Investigadores del grupo GISMAR en

1er Congreso Internacional Ciencia, Tecnología, Innovación y Desarrollo Territorial en la Corporación Universitaria Autónoma de Nariño, Pasto – 2016

José Javier Villalba Romero
Giovanni Albeiro Hernández Pantoja
Docentes del Programa de Ingeniería de Sistemas
Universidad Mariana

Figura 1. Participación en el 1er Congreso Internacional 2016.

El 1er Congreso de Ciencia, Tecnología e Innovación, C+T+I, y Desarrollo Territorial, es un evento académico-investigativo que reunió a connotados investigadores del orden local, nacional e internacional con el fin de presentar los resultados de investigaciones y estudios relacionados con el papel que tiene la ciencia, la tecnología e innovación con el desarrollo endógeno territorial en el nivel micro, meso, macro y meta, que se realizó en la ciudad de San Juan de Pasto y organizado por la Corporación Universitaria Autónoma de Nariño AUNAR del 19 al 21 de octubre de 2016. Participación en evento en la Figura 1.

En este evento se presentaron y discutieron resultados de investigación y reflexiones académicas sobre algunos aspectos que articulan la C+T+I como generadores de soluciones de los variados problemas de la sociedad actual y en donde participaron investigadores, profesionales, formuladores de políticas públicas, estudiantes, empresarios, industriales y público en general interesados en el tema.

El 1er Congreso de Ciencia, Tecnología e Innovación, C+T+I, y Desarrollo Territorial realizó un proceso exhaustivo de selección de artículos que se presentaron en la modalidad de ponencias en diferentes ejes temáticos entre los que se encontraban: Gestión del Conocimiento, Innovación y Emprendimiento, Globalización, Competitividad y Desarrollo Sostenible, Políticas de Ciencia, Tecnología e Innovación y Desarrollo Territorial, Prospectiva y Desarrollo Territorial, Mecatrónica, Competitividad y Sostenibilidad, Economía, Administración y Desarrollo Sostenible, Ciencia, Tecnología y Sociedad, Pedagogía, Educación y Desarrollo Integral Humano.

El grupo de investigación GISMAR del programa de Ingeniería de Sistemas de la Universidad Mariana, presentó los resultados del proceso de investigación sobre el tema de la "Aplicabilidad de Ley 1273 de 2009 o Ley de delitos informáticos en entidades públicas del municipio de Pasto – Nariño", dentro del eje temático Ciencia, Tecnología y Sociedad. Esta investigación fue realizada por los docentes José Javier Villalba Romero y Giovanni Albeiro Hernández Pantoja como investigadores principales y miembros activos del grupo y con el apoyo de estudiantes coinvestigadores: Andrés Felipe Quiñones Calpa y Jesús Alejandro Serrato Córdoba y cuyo tema, fue aprobado por el comité científico del evento para ser presentado en la modalidad de ponencia magistral en las fechas definidas por los organizadores.

Aplicabilidad de Ley 1273 de 2009 o Ley de delitos informáticos en entidades públicas del municipio de Pasto - Nariño

El proceso investigativo de "La caracterización de la aplicabilidad de Ley 1273 de 2009 o Ley de delitos informáticos en entidades públicas del municipio de Pasto – Nariño" se realizó de la siguiente manera:

Elaboración del instrumento. El instrumento que se utilizó para la recolección de datos en lo referente a la aplicabilidad de la ley fue una encuesta, la cual permitió hacer un vaciado de la información recogida de las entidades públicas de la ciudad de Pasto; contó con cuatro preguntas de aspectos generales, diecinueve preguntas específicas y una pregunta de tipo única. La encuesta es el medio de recolección de información circunstancial directo que permitió conocer el nivel de conocimiento de la Ley 1273 de 2009 o ley de delitos informáticos en las entidades en donde se aplicó, además de evidenciar el manejo de información de la misma y los protocolos de seguridad en el manejo de los datos que el encuestado pone en práctica, con este instrumento se detectaron situaciones de riesgo en las entidades públicas.

Validación del instrumento. Para la validación de la encuesta se utilizó la técnica de validación por criterio de expertos, que consiste en seleccionar 2 miembros del Grupo de Investigación de Ingeniería de Sistemas (GISMAR), que se encargaron de revisar y evaluar el formato, dando su respectiva observación y así proceder al mejoramiento de la misma. Las correcciones constaron de: cambio del volumen de preguntas, eliminación de preguntas innecesarias o que no aportaban al cumplimiento de los objetivos a los que estaban ligadas, redacción y replanteamiento de las preguntas abiertas.

Aplicación del instrumento (encuesta). La aplicación de la encuesta se realizó en un periodo de 2 semanas, se presentó en formato físico a cada una de las entidades listadas y se acompañó al encuestado durante todo el proceso, para evitar respuestas producto del mal entendimiento de la pregunta. La mayor parte de la encuesta cuenta con una firma del participante para garantizar la veracidad de los datos, habiendo una menor parte que se rehusó a cooperar en este aspecto por cuestiones de privacidad u otro inconveniente de tipo laboral. Se encuestó a un total de 20 personas, diferidos en 10 entidades públicas del municipio de Pasto, cada entidad proporcionando una encuesta por parte del jefe del área de sistemas, y otra proveniente de un funcionario que se escogió de manera aleatoria dentro de la misma.

Aspectos específicos de la encuesta

Las preguntas que compusieron esta parte del instrumento, estaban enfocadas en conocer el estado del conocimiento del participante, frente a la Ley 1273 de 2009 y por consiguiente, todo lo relacionado con los delitos informáticos, el impacto en la empresa y la aplicabilidad de estos conceptos en el funcionamiento y reglamentación de la misma. Al respecto, se obtuvieron los siguientes resultados:

Pregunta: ¿Ha escuchado usted sobre los delitos informáticos?

