad de una organización que utiliza la red para interconectar equipos (Stallings, 2004). Por su parte, la seguridad en las organizaciones es considerada como un factor primordial bajo el contexto del proceso de comunicación, pero el enfoque sobre la forma y los elementos a proteger, han cambiado radicalmente debido a los medios y componentes que se utilizan para resguardar los activos de dicha organización. (Koontz, Weihrich, y Cannice, 2012)

En cuanto a la protección de la información a nivel organizacional es concebida como el proceso de asegurar que los datos sean recuperables de manera confiable y consistente en un formato útil para los usuarios autorizados (Williams, 2013). Por lo que, el concepto de seguridad en redes de área local, surge como consecuencia de la necesidad de utilizar medios y procedimientos para reducir riesgos debido a las posibles amenazas sobre la red física, la información y el personal. (Alarcón, 2007)

La seguridad en las redes de área local está relacionada con la seguridad y control de contingencias para la protección adecuada de los sistemas de redes de computadoras; en cuanto a la salvaguarda de los datos y de la información que fluyen a través de las redes, la seguridad en el acceso a los sistemas computacionales, a la información y a los programas del sistema, así como la protección de accesos físicos, del mobiliario, del equipo, de los usuarios de los sistemas, incluyendo el respaldo de información y los privilegios de accesos a sistemas (Muñóz, 2002); y de las políticas de seguridad, las cuales proporcionan las reglas, normas y procedimientos que gobiernan la administración de las actividades y procesos a través de las redes de computadoras y de los sistemas informáticos, basados en la misión, visión, valores y en la filosofía institucional. (Maiwald, 2005)

El objetivo de la seguridad en las redes de área local es el de detectar las deficiencias y vacíos dejados por los responsables o encargados de diseñar, configurar, gestionar y administrar las redes de computadores; contrarrestar los posibles ataques, intrusiones y afectaciones virales, así como corregir las fallas que puedan presentarse en las comunicaciones (Alarcón, 2007).

Como propósito principal del estudio, se presenta determinar el nivel de seguridad de las Redes de Área Local en algunas instituciones públicas ubicadas en el distrito de Santiago, provincia de Veraguas a través de la cual se intenta explicar las condiciones reales detectadas en las que actualmente se encuentran las redes de computadoras y las políticas de seguridad en dichas instituciones. Esta situación representa una gran motivación profesional y una valiosa oportunidad para resaltar la importancia de la seguridad como factor prioritario dentro del entorno y funcionamiento de las redes de computadoras.

## 2. Materiales y Métodos

Se aplicó una encuesta a los administradores de las redes de computadoras de 15 instituciones gubernamentales ubicadas en el distrito de Santiago, provincia de Veraguas. Dicha encuesta contenía 16 ítems, de los cuales el 37,5% fueron preguntas cerradas y el 62,5% de preguntas abiertas. Dichos ítems estaban asociadas a tópicos técnicos investigativos como: cargo que desempeña en la institución, años de servicio, la existencia de documentos y políticas de seguridad en la institución, el acceso a dichos documentos, amenazas físicas y ambientales, protección contra fallas del fluido eléctrico, políticas sobre los servicios de red, mantenimiento de equipos, uso de software especializados, auditoría y evaluaciones a la red, controles internos, acceso a la información, administración de direcciones de red y el control de acceso de equipos y dispositivos móviles en la institución.

Se analizaron tres condiciones como aspectos esenciales que se deberían cumplir para ser consideradas como objeto de investigación; mismas que certifican el proceso de evaluación de los niveles de seguridad en las redes de área local en estas instituciones. Estos criterios fueron las funciones y procesos administrativos sobre la red, la cantidad de colaboradores-usuarios y las tecnologías existentes en la institución (Williams, 2013).

