EL LIDERAZGO DE LOS RECURSOS CIBERNÉTICOS EN LA EMPRESA Y LA RESPONSABILIDAD DE LA ACADEMIA

Por: Jenis del Carmen Sagbini Echávez

Las Nuevas tecnologías de la Información y la Comunicación (NTIC) han sido las protagonistas de las últimas transformaciones sociales en el mundo. Los cambios han sido tan gigantescos que hoy los seres humanos se comunican y hacen las cosas de manera diferente. Ha sido tanto el impacto de estas herramientas, que actualmente la gente sabe demasiado y no hay lugar donde esconderse (en Jofré,2000:158), reafirmando que se hizo realidad lo de la "*aldea global*" que hace 49 años expresó Marshall McLuhan en su libro "Guerra y Paz en la Aldea Global".

Si bien, las empresas están involucradas indiscutiblemente en estas transformaciones y se sumergen cada día más en una dependencia de la interconexión abierta y de la promoción para generar capital. Esto ha permitido que la información, que es el principal factor clave para la toma de decisiones, esté expuesta en los canales digitales conllevándola a ser susceptible a sufrir ataques de cualquier magnitud. Es aquí donde el liderazgo administrativo tiene la obligación de diseñar estrategias para utilizar de manera eficiente los recursos cibernéticos asegurando su integridad llevando a la empresa a algo tan antiguo como el arte de la guerra o los ejércitos a la victoria. En este marco, una estrategia no es más que un plan de acción que, teniendo en cuenta los recursos disponibles y las posibles reacciones del enemigo, se propone alcanzar la victoria. (Alfonso, 2000)

Hechas las consideraciones anteriores, el presente escrito tiene como objetivo, hacer una reflexión teórica debido a la necesidad de implementar el concepto de ciberseguridad organizacional en los futuros administradores de recursos informáticos, resaltando la responsabilidad que tiene la academia en la formación del talento humano.

En este mismo orden y dirección, se justifica este escrito por los estudios que se han encontrado y que se analizan a continuación, los cuales muestran la necesidad de la realización de una intervención en el tema. Es evidente entonces, que la información presentada aquí es útil para los directores de tecnologías de información y podrían encontrar herramientas que le permitan sensibilizar e implementar para el desarrollo de actividades de ciberseguridad. Cabe agregar que la evidencia de literatura indexada con respecto al tema, es limitada y en su mayoría, fueron extraídos de documentos publicados por organismos internacionales y entidades del estado colombiano.

Entrando en contexto, el último informe del Banco Interamericano de Desarrollo (BID) y la Organización de Estados Americanos (OEA), que lleva por título: "Ciberseguridad 2016, Estamos preparados en América Latina y el Caribe?", asegura que Colombia está incluida en los únicos 6 países de Latinoamérica y el Caribe que tienen planes de seguridad cibernética: le acompañan Brasil, Jamaica, Uruguay, Panamá, Trinidad y Tobago.

Estos planes de seguridad cibernética están basados en el gran compromiso que tiene el Estado Colombiano y que a través del auspicio del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el Ministerio de Defensa, el Departamento

Nacional de Planeación y otras instituciones nacionales claves; se logró establecer la política nacional de Seguridad Cibernética CONPES 3701. A los efectos de éste, se creó el Centro Cibernético Policial (CCP) especializado dentro de la Policía Nacional de Colombia, bajo la Dirección de Investigación Criminal e INTERPOL (DIJIN), quien es la principal unidad designada para investigar delitos cibernéticos en todo el país.