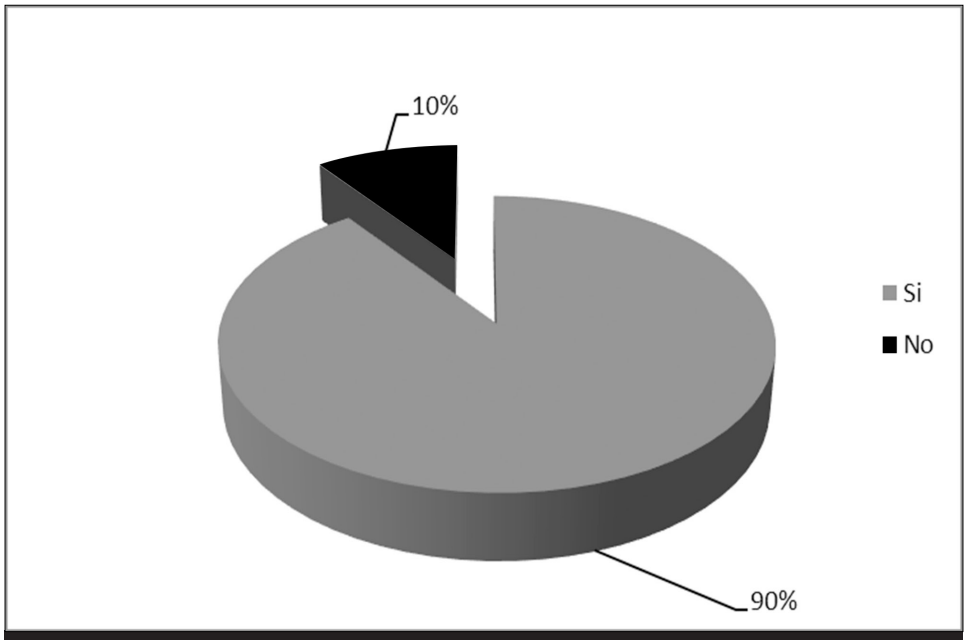

Figura 2. Nivel de conocimiento del concepto de delito informático.

En la Figura 2 se muestra que el 90% de las personas encuestadas tienen conocimiento respecto al concepto de delito informático, este valor es clave para esta investigación, aunque el nivel de conocimiento de cada persona varié; que el 90% de los participantes responda afirmativamente a esta pregunta, denota un gran avance en cuanto a la cultura informática y la promoción de la seguridad de la información en las entidades públicas.

Pregunta: ¿conoce usted sobre la Ley 1273 de 2009 o ley de delitos informáticos en Colombia?

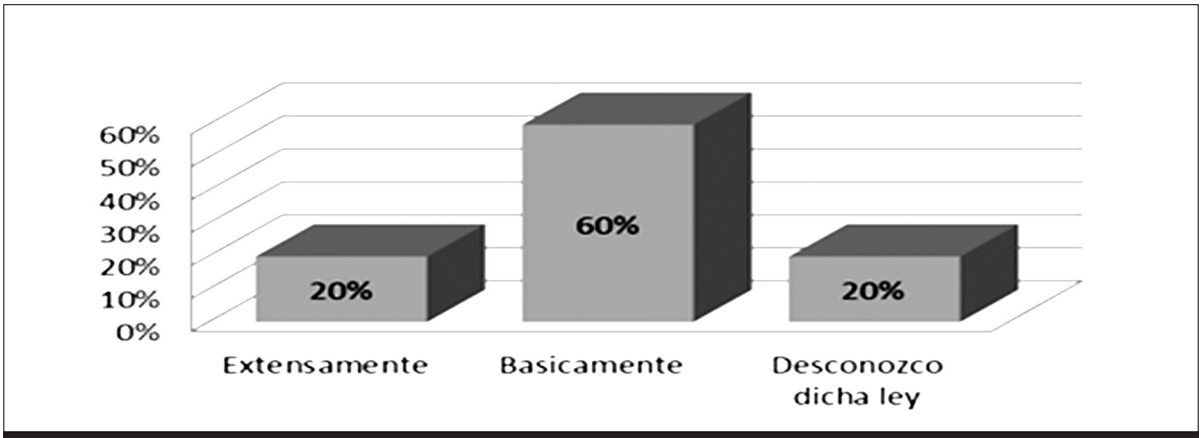

Figura 3. Nivel de conocimiento de la Ley 1273 o Ley de delitos informáticos.

En la Figura 3 se evidencia que la mayoría de los participantes de la encuesta, con un porcentaje del 60%, poseen un conocimiento básico de la ley de delitos informáticos y, un 20% que conocen extensamente dicha Ley. Pero el que un 20% de las personas objeto de investigación desconozcan la ley es un problema para las organizaciones, ya que se pueden estar presentando incidentes y estos no se reportan o no se sabe qué hacer con ellos. De igual manera, la falta de conocimiento puede provocar un aumento en la tasa de impunidad que se presenta actualmente en caso de ser víctima de un ataque.

Pregunta: Si su respuesta anterior fue afirmativa, seleccione el medio por el cual usted escuchó acerca de los delitos informáticos o acerca de la Ley 1273 de 2009.