El 93,33% de las instituciones públicas investigadas cumplieron al 100% con los criterios técnicos establecidos para dicho estudio de investigación. El instrumento utilizado fue validado por el juicio de expertos en el área de redes de computadoras y seguridad informática que laboran en las siguientes instituciones de educación superior públicas y privadas en la provincia de Veraguas: Universidad de Panamá (Centro Regional Universitario

de Veraguas), Universidad Tecnológica (Centro Regional de Veraguas), Universidad Latina (Sede de Santiago) y Universidad Especializada de las Américas (Extensión de Santiago); los cuales analizaron, discutieron y propusieron ajustes al instrumento, lo que permitió una mejor estructura técnica de esta herramienta para la recopilación de la información.

Se conformó el tamaño de la muestra en $(n \cong 14)$ instituciones, basado en (Hernández, Fernández, y Baptista, 2010), mientras que la probabilidad $(\mathrm{P} = 0.9333)$ de ocurrencia de que los elementos seleccionados en la población total, presenten los atributos de interés en la encuesta, obtenida a través de un pre-muestreo (Levine, Krehbiel, y Berenson, 2014), (Servin y Abad, 1982).

Se estableció un patrón de referencia a cada una de las preguntas aplicadas dentro de la encuesta y se le asignó un valor o peso en escala valorativa entre (1 y 10), en donde (1) sería de menor valor y (10) el máximo; correlacionado con la dificultad para responder la pregunta dentro de la encuesta.

Un valor de (1) representa la pregunta cuya respuesta implica el mínimo nivel de estado de seguridad de la red de área local; en tanto, el valor de (10), señalará una pregunta que posee el máximo nivel de seguridad requerido en la red.

Se empleó una Distribución Normal de Probabilidades con el propósito de establecer la valoración de los resultados de las pruebas aplicadas (Stuffelebeam y Coryn, 2014); adicional se determinó a través de la evaluación de la sumatoria de los porcentajes, la valoración de cada criterio de seguridad, lo que dio como resultado el valor total de la unidad de análisis como aspecto prioritario de la investigación.

Se establecieron (7) niveles de seguridad, determinados a través de la relación general: $\text{Nivel de Seguridad [NS]} = \frac{\text{Escala Valorativa (100)}}{\text{Número de parámetros deseados (7)}}$., el cual dio como resultado el valor nominal de 14,285$\cong 14{,}29$; lo que representa la media de referencia para determinar los rangos de los Niveles de Seguridad buscados.

Para comparar el valor obtenido, se estableció una matriz de rangos al cual se le asignó la letra [V], luego a éstos, se le estableció un calificativo equivalente a su condición numérica determinada en una escala de cero hasta cien. Entonces:

$$\forall\, [V] \in R\,, \text{donde}\ \ 0 \ \leq\ [V] \leq 100$$

El valor [V] puede obtener una calificación de la siguiente manera:

- Si [V] es menor o igual a 14,29% se considerará como un parámetro de seguridad **Malo**.
- Si [V] es mayor que 14.29%, pero menor o igual que 28,58%, se calificará como un parámetro de seguridad **Deficiente**.
- Si [V] es mayor que 28,58%, pero menor o igual que 42,87%, tendrá un parámetro de seguridad **Mínimo**.
- Si [V] es mayor que 42,87%, pero menor o igual que 57,16%, se calificará como un parámetro de seguridad **Regular**.
- Si [V] es mayor que 57,16%, pero menor igual que 71,45% se calificará como un parámetro de seguridad **Aceptado**.
- Si [V] es mayor que 71,45%, pero menor igual que 85,74% se calificará como un parámetro de seguridad **Bueno**.
- Si [V] es mayor que 85,74%, entonces obtendrá un parámetro de seguridad **Óptimo**.

## 3. Resultados y Discusión

La Tabla 1, muestra los resultados de las ponderaciones obtenidas de las preguntas aplicadas en la encuesta.

**Tabla 1. Ponderaciones obtenidas según el grado de dificultad al responder las preguntas de la encuesta.**

| N° de Pregunta | Ponderación (de 1 a 10) |
|---|---|
| 1 | 5 |
| 2 | 6 |
| 3 | 10 |
| 4 | 7 |
| 5 | 10 |
| 6 | 10 |
| 7 | 10 |
| 8 | 9 |
| 9 | 8 |
| 10 | 8 |
| 11 | 9 |
| 12 | 7 |
| 13 | 10 |
| 14 | 8 |
| 15 | 7 |
| 16 | 6 |
| **Valor total de la encuesta** | **130** |

Fuente: Encuesta aplicada por los autores.

