La significativa evolución en seguridad de la información para la Policía Nacional de Colombia

The significant evolution in information security for the Colombian National Police

A evolução significativa na segurança da informação para a Polícia Nacional de Colômbia

Natalia Sánchez Molina *
Benly Gruchenska Pulido Ángel **
Jhon Henry Camacho Rodríguez ***

Policía Nacional de Colombia

Resumen

La lectura que los autores esbozan establece una contextualización cronológica sobre los procesos y alcances relacionados con la seguridad de la información en la Policía Nacional de Colombia, contextualizando al lector acerca de los estándares instaurados al interior de la institución y su impacto en la sociedad. Se mencionan las estrategias frente a la administración del talento humano de la institución como principal actor de riesgo en el tratamiento de la información; de igual manera se señalan las acciones normativas y estructurales para la formación de los policías y el control efectivo de la información.

Palabras Clave: Seguridad, información, Policía, Colombia, normatividad, cibercrimen.

Abstract

Reading the authors outline establishes a chronological contextualization of the processes and scope related to information security in the National Police of Colombia, contextualizing the reader about the standards in place within the institution and its impact on society. Strategies

Fecha de recepción del artículo: 6 de febrero de 2017
Fecha de aceptación del artículo: 8 de junio de 2017
DOI: http://dx.doi.org/10.22335/rlct.v9i1.267

* Artículo avance proyecto de investigación "Evolución en seguridad de la información para la Policía Nacional de Colombia"

** Policía Nacional de Colombia, Dirección de Talento Humano, Colombia. Email: alix.sanchez@correo.policia.gov.co Orcid. http://orcid.org/0000-0002-6467-1781

*** Policía Nacional de Colombia, Dirección de Inteligencia Policial, Colombia. Email: pulidobenly.macri@espolvirtual.com.co ORcid. orcid.org/0000-0002-1203-6911

**** Policía Nacional de Colombia, Escuela de Telemática y Electrónica, Colombia. Email: jhon.camacho6031@gmail.com Orcid: http://orcid.org/0000-0002-9882-0837

mentioned in the administration of human talent of the institution as a major player in the treatment of risk information; equally the policy and structural measures for police training and effective control of information listed.

Keywords: Security, information, Police, Colombia, regulations, cybercrime.

Resumo

A leitura do resumo dos autores estabelece uma contextualização cronológica dos processos e escopo relacionados à segurança da informação na Polícia Nacional da Colômbia, contextualizando o leitor sobre os padrões implementados dentro da instituição e seu impacto na sociedade. Estratégias mencionadas na administração do talento humano da instituição como principal participante no tratamento de informações de risco; Igualmente as medidas políticas e estruturais para treinamento policial e controle efetivo de informações listadas.

Palavras-chave: Segurança, informação, Polícia, Colômbia, regulamentos, cibercrime.

Introducción

La globalización de la información fundamentada en el internet, ha generado importantes beneficios para la humanidad (Cáceres, 2015) sin embargo los agentes criminales también se aprovechan de esta noble herramienta para afectar los intereses de las instituciones y de las personas que acceden a la WEB. Frente a estos desafíos, particularmente la Policía Nacional de Colombia ha evolucionado de manera efectiva para asegurar sus activos intangibles instaurando estrategias que incluyen el talento humano, la normatividad, y la infraestructura.

Desarrollo

Los importantes avances logrados por la Policía Nacional de Colombia en materia de seguridad de la información, se ven reflejados en la certificación otorgada por Instituto Colombiano de Normas Técnicas (ICONTEC) para el Sistema de Gestión de Seguridad de la Información (SGSI) en siete unidades policiales, acorde a la norma ISO/IEC 27001:2013; lo que ha permitido extender a todo nivel la implementación de políticas y controles a la información producida y utilizada por cada una de las actividades misionales desarrolladas por los funcionarios que laboran en las unidades de la Policía Nacional.

De esta manera, al interior de la institución se ha establecido la Resolución Nº 03049 del 24/08/2012 "Por la cual se adopta el Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional", con el propósito de establecer la política de seguridad de la información, así como los procedimientos y controles para el manejo de los activos de información y orientando sobre la gestión del riesgo frente a posibles amenazas que afecten a la Institución; de igual forma, se describe en el artículo 5 del acto administrativo en mención, la conceptualización de seguridad de la información como "la preservación de la Confidencialidad, Integridad y Disponibilidad de la información Institucional y propender por la autenticidad, trazabilidad, no repudio y fiabilidad de la misma", definición que se encuentra alineada al Modelo de seguridad y privacidad de la información emitido por el Ministerio de las Tecnologías de la Información y las Comunicaciones (MINTIC), y a la norma ISO/IEC 27001:2013.