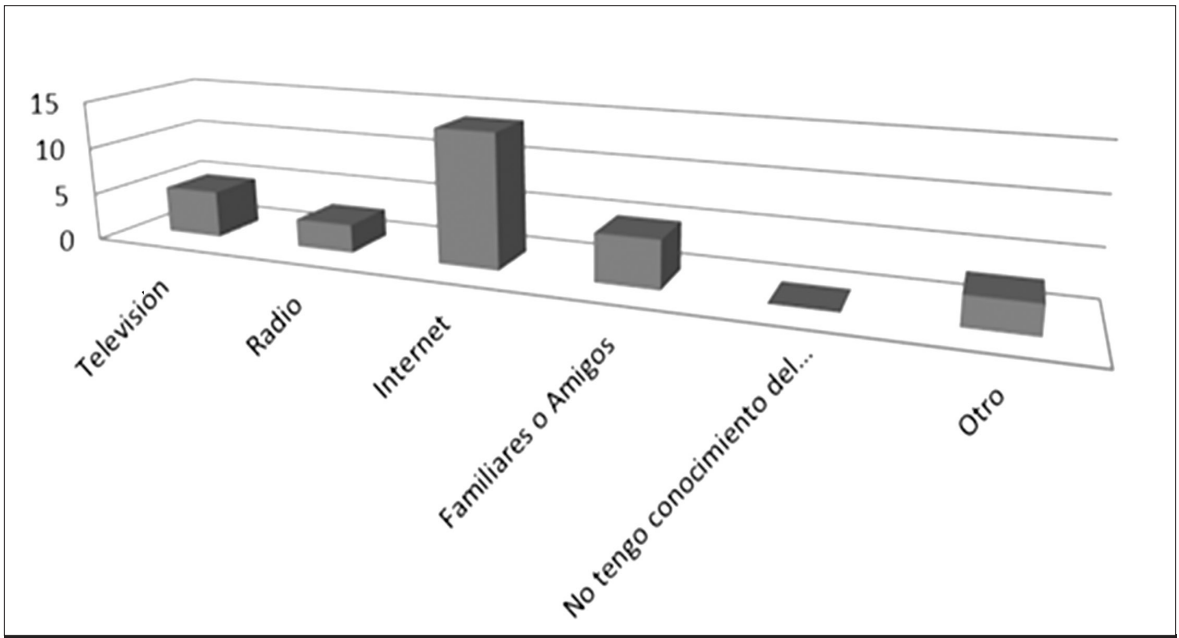

Figura 4. Medio de difusión más eficaz.

Al analizar los resultados de las respuestas a ésta pregunta se puede deducir que el medio de difusión de información más efectivo en cuanto a promover el concepto de la Ley de delitos informáticos y todo lo relacionado es el internet, con un porcentaje del 75%, seguido de la televisión y el contacto con familiares o amigos. Para la investigación es importante ésta información, ya que con ello se podrán fortalecer los medios de difusión de la Ley como es el internet y establecer estrategias que permitan una mayor difusión con otros medios (Ver figura 4).

Pregunta: ¿la entidad en la que usted desempeña su trabajo cuenta con un sistema de información?

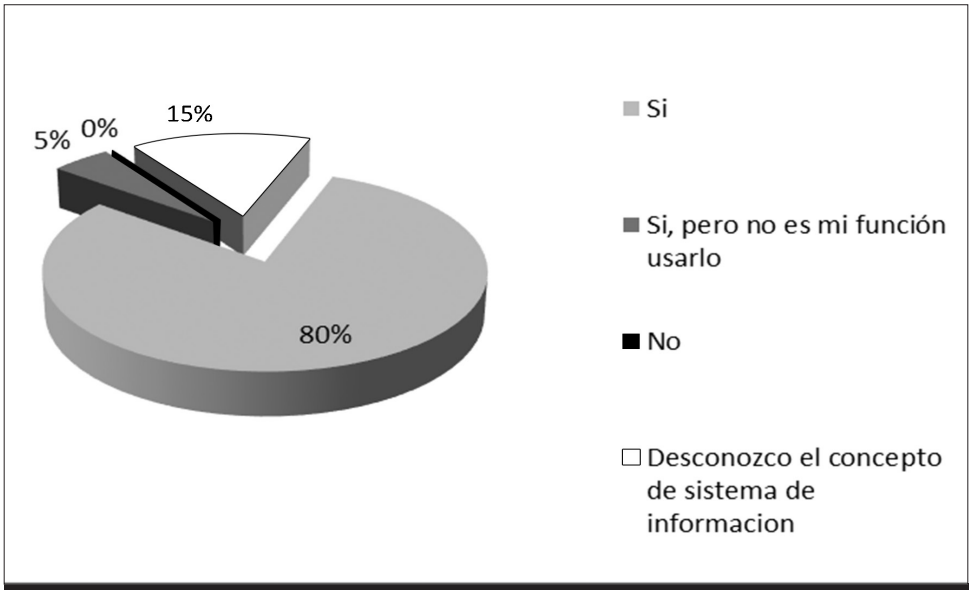

Figura 5. Uso de los sistemas de información en las entidades públicas de Pasto.

Siendo los sistemas de información uno de los puntos principales de los delincuentes informáticos, el objetivo de este ítem es determinar el uso de los sistemas informáticos en las entidades públicas del municipio. Un 85% de los participantes confirmó la existencia de dichos sistemas, aunque una minoría de ellos hizo evidente su baja participación o conocimiento sobre su funcionamiento. Por otro lado, un 15% de los participantes expresó desconocer dicho concepto, aunque la cifra no es alarmante, este porcentaje proyectado a una muestra mayor puede significar una considerable cantidad de personas cuyo desconocimiento puede conllevar a convertirse en un blanco fácil de un ataque informático. Por otro lado, la presencia de sistemas de información en la gran mayoría de las entidades públicas, sugiere que cada entidad debería tener protocolos y lineamientos de seguridad rigurosos (Ver Figura 5).

Pregunta: Seleccione los dispositivos mediante los cuales usted accede a Internet en su entidad.