Las preguntas 3, 5, 6, 7 y 13, obtuvieron mayor grado de dificultad, denotando la relación del máximo nivel de seguridad requerido en la red, las que se vinculan a la existencia de documentos y políticas de seguridad en la institución, los procedimientos a seguir en caso de contingencias, protección de los equipos frente a amenazas físicas y ambientales, protección contra fallas eléctricas y la pérdida de información, y el acceso a la información, respectivamente.

Las trayectorias del valor de [V] presentadas en la Tabla 2, están basados en el concepto de distribución normal de una población, utilizando una escala de cero hasta cien. De esta forma, se obtienen siete intervalos o rangos que expresan cuál sería la distribución normal teórica del comportamiento de la población, su relación con los Niveles de Seguridad y la representación porcentual de los valores obtenidos.

**Tabla 2. Distribución normal de las ponderaciones y su relación con el nivel de seguridad**

| Valor de [V] | Unidades de desviación estándar | Niveles de Seguridad | Valores Porcentuales |
|---|---|---|---|
| V ≤ 14,29% | -3 $\sigma$ | Malo | Deficiente |
| 14,29% < V ≤ 28,58% | -2 $\sigma$ | Deficiente | |
| 28,58%< V ≤ 42,87% | -1 $\sigma$ | Mínimo | |
| 42,87% < V ≤ 57,16% | $\sigma$ sigma | Regular | |
| 57,16% < V ≤ 71,45% | 1 $\sigma$ | Aceptado | Adecuada |
| 71,45% < V ≤ 85,74% | 2 $\sigma$ | Bueno | |
| 85,74% < V | 3 $\sigma$ | Optimo | |

Fuente: Elaborada por los autores.

En la Tabla 3 se muestra la correlación entre los valores de la ponderación por cada pregunta y sus respectivos porcentajes, lo que permite señalar la condición vinculada a la seguridad categorizada según la Tabla 2 en Adecuada o Deficiente.

Para determinar este porcentaje se analizó el total de cada encuesta aplicada, cuántas coincidieron o señalaron la misma respuesta para así determinar su porcentaje, lo que facilitó realizar el cálculo de la condición [X] y ubicar el resultado porcentual obtenido, bajo la siguiente condición:

$\forall$ valor $[X] \in$ % de R , donde$[\mathrm{X}] \geq 57{,}0\%$, "ADECUADA"; de lo contrario "DEFICIENTE"

La Tabla 3 muestra estos resultados, luego se estableció la Σ de los valores (%SA) y (%SD) y se calculó el promedio de los porcentajes obtenidos, resultando así la referencia final del nivel de seguridad como punto esencial del estudio.

**Tabla 3. Correlación de las ponderaciones de las preguntas y promedios de los porcentajes calculados**

| N°de pregunta | Ponderación de las preguntas | Porcentaje de seguridad adecuada (%SA) | Porcentaje de seguridad deficiente (%SD) |
|---|---|---|---|
| 1 | 5 | 57 | 43 |
| 2 | 6 | 43 | 57 |
| 3 | 10 | 43 | 57 |
| 4 | 7 | 33 | 67 |
| 5 | 10 | 17 | 83 |
| 6 | 10 | 28 | 72 |
| 7 | 10 | 17 | 83 |
| 8 | 9 | 27 | 73 |
| 9 | 8 | 100 | 0 |
| 10 | 8 | 57 | 43 |
| 11 | 9 | 27 | 73 |
| 12 | 7 | 26 | 74 |
| 13 | 10 | 43 | 57 |
| 14 | 8 | 43 | 57 |
| 15 | 7 | 50 | 50 |

| | | | |
|---|---|---|---|
| 16 | 6 | 34 | 66 |
| **Valor total de la encuesta** | **130** | **40,31** | **59,69** |