Con referencia a lo anterior, según el Observatorio de la Ciberseguridad en América Latina y el Caribe, ((OEA) B. I.), Colombia ha madurado la conciencia social sobre la importancia de la privacidad y la seguridad en internet y la confianza en los sistema digitales del país ha crecido notablemente; en parte, debido a las campañas nacionales del MinTIC, a estrategias de entidades como el Grupo de Respuesta de Emergencias Cibernéticas de Colombia (ColCERT), al programa CERT de Colombia que funciona principalmente como un mecanismo de respuesta a incidentes cibernéticos específicos de la organización, y los programas de gestión del riesgo que han comenzado a surtir efecto. Este informe afirma, que existen leyes en vigor que obligan a las empresas a implementar políticas de protección de datos en el lugar de trabajo como la Ley 1581 de 2012 y el Decreto 1377 de 2013 y que Colombia ha probado una legislación procesal penal integral y de efectiva penalización (Ley 1273 y Ley 906) abordando los delitos cibernéticos y reconociendo los tratados internacionales con Interpol y Europol. ((OEA) B. I., 2016)

En este propósito, en el último informe del Centro Cibernético Policial (marzo 2017) menciona, que en el año 2014, del total de incidentes atendidos, el 92% afectaban los ciudadanos del común y que este porcentaje se vió disminuido en 63% para el 2015 y en 57% para el 2016. Mientras tanto, en el sector empresarial pasó de un 5% a un incremento del 28% en los reportes atendidos. Estas cifras ratifican lo planteado en el documento IOCTA 201610 (Internet Organised Crime Threat Assessment) del European Law Enforcement Agency de EUROPOL11 , referente a la Tricotomía del delito, en donde se estipula que a mayor volumen de ataque, con mayor número de víctimas, donde su nivel de seguridad y protección es bajo, el beneficio por ataque es menor. Pero si por el contrario, el ataque se realiza a un sector reducido o especializado, por ejemplo, el sector financiero, con un ataque más sofisticado, que requiera de mayor habilidad y destreza, con niveles de innovación alto, el beneficio por ataque será mucho mayor. (Policía Nacional, 2017)

En este mismo orden de ideas, este informe revela que durante los años 2014, 2015, 2016 y lo que va del 2017, se han recibido 13.77427 denuncias por violación a la ley 1273 de 2009, dando un panorama de los delitos que más se denuncian en el país. En cuanto a las tipologías criminales denunciadas ante la Policía Nacional en el citado período de tiempo, se evidencia un aumento significativo en el número de estas por conductas delictivas que vulneraron la integridad personal, patrimonio económico de entidades públicas y privadas y así como la integridad, disponibilidad y confidencialidad de la información que circula a través del ciberespacio. Los porcentajes más elevados de los principales delitos informáticos reportados, está encabezado por el hurto por medios informáticos y semejantes con un 68%, seguido del acceso abusivo a un sistema informático que se ubica en el segundo ítem con un 13% y la violación de datos personales con un 12%.

Así lo demuestran el Tercer Estudio de Transacciones No Presenciales 2015 y el Estudio de Hábitos del Comprador Online 2016, presentados por la Cámara Colombiana de Comercio Electrónico (CCCE), en los cuales se señala que en 2014 el 76% de los internautas colombianos compraron al menos un producto o servicio en línea; las transacciones no presenciales crecieron en 2015 un 64% respecto al 2014; las plataformas de pago en línea (CredibanCO, Redeban y PSE) reportaron un total de 49 millones de transacciones por valor de 16.329 millones de dólares, que equivale al 4,08% del PIB 2015, frente al 2,63% del PIB 2014. (CCCE, 2016)

De acuerdo con los razonamientos que se han venido planteando, las empresas, los gobiernos y los ciudadanos no están exentos de ser víctimas de un ciberataque en Colombia. Las amenazas aumentan cada día, tanto así que en desde agosto del 2016 hasta agosto del 2017, se han presentado un total de 198 millones de ataques según revela un informe de la firma de ciberseguridad DIGIWARE. De acuerdo con la compañía, diariamente se registran en promedio 542.465 incidentes y el impacto de los delitos informáticos ha generado pérdida por 6.179 millones de dólares en el país. El sector financiero es el más afectado por los delitos informáticos en el país, con 214.600 ataques por día, seguido de telecomunicaciones con 138.329; Gobierno con 83.756 e industria con 51.263 casos. (Tecnóferas, 2017)