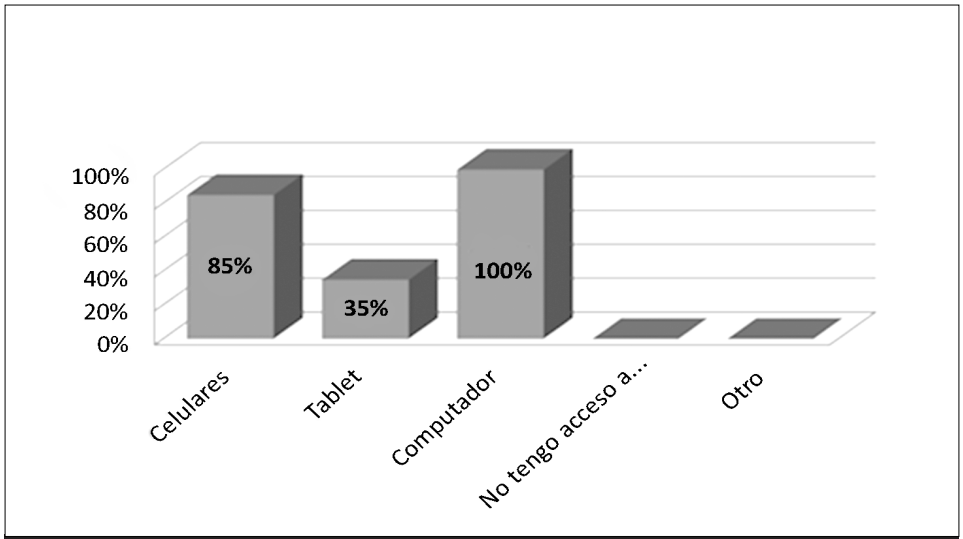

Figura 6. Dispositivos más usados para acceder a internet.

La Figura 6 muestra que un 100% de los participantes usa un computador, bien sea de escritorio o portátil, para acceder a internet en la entidad donde labora. Al ser esta una pregunta de selección múltiple, se tiene que de este 100% de participantes un 85% también usa los celulares y un 35% las tablet. La importancia de estos valores radica en el enfoque de las estrategias tanto de la entidad como de esta investigación, en cuanto a la prevención y aseguramiento de dichos medios, debido a que los protocolos y políticas de seguridad varían de dispositivo a dispositivo.

Pregunta: ¿Maneja usted información personal importante de otras personas?

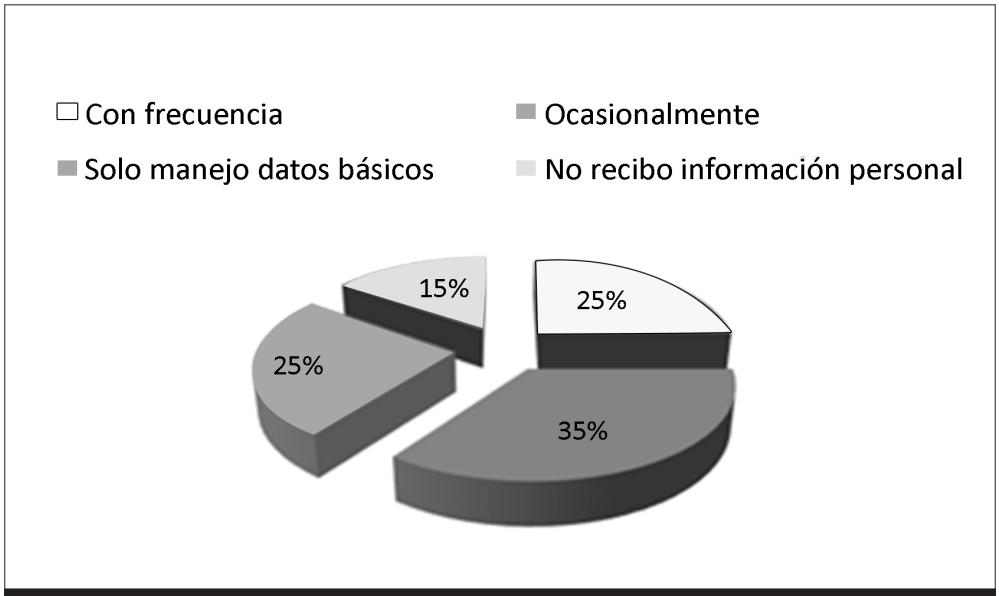

Figura 7. Manejo de información personal en las entidades públicas.

Analizando la Figura 7 se encuentra que el 60% de los participantes encuestados manejan información personal en la entidad que trabajan de manera frecuente u ocasional, esto comprende un gran porcentaje de personas cuya responsabilidad con la información es considerable, de ahí que las personas que se incluyan en este grupo compartan pertenencia con el grupo de participantes que desconoce la Ley 1273 y/o el concepto de delito informático, supondría un gran riesgo frente a dicha información. El 15% no recibe información personal esto no los hace menos vulnerables, pues esta pregunta contempla el manejo de datos de terceros, pero cada individuo maneja su propia información personal. Por último, el 25% maneja información básica, pero aplica en todo caso los puntos especificados anteriormente.

Pregunta: ¿Ha sido víctima de pérdida de información en su estación de trabajo?