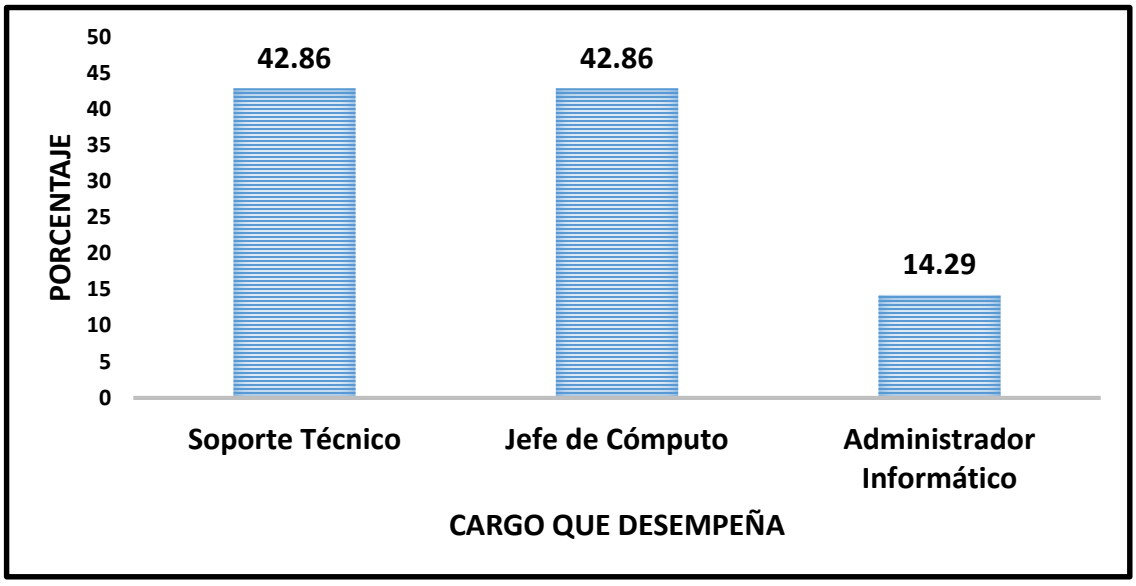
Fuente: Elaborada por los autores.

La tabla 3 también muestra el resumen porcentual de la condición de la seguridad en las entidades objeto de estudio, el cual presentó un 40,31%, lo que indica resultados no tan favorables en cuanto al nivel de seguridad de la red; estableciendo un parámetro de seguridad deficiente marcado por el orden del 59,69% en cuanto a la protección de las redes de área local y de los datos que fluyen a través de éstas.

Un aspecto muy importante en el análisis de los resultados es que claramente se reafirma que las preguntas 3, 5, 6, 7 y 13, presentaron bajos porcentajes de seguridad adecuada (%SA): 43, 17, 28, 17 y 43%, respectivamente, la cual se vincula al grado de dificultad al resolver la pregunta planteada. Sin embargo, la pregunta 1 del instrumento aplicado, recibió una ponderación media de (5) en la escala valorativa utilizada, la cual obtuvo una ponderación porcentual del 57%, destacándose como el mayor resultado positivo. En ese mismo orden de ideas, la pregunta 9 obtuvo una ponderación de (8); no obstante, alcanzó el mayor porcentaje en el análisis de seguridad al presentar un 100%. Esto se debe a que, a pesar de las dificultades y a la burocracia existente en estas instituciones, los funcionarios encargados de la administración y funcionamiento de las redes, desarrollan acciones básicas en materia de seguridad.

Un aspecto importante que se muestra en la figura 1, es la denominación a los cargos que desempeñan los funcionarios que laboran en las entidades públicas objeto de investigación, los cuales se presentan un poco ambiguos. Con un porcentaje similar, se ubican tanto el Soporte Técnico como el denominado Jefe de Cómputo (42,86%) y con un muy bajo porcentaje el Administrador Informático (14,29%).