A pesar de estos grandes esfuerzos e iniciativas en materia de seguridad y delitos cibernéticos que lleva a cabo el Gobierno de Colombia y que han dado resultados, existen muchas oportunidades para mejorar pues el abanico de responsabilidades relacionadas con asuntos cibernéticos es amplio, tanto en el ámbito organizacional y social. Las empresas del sector productivo y de servicios, tienen una amplia participación cuando realmente consideran expandirse utilizando internet y herramientas tecnológicas de alto impacto. Si bien, la academia como generadora de administradores de recursos cibernéticos, también es fuente de conciencia para las empresas y forma parte de la llamada Triple Hélice de Desarrollo (THD) que Etzkowitz mencionó en los años 90. Esta estrategia fue diseñada para actuar y promover la innovación, contribuyendo a la formación del tejido social y empresarial. La Universidad no solo tiene la responsabilidad de formar profesionales para ser los futuros administradores de recursos cibernéticos, si no también, debe evolucionar tomando como base la investigación a esferas de transferencia del conocimiento a la sociedad y las empresas.

De los anteriores planteamientos se deduce que los ataques seguirán existiendo y que tanto el usuario de las NTIC, así como las empresas, tienen una gran responsabilidad para la mitigación del riesgo. La ausencia de una cultura de información y seguridad cibernética está en igual responsabilidad. Es por ello, que a nivel organizacional, la administración de la seguridad cibernética juega un rol muy importante y se hace necesario establecer una fuerza de trabajo capacitada y disciplinada en un marco de modernización que permita diseñar mecanismos y estrategias de seguridad cibernética en los campos operativos y administrativos. Bajo este esquema, el liderazgo de recursos cibernéticos debe estar enmarcado en un profesional que desarrolle habilidades con visión integradora, capacidad de evaluar contingencias, analizar riesgos, elaborar procesos de monitoreo y control y desarrollar competencias que permitan enfrentar cualquier cambio generado por la fuentes externas de la organización.

Tal como se ha dicho, para una empresa que administre sus recursos cibernéticos adecuados, deberá contemplar unos vectores de mitigación como la creación de una política adecuada para la gestión de aplicaciones, establecer un límite en el uso de aplicaciones e intercambio de archivos, realizar de manera periódica y adecuada las copias de seguridad, establecer perímetros de seguridad en las redes de acceso para poder filtrar y restringir los puntos de acceso, implementar un proceso continuo de gestión de la ciberseguridad y de cambios derivados de los incidentes y por último; y muy importante, formar al personal de operación y mantenimiento desarrollando un espíritu de sentido de pertenencia con respecto a la seguridad cibernética de la organización.

Liderar los recursos cibernéticos en una organización genera una gran responsabilidad por lo que el profesional a cargo deberá estar en un continuo aprendizaje por el dinamismo que generan las NTIC. Es por ello y con referencia a lo anterior, que para la autora de este escrito; se hace pertinente el desarrollo de una formación integral para todos esos profesionales que se desarrollarán en las organizaciones de administración de los recursos cibernéticos. Como formadora del capital humano que liderará la protección de la integridad, la disponibilidad y la seguridad de la información en las empresas; el impacto que se generaría será alto debido a la alineación de nuevos profesionales que contribuirán a mejorar el *corpus* teórico y didáctico de un área del conocimiento favoreciendo al progreso, la calidad y la excelencia.

Dadas las condiciones que anteceden, la formación que la academia imparte deberá dar respuesta a la consecución de desarrollo de competencias que en la realidad laboral actual existe. Se observa claramente que en Colombia se estima un déficit de profesionales tecnológicos en 50.000 para el año 2018 y que en dos años será de 80.000. (Colombiana, 2016) Las universidades son consciente de esta gran oportunidad y se preocupa por capacitar cada vez mas a sus docentes debido a los constantes cambios que las NTIC implanta en las empresas.