Aun cuando se han realizado alineaciones con las políticas de estado que referencian la seguridad de la información, para la Policía Nacional de Colombia se ha convertido en una prioridad garantizar este tema y aún más propender por la protección de datos en el marco del desarrollo estratégico, táctico y operacional frente a la evolución de fenómenos delictivos que ven la oportunidad en las vulnerabilidades de los sistemas y redes de una organización para la sustracción de información; sin embargo, no solo es mantener segura la información de las actividades al servicio de la policía, sino garantizar la confidencialidad de la información de sus funcionarios, actividades administrativas y todo aquel dato o documento

que pueda comprometer la integralidad de la institución.

Referente a esto y a fin de garantizar la reducción de riesgos relacionados con el correcto manejo de la información el MINTIC, en su Modelo de seguridad y privacidad de la información menciona los tres (3) principios de la información que deben garantizarse y que la Policía Nacional de Colombia en la Resolución Nº 03049 del año 2012, define así: "1) Disponibilidad: Establece que la información debe estar disponible para su uso en todo momento, para ser usada o vista solo por personal autorizado; 2) Integridad: Consiste en salvaguardar la exactitud y estado completo de los activos de información, es decir que la información solo pueda ser modificada por personal autorizado; y 3) Confidencialidad: Establece que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados".

Con relación a este último principio, la confidencialidad de la información ha sido un foco de atención para las compañías, teniendo en cuenta el servicio o producto que se preste, en este sentido como lo menciona Cabarique, Salazar & Quintero (2015, pág. 68) es preciso establecer políticas de seguridad frente a la fuga de información, la cual se conoce como "el incidente que pone en poder de una persona ajena a la organización, información confidencial que solo debería estar disponible para integrantes de la misma", aún más cuando la fuga de información se presenta con datos sensibles, los cuales están definidos en el artículo 5 de la Ley estatutaria 1581 de 2012, de la siguiente manera: "se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos".

Teniendo en cuenta los últimos antecedentes acaecidos en las instituciones del Estado frente a servidores públicos que han divulgado información no autorizada poniendo en riesgo la estabilidad del Gobierno Nacional y de la institución, se puede evaluar el contexto del comportamiento ético de los empleados, quienes de acuerdo a Cabarique, Salazar & Quintero (2015, pág. 69) constituyen un factor interno de fuga de información sensible en las empresas.

Este tipo de comportamiento ético o no ético es referenciado por Palomo & Amaya (2011) donde se describen tanto factores organizacionales como individuales, entendiéndose factores organizacionales como el liderazgo de la alta dirección o superiores inmediatos, instrumentos de conocimiento organizacional como códigos de ética y todos aquellos rasgos que se perciban y que hacen parte de la cultura organizacional; y factores individuales como aspectos cognitivos y de personalidad que pueden propiciar la toma de decisiones de carácter ético frente a una situación en particular.

Sin embargo, la decisión de asumir comportamientos éticos o no éticos puede asociarse al nivel de compromiso que un empleado tenga con su organización, frente a este tema, Grueso (2010, pág. 84) retoma la teoría tridimensional del compromiso con la organización propuesta por Meyer y Allen en 1991, en la cual se describe el compromiso en tres escalas: 1) Afectivo: "como la vinculación emocional, la participación e identidad del empleado con la organización", 2) Continuo: como la valoración que hace el empleado de los costos asociadas con el abandono de la organización, y 3) Normativo: como el sentido de obligación moral de permanecer en la organización. Es así que el tipo de compromiso que el empleado genere con la organización, será acorde a su comportamiento y cumplimiento de los parámetros laborales establecidos por la misma.

Bajo estos conceptos, el vínculo empleado – organización, tiene más sentido si se entiende que un funcionario comprometido estará presto a cumplir con los protocolos de seguridad de la información ya establecidos y no presentará conductas no éticas generando fugas de información o manejos inadecuados de la misma, que puedan afectar la imagen o estabilidad de la organización. Este tipo de compromiso se hace más fuerte cuando se establecen parámetros claros por parte de la organización y se enriquece la cultura, para nuestro caso la Policía Nacional de Colombia, expide el Instructivo Nº 011 del 22/02/2016 "Parámetros para el correcto uso y administración de las redes sociales", teniendo en cuenta que estos medios tecnológicos son herramientas de fácil acceso para la fuga de información. Por lo cual, en ese instructivo se determinan lineamientos para generar un comportamiento colectivo idóneo, que se constituye en el soporte de la gestión del conocimiento que requiere toda institución para garantizar la protección de los principales activos de la información.

De igual forma, la Policía Nacional ha visto la necesidad de implementar diferentes métodos de supervisión y control a los funcionarios para garantizar que la información no sea divulgada con fines distintos a los