**Figura 1. Cargo que desempeña el funcionario en la entidad investigada.**

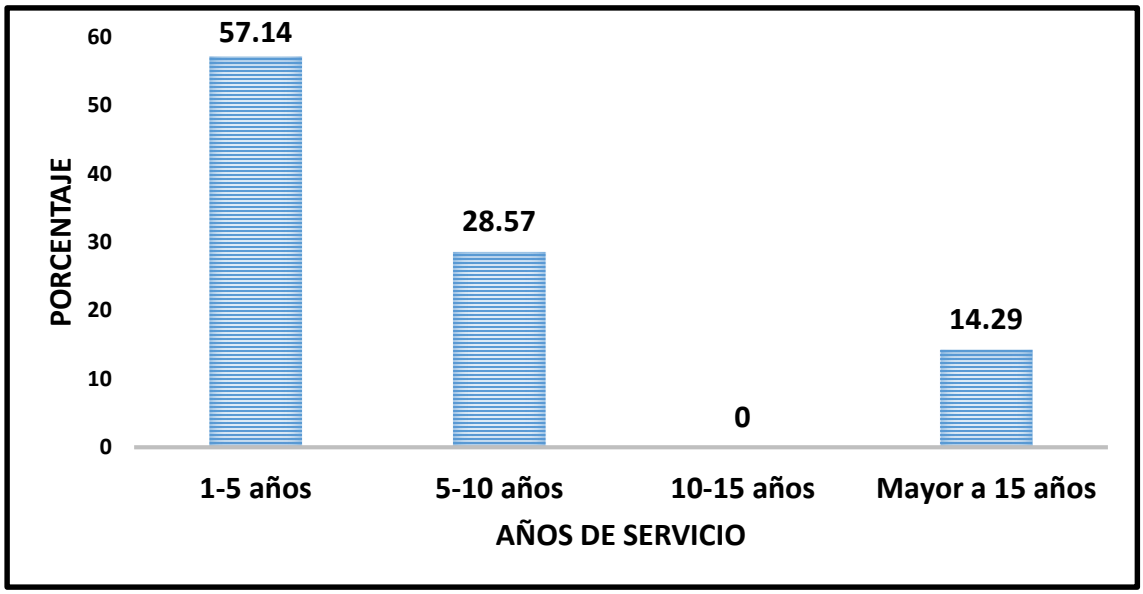



Fuente: Encuesta aplicada por los autores.

Los resultados muestran que los funcionarios que administran las redes de área local en las entidades investigadas desarrollan funciones generales en cuanto a la administración de redes de área local; un aspecto importante es que poseen conocimientos en el área de informática, lo que se vincula al desarrollo de actividades técnicas y no a funciones administrativas.

En la figura 2 se detallan los años de servicio de los funcionarios que administran las redes de área local en las instituciones objeto de estudio, destacando un rango mayoritario entre 1 a 5 años con porcentaje por el orden de los 57,14%; lo que indica que tienen poco tiempo en el entorno de trabajo de la institución. Esta situación presenta dos condiciones básicas: la primera se vincula a los funcionarios que ejercen funciones de administrador o de soporte técnico de las redes de área local, que por su condición laboral en la institución no han sido capacitados plenamente en sus funciones; y por otro lado, el desconocimiento de la existencia de documentos técnicos en materia de seguridad, que emanan de las direcciones superiores de la institución, dejan claro un punto importante y muy notable en lo que a políticas y administración de la seguridad de redes se refiere.

**Figura 2. Años de servicio de los funcionarios que administran las redes de área local en las entidades investigadas**.