A manera de conclusión, se puede afirmar que los cambios tecnológicos generan grandes transformaciones sociales por lo que las empresas y los usuarios que hacen parte de estos cambios, también poseen responsabilidades en la minimización de los riesgo cibernéticos. Colombia ha logrado avances en materia de ciberseguridad debido a políticas gubernamentales pero aún, se requiere de profesionales capacitados en TI basados en lo que el mercado laboral oferta. Es entonces, donde la academia, quien forma los futuros profesionales que administrarán los recursos cibernéticos en las organizaciones, deberán desarrollar habilidades y competencias adecuadas a las que el entorno laboral requiere.

Bibliografía consultada

Teresa, A. P. (2012). Marshall Mcluhan, Las Redes Sociales y la Aldea Global. *Revista Educación y Tecnología* (2), 20.

David, H. (s.f.). *El Medio es el Mensaje: La Aldea Global de Marshall Mcluhan*. Obtenido de http://davidhuerta.typepad.com/blog/2011/12/la-aldea-global-marshall-mcluhan.html

Orlando, R. C. (2016). *Administración del Riesgo Cibernético, un Enfoque desde la Alta Gerencia Empresarial en Colombia.* Universidad Militar Nueva Granada, Facultad de Estudios a Distancia, Especialización en Alta Gerencia, Bogotá.

Alfonso, M. E. (2000). *Hacia una Nueva Teoría de la Empresa* (79 ed.). (I. E. Humanismo, Ed.) Navarra, España: Universidad de Navarra.

Fernando, N. W. (2015). *Importancia de la Implementación del Concepto de Ciberseguridad Organizacional en las Organizaciones tipo Pymes* (Universidad Militar Granada ed.). Bogotá, Cundinamarca, Colombia.

OEA, O. d. (2014). *Tendencias de Seguridad Cibernética en América Latina y el Caribe.*

(OEA), B. I. (2016). *Ciberseguridad 2016, Estamos preparados en América Latina y el Caribe?*

(OEA), B. I. (s.f.). *Observatoriociberseguridad.com*. Recuperado el 3 de dic de 2017, de Observatorio de la Ciberseguridad en América Latina y el Caribe: http://observatoriociberseguridad.com

Policía Nacional, D. d. (2017). *Informe Amenazas del Cibercrimen en Colombia 2016-2017.* Centro Cibernético Policial.

Tecnóferas. (27 de sept de 2017). A diario se registran 542.465 ataques informáticos en Colombia. *El Tiempo* .

Mas Torelló, O. (2011). El Profesor Universitario: Sus Competencias y Formación. *Profesorado Revista de Currículum y Formación del Profesorado , 15* (3), 17.

CCCE, C. C. (2016). Tercer Estudio de Transacciones No Presenciales 2015 y Estudio de Hábitos del Comprado Online 2016.

CCP, C. C. (2017). *Informe Amenazas del Cibercrimen en Colombia 2016-2017.* Policía Nacional de Colombia, Dirección de Investigación Nacional e INTERPOL, Bogotá.

MINTIC, v. d. (2016). *Política Pública de Seguridad Digital en Colombia*. Recuperado el 3 de dic de 2017, de https://www.sites.oas.org/cyber/Documents/2016%20-%20Poli%CC%81tica%20Pu%CC%81blica%20de%20Seguridad%20Digital%20en%20Colombia-Juan%20David%20Duque,%20Viceministro%20TI%20(e)%20MinTIC.pdf

Colombiana, U. (8 de dic de 2016). *Colombia tiene Déficit de Ingenieros en TI*. Recuperado el 4 de dic de 2017, de Observatorio Universidad Colombiana: www.universidad.edu.co