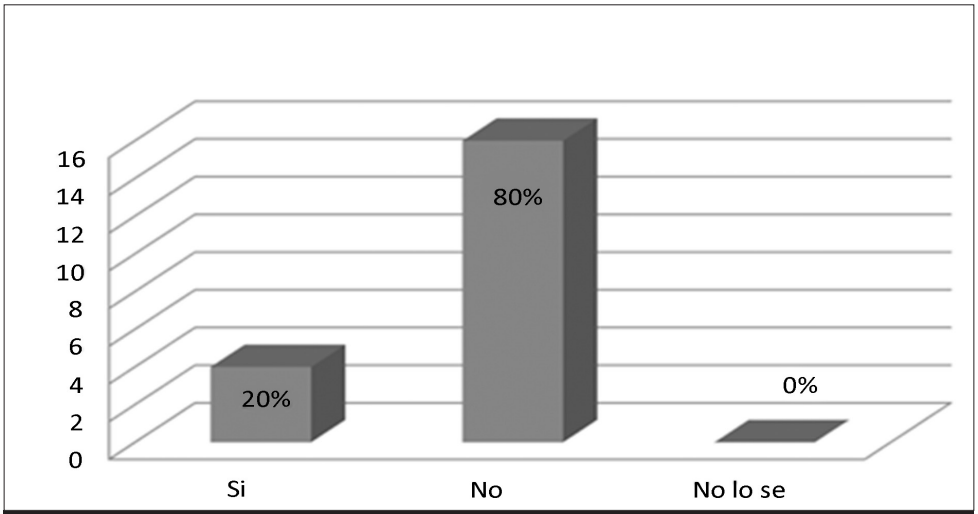

Figura 8. Perdida de información en el puesto de trabajo.

Los datos de la Figura 8 evidencian que no se ha presentado pérdida de información en un gran porcentaje de los participantes con un 80%, esto no siempre sugiere que la seguridad de las entidades sea óptima, puede derivarse del nivel de conocimiento del individuo, sus prácticas personales de seguridad o del simple hecho de que la información que maneje no represente un blanco común para los ataques. Por otro lado, un 20% confirmó casos de pérdida de información, aunque ninguno lo reportó como un delito; este valor es preocupante, ya que evidencia malas prácticas de seguridad en las entidades y que han incidido en ataques informáticos que han ocasionado pérdida de información.

Pregunta: ¿Conoce usted sobre los delincuentes informáticos?

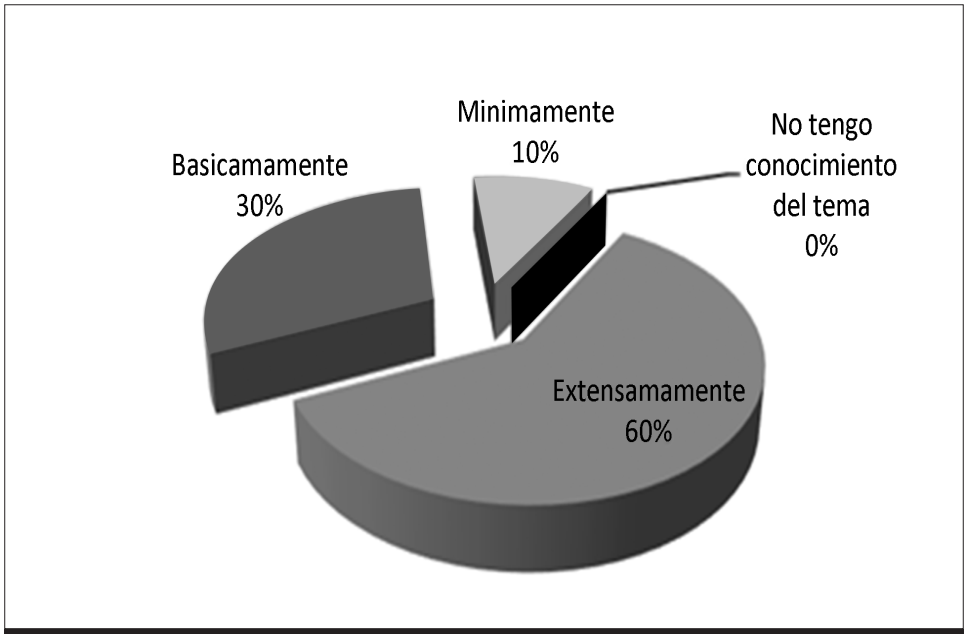

Figura 9. Conocimiento sobre delincuentes informáticos.

La Figura 9 muestra que la totalidad de los participantes, aunque en diferentes niveles, conocen sobre los delincuentes informáticos. Un porcentaje del 60% conociendo extensamente sobre el tema, debido a que el 50% de la muestra son jefes de áreas de sistemas, se presumía que al menos un porcentaje equivalente a éste tendría esta afirmación, el 10% adicional indica que el conocimiento sobre el tema se ha extendido incluso a áreas donde su relevancia no es significativa. El 40% restante, con un conocimiento básico o mínimo, son objetivos de cuidado, aunque tener un conocimiento superfluo de un tema puede ser de gran ayuda, la constante evolución de los delitos informáticos sugiere que básico no es suficiente, y dichos individuos deberán ser capacitados en este tema.

Pregunta: ¿Conoce usted algún caso de delito informático que haya ocurrido en su entidad?