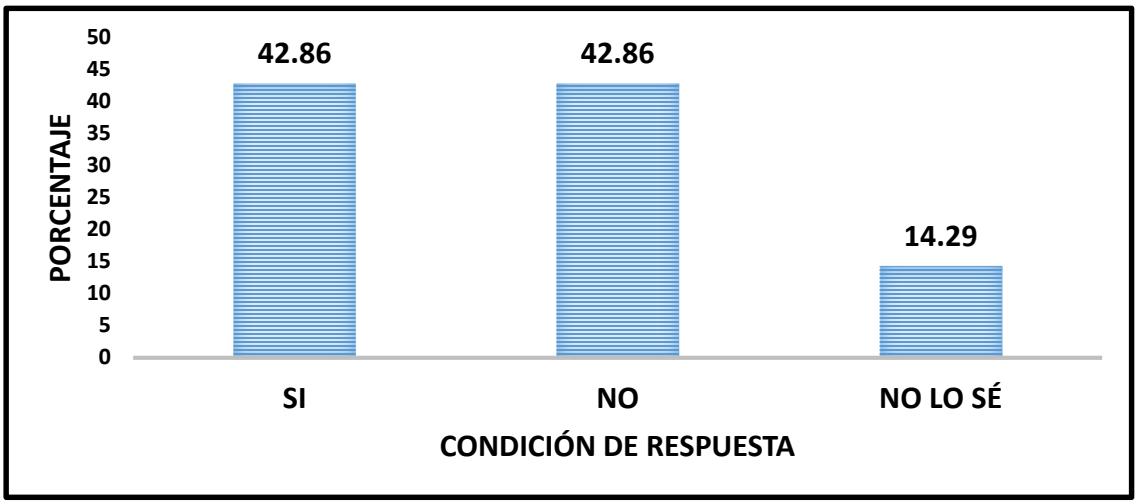



Fuente: Encuesta aplicada por los autores.

Esto es un factor que puede originar que se desconozcan todos los procedimientos administrativos requeridos para enfrentar algún tipo de inconvenientes dentro de la administración y seguridad de las redes de computadora y, por otro lado, el grado de dificultad al responder la pregunta radica principalmente a lo explicado previamente asociado a su condición administrativa actual, ya que en ese momento no estaba claro la permanencia en el cargo asignado.

Bajo la condición directa de la existencia de documentos que establezcan las políticas en materia de seguridad dentro de la organización, se destaca que el 42,86% cuenta con un instrumento que determina las consideraciones mínimas que permiten la administración y uso adecuado de las redes de área local, como se muestra en la figura 3; sin embargo, bajo ese mismo porcentaje se representa la inexistencia de dicho documento.

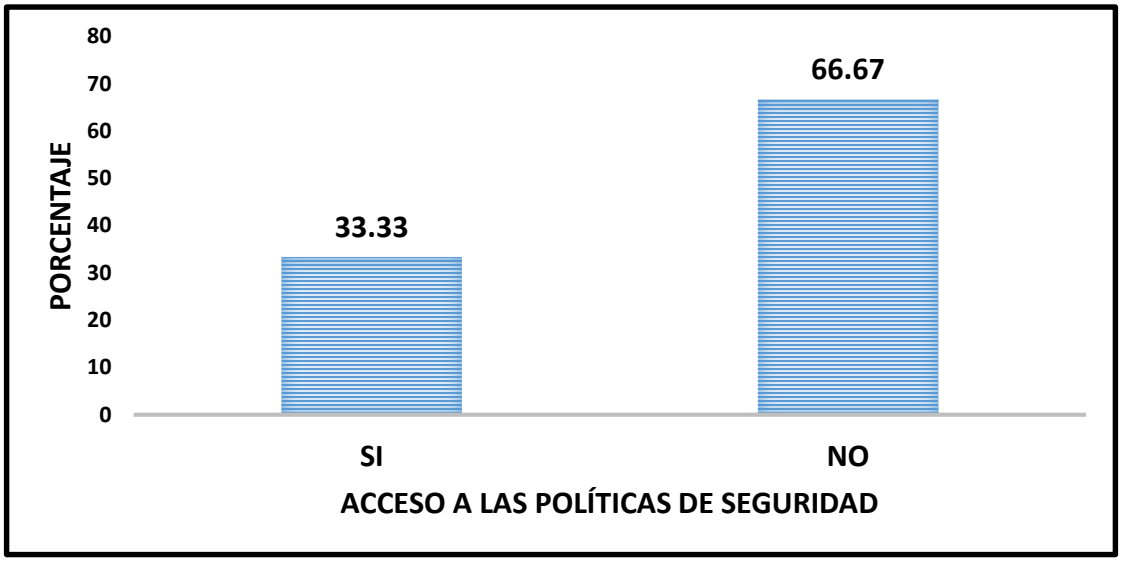
**Figura 3. Existencia de documentos que establezcan las políticas de seguridad en las redes de área local**.




Fuente: Encuesta aplicada por los autores.

Un elemento significativo que se recopiló al aplicar el instrumento fue la condición particular que el personal no conoce, ni tampoco tiene el acceso al documento sobre las políticas de seguridad de la organización. Este porcentaje está por el orden de los 66,67%; lo que denota un factor fundamental que se debe tener en cuenta en el proceso de la administración sobre la seguridad de las redes de computadoras, como se muestra en la figura 4.

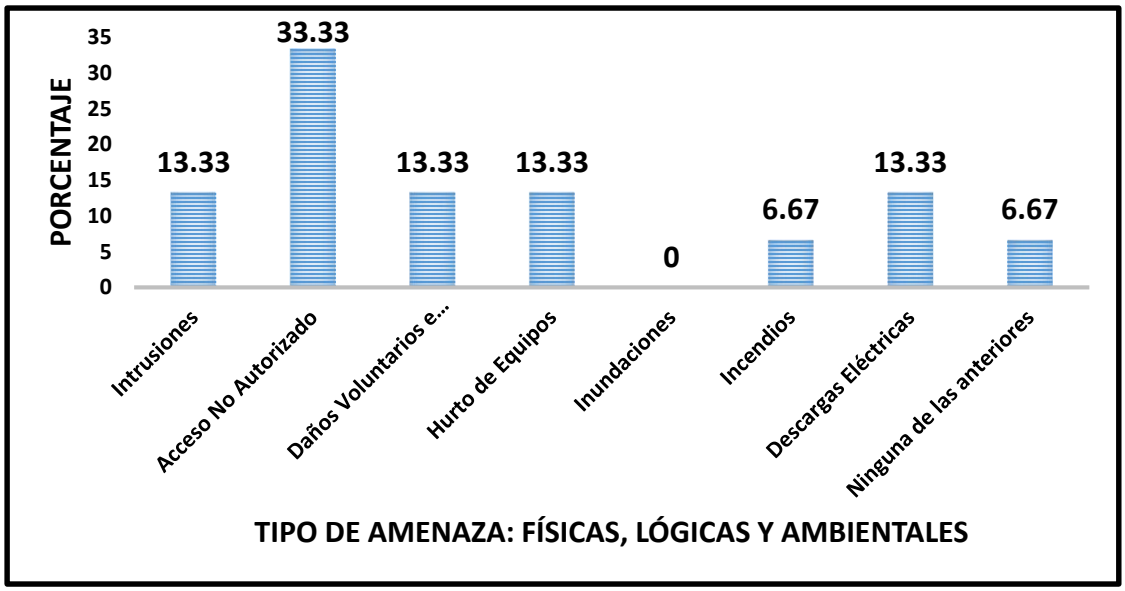
**Figura 4. El personal tiene acceso y conoce las políticas de seguridad de la institución.**




Fuente: Encuesta aplicada por los autores.

Ante la indagación relativa a la protección de los equipos sobre posibles amenazas físicas, lógicas y ambientales como: Intrusiones, Accesos No Autorizados, Daño Voluntario e Involuntario a la estructura y equipos de Red, Hurto de Equipos, Inundaciones, Incendios, Descargas Eléctricas por tormentas y demás se puede indicar en la figura 5, que el 33,33% da la mayor relevancia al Acceso No Autorizado a la Red, puesto que es la medida que más se ejecuta en las entidades investigadas.

**Figura 5. Los equipos están protegidos sobre posibles amenazas físicas, lógicas y ambientales.**




Fuente: Encuesta aplicada por los autores.

## 4. Conclusiones

- Con el advenimiento y desarrollo de las tecnologías de transmisión de datos, la seguridad se ha convertido en uno de los elementos fundamentales para el análisis del proceso de flujo de información a través de las redes de computadoras, lo cual se convierte en punto principal y sensitivo de estudio en la actualidad.
- Cada institución investigada presenta características muy particulares en cuanto a la gestión y seguridad de los activos de información que se administran en ellas, lo que presenta un reto mayor para su análisis, ya que al investigar temas sensitivos como

éstos, se requiere de la aprobación de niveles administrativos superiores para desarrollar una investigación a mayor escala técnica.