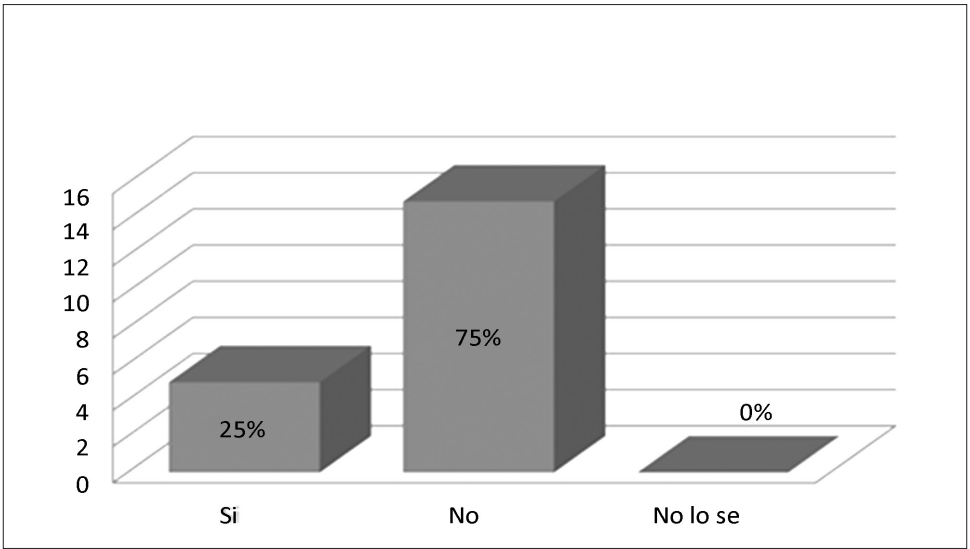

Figura 10. Conocimientos sobre casos de delitos informáticos.

En la Figura 10 con un porcentaje de 75%, manifiesta que no conoce sobre casos de delitos informáticos, esto no siempre significa que realmente no se hayan presentado casos; el desconocimiento de lo que se conoce como delito, puede causar que los funcionarios estén siendo víctimas sin siquiera saberlo, además, por medio de observación directa e intercambio de información con los jefes de las áreas de sistemas, se conoce que las entidades prefieren mantener en confidencia cualquier tipo de ataque que se presente, esto puede afectar de manera considerable los resultados obtenidos en este ítem.

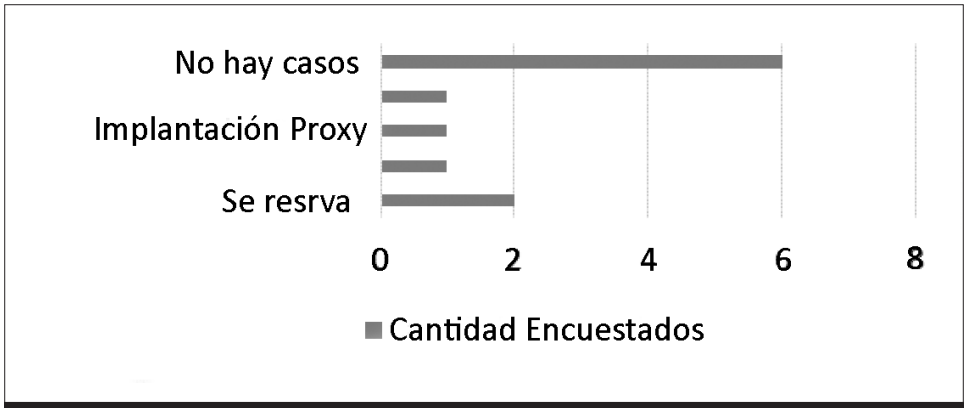

Figura 11. Casos de pérdida de información.

Luego de observar los datos de la Figura 11 es notorio que en la mayoría de la muestra no existen casos de pérdida de información, algunos expresaron situaciones que no ameritan ser mencionadas y no entran dentro el rango de esta investigación, en otros casos, se evidencia accesos a los sistemas de la empresa, aunque en menor medida considerando el flujo de información sensible descrito en los ítems anteriores, solo se obtuvo un caso de robo de identidad, este dato resulta ser curioso al ser contrastado con la información proporcionada por el CTI, donde claramente se afirmó que los casos de robo de información son comunes en la ciudad, aunque se debe aclarar que puede que el encuestado haya hecho referencia a su identidad corporativa.

Pregunta: ¿Ha sido usted víctima de suplantación de identidad, robo de perfiles sociales, extorsión electrónica o algún tipo de perjuicio que se haya originado desde Internet?

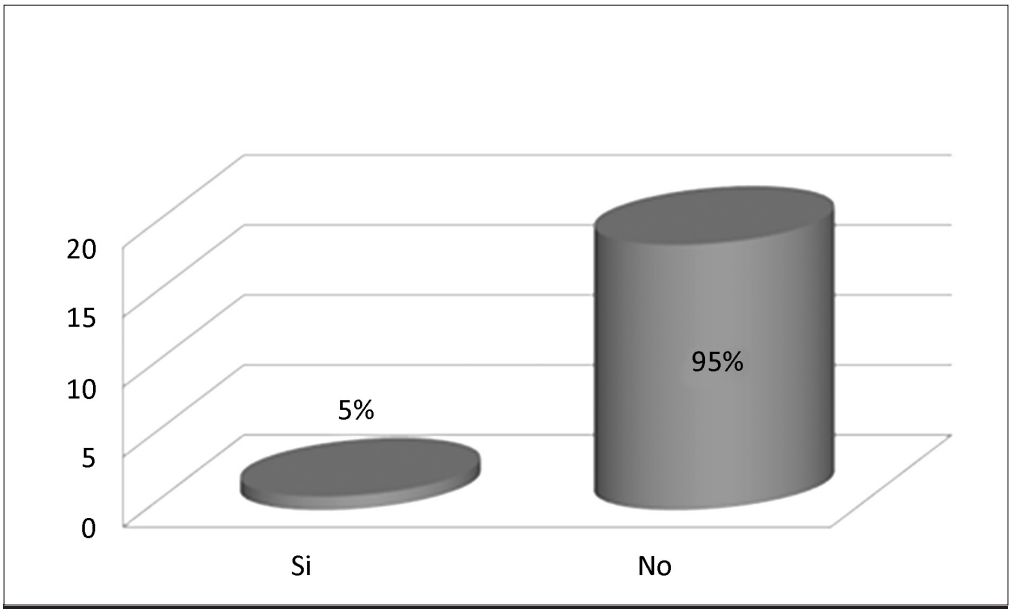

Figura 12. Víctimas de delitos informáticos.

La Figura 12 evidencia que la mayoría de personas no ha sido víctima de un delito informático, al igual que el ítem anterior, este resultado puede verse afectado por diferentes factores, como el desconocimiento, motivos personales, políticas de la empresa. Se debe tener en cuenta que el 50% de los participantes son jefes de áreas de sistemas, por lo tanto, se presumía que el resultado sería un porcentaje mayor al 50%.

Pregunta: ¿Conoce usted el reglamento de seguridad de su entidad en cuanto al tratamiento de la información?

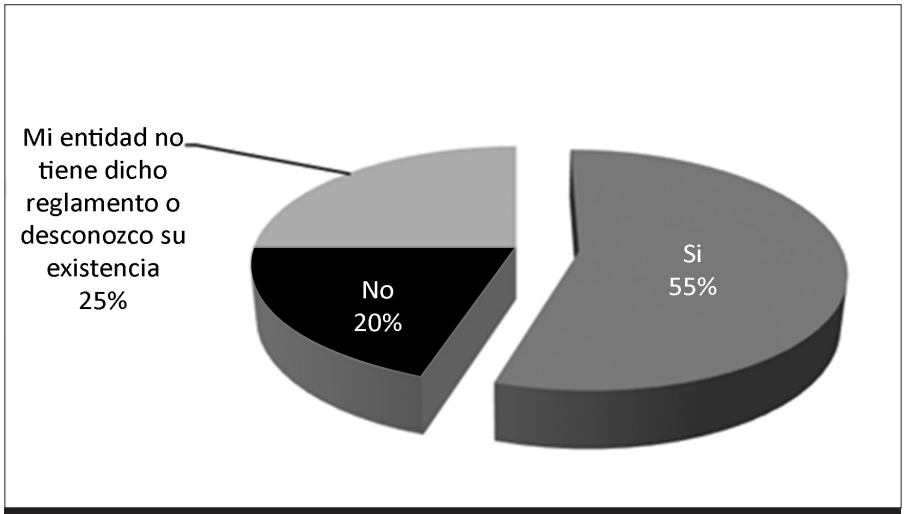

Figura 13. Conocimiento sobre políticas de seguridad.

Los datos que evidencian la Figura 13 muestran que el 55% de las personas tienen conocimiento respecto a políticas de seguridad que se presentan en la entidad pública, frente a un 45% de los participantes que no conoce dicho reglamento o afirma que la entidad no tiene reglamentos frente a esto. Esta cifra es alarmante, considerando la presencia de los sistemas de informáticos y el manejo de la información sensible en las mismas. La ausencia de los reglamentos para controlar o reglamentar estas situaciones, sugiere un bajo conocimiento sobre el impacto que puede tener un ataque informático no controlado, esto dejando en evidencia que, aunque un gran porcentaje conoce el concepto de delito informático, su impacto en la realidad del entorno empresarial aún no está bien definido.

Pregunta: Mencione las prácticas de seguridad que usted aplica en la entidad de acuerdo con su nivel de educación y/o los lineamientos de la misma.

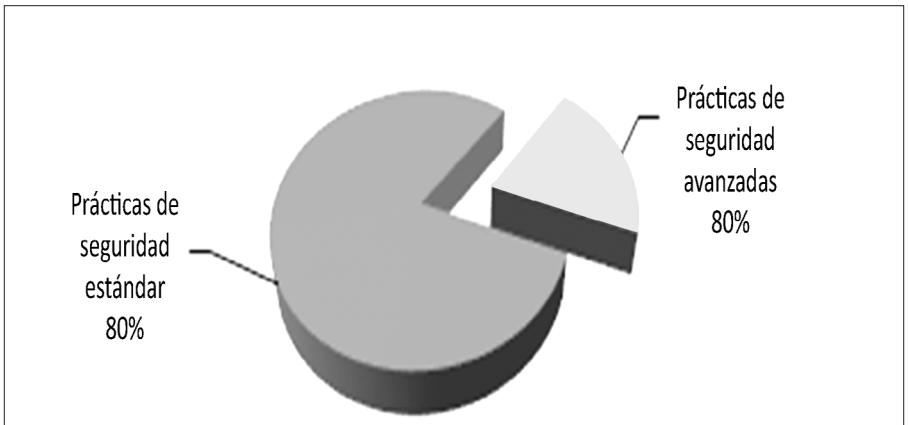

Figura 14. Prácticas de seguridad informática por tipo.

En la Figura 14 se nota que un 80% de los encuestados manifiestan disponer de prácticas estándares de seguridad y solo un 20% realiza prácticas avanzadas. Las prácticas de seguridad que emplean los jefes de sistemas en la entidad en la cual laboran, para efectos de análisis de información en esta investigación, se dividieron en: prácticas de seguridad estándar, que comprenden los lineamientos básicos de la informática, prácticas de seguridad actualizadas y estandarizadas, que comprenden protocolos como uso de conexión END POINT, acceso remoto, sesiones de usuario personalizadas, clasificación de credenciales por zonas, cifrado de datos, contraseñas robustas, IPS/IDS y aplicando normas PCI e informando una amenazada de riesgo. De acuerdo con estas respuestas, los profesionales del área de sistemas, en su gran mayoría aplican técnicas básicas que de ninguna manera pueden ser suficientes para la protección de una entidad de orden público, solo dos de las diez empresas encuestadas, utiliza prácticas de seguridad actualizadas y estandarizadas, lo cual es alarmante al proyectar este porcentaje a nivel departamental, debido al bajo impacto de los delitos reflejado en los resultados, el área de sistemas ha dejado a un lado la constante evolución e implementación de nuevas técnicas de seguridad, enfocando sus esfuerzos a otras áreas, este comportamiento debería ser replanteado, pues es claro que tanto en el ámbito laboral, profesional, incluso en el ámbito económico, prevenir una pérdida es más viable que remediarla.