- Los resultados obtenidos denotan que existe un deficiente nivel de seguridad por el orden de los 40,31% en las instituciones objeto de investigación, lo que requiere de apropiadas acciones administrativas y técnicas que permitan mejorar la condición en las que se encuentran las redes de área local, pues se evidencia un riesgo latente en el proceso de administración de dichas redes.
- Se debe aplicar los estándares internacionales y utilizar métodos y estrategias más proactivas que permitan afianzar mayor seguridad a las redes y a los datos e información que fluyen a través de éstas, como: ISO/IEC 13335, ISO/IEC 17799 (27002), ISO/IEC 18028, RFC2196, IT Baseline, Cobit, ISO 27001.
- A pesar de que el 93,33% de las instituciones investigadas cumplen con todos los criterios técnicos establecidos para la buena administración de las redes de área local, los resultados expresan que no se ejecutan de forma adecuada.
- Las amenazas o problemas que se susciten sobre el funcionamiento de la red deben ser reportados, ya sea al departamento de informática, sistemas o soporte técnico en sus respectivos ministerios o entidades, las cuales están ubicadas en la ciudad de Panamá; lo que ocasiona que el tiempo de solución a los problemas presentados, sea muy lento y dependiendo del tipo de daño, deben esperar a que los especialistas en redes o de mantenimiento, lleguen a la entidad y resuelvan el problema, o en su defecto, autoricen para proceder a resolver el problema.

**Agradecimientos**

A todos los Administradores de las redes de área local y a los funcionarios de las distintas entidades gubernamentales que colaboraron con sus comentarios y aportaron mucha información a través de sus experiencias.

**Referencias bibliográficas**

Abad, A. (2012). *Redes locales* (primera ed.). Madrid, España: McGraw-Hill.

Aguilera, P. (2010). *Seguridad informática* (primera ed.). Madrid, España: Editex.

Alarcón, R. (2007). Artículo de reflexión, seguridad en redes como eje temático de investigación. *Seguridad en redes, sexto*, 165-173.

Gómez, Á. (2014). *Auditoría de seguridad informática.* Madrid, España: RA-MA.

Hernández, R., Fernández, C., Baptista, M. (2010). *Metodología de la investigación* (quinta ed.). México: McGraw-Hill.

Koontz, H., Weihrich, H., Cannice, M. (2012). *Administración: una perspectiva global y empresarial* (catorce ed.). México: McGraw-Hill.

Maiwald, E. (2005). *Fundamentos de seguridad de redes* (segunda ed.). México: McGraw-Hill.

Muñóz, C. (2002). *Auditoría en sistemas computacionales* (primera ed.). México: Pearson.

RISCCO. (2010). *Estudios sobre seguridad de información y privacidad de datos*. Recuperado de www.riscco.com: http://issuu.com/bellatorcreative/docs/2010_estudio_seguridad_privacidad_d/1?e=11504475/7402750

RISCCO. (2011). *Estudios sobre seguridad de información y privacidad de datos. Protegiéndose del riesgo interno*. Recuperado de www.riscco.com: http://issuu.com/bellatorcreative/docs/2011_estudio_sobre_la_seguridad_inf/1?e=11504475/7402524

RISCCO. (2012). *Moviéndose a la nube con cautela. Estudios sobre seguridad de información y privacidad de datos*. Recuperado de www.riscco.com: http://issuu.com/bellatorcreative/docs/2012_estado_de_la_seguridad_y_priva/15?e=11504475/7402389

Servin, L., Abad, A. (1982). *Introducción al muestreo* (segunda ed.). México, México: LIMUSA.

Stallings, W. (2004). *Comunicaciones y redes de computadores* (séptima ed.). Madrid: Pearson Prentice Hall.

Stuffelebeam, D., Coryn, C. L. (2014). *Evaluation theory, models, y applications* (segunda ed.). San Francisco, CA: Jossey-Bass.

Williams, C. (2013). *Administración* (sexta ed.). México: Cengage Learning.