Si bien el nivel de conocimiento en cuanto al concepto de delito informático y ley de delitos informáticos es superior al esperado, se encuentra una grave falencia frente a la interpretación de ese conocimiento por parte de los participantes. Conocer el tema no garantiza al individuo su seguridad, solo lo hace más preventivo frente a ella; es evidente que aunque las personas, por diferentes motivos, conocen el concepto, no le dan la importancia que requiere, subestimando el daño que un incidente de este tipo puede causar, esto viéndose reflejado en la falta de lineamientos institucionales para tratar delitos informáticos, la poca motivación a denunciar estos delitos y la carencia de prácticas de seguridad robustas. De esta manera, se concluye de la información recolectada por medio del instrumento, que la ley de delitos informáticos y el concepto de delito informático, se conoce en las entidades públicas, pero contrario al resultado lógico que esto denota, su aplicabilidad ha sido en extremo baja y no ha influenciado su funcionamiento como debería haberlo hecho.

Conclusiones

Si bien el nivel de conocimiento en cuanto al concepto de delito informático y ley de delitos informáticos es superior al esperado, se encuentra una grave falencia frente a la interpretación de ese conocimiento por parte de los participantes. Conocer el tema no garantiza al individuo su seguridad, solo lo hace más preventivo frente a ella, es evidente que aunque las personas por diferentes motivos conocen el concepto, no le dan la importancia que este requiere, subestimando el daño que un incidente de este tipo puede causar; lo anterior, viéndose la poca motivación a denunciar estos delitos y la carencia de prácticas de seguridad robustas. De la información recolectada se concluye que, el reflejo en la falta de lineamientos institucionales para tratar delitos informáticos y el concepto de delito informático, se conoce en las entidades públicas, pero contrario al resultado lógico que esto denota, su aplicabilidad ha sido en extremo baja y no ha influenciado el funcionamiento de estas como debería de haberlo hecho.

En cuanto a los resultados de la encuesta, se obtuvieron valores relevantes que vale la pena resaltar; el 90% de la muestra conocía el concepto de delitos informáticos y, el 80% de los mismos conocía a nivel básico o extenso, la Ley 1273 de 2009, lo cual muestra una relación directa frente al conocimiento del tema como tal y la necesidad de profundizar frente a los mecanismos jurídicos que la regulan. Por otro lado, se encontró que la totalidad de las entidades objeto de investigación, poseen un sistema de información, aunque no todos los participantes manifestaron tener alguna relación con el o conocer su funcionamiento. Con respecto a los casos de delitos informáticos a nivel institucional, 5 participantes, manifestaron haber tenido casos de delitos informáticos en la entidad en la cual se desempeñaban, aunque ninguno de ellos denunció dicho suceso ante las autoridades. A nivel personal, el 90% de la muestra total, afirmó nunca haber sido víctima de ningún tipo de ataque informático que afecte directamente su integridad a nivel social, casos como robo de identidad o perfiles de redes sociales, el 10% restante, se opuso a hablar sobre los sucesos. Como parte final, se evidenció que el 45% de la muestra desconoce sobre las políticas de seguridad informática de su entidad, débase a negligencia del funcionario o por la inexistencia de dicho documento, y partiendo de este hecho, la pregunta única diseñada para los jefes de sistemas, mostró que el 80% de los participantes que representaban el área de sistemas, aplican prácticas de seguridad básicas que muchas veces, no son suficientes, considerando el tipo de entidad y la información que manejan.

De la entrevista a las autoridades encargadas de regular y llevar a términos judiciales los casos reportados, se concluyó que el impacto de los delitos informáticos en la ciudad, de acuerdo a la información obtenida, ha sido mínimo a nivel de las entidades públicas, pero amplio en cuanto a la población se refiere; aunque no impliquen bienes materiales o grandes catástrofes administrativas, vulnerar la privacidad de un sujeto no debería ser objeto de menor atención o preocupación. El promover el concepto de delito informático y fomentar el entendimiento de la Ley 1273 de 2009 tanto en la ciudadanía, como en los entes jurídicos, es clave para detener y combatir efectivamente la creciente amenaza que esto representa para todos.

Bibliografía

Acosta, B. (2012). Los delitos informáticos y su perjuicio en la sociedad. Trabajo de grado (Abogado). Universidad Técnica de Cotopaxi, Unidad Académica de Ciencias Administrativas y Humanísticas. Ecuador. Recuperado de http://repositorio.utc.edu.ec/bitstream/27000/197/1/T-UTC-0224.pdf

Cerón, M. (2006). *Metodologías de investigación Social*. Santiago, Chile: Lom ediciones.

McAfee Labs. (2016). Informe de predicciones sobre amenazas para 2016. Madrid. España. Recuperado de http://www.intel.es/content/dam/www/public/emea/es/es/documents/reports/mcafee-labs-2016-threats-and-predictions-report.pdf >

Ochoa, S. (2007). Habermas. Conocimiento e interés: El nuevo estatuto de la razón comprensiva. Recuperado de http://serbal.pntic.mec.es/~cmunoz11/ochoa55.pdf

Symantec. (2013). Informe de seguridad informática. Dos de cada 10 empresas, víctimas de robo de datos: El 31 por ciento de los ataques informáticos en Colombia apuntan a las pyme. *El Tiempo*. Recuperado de http://www.eltiempo.com/archivo/documento/CMS-12758292>

Tiedemann, K. (1985). *Poder informático y delito.* Barcelona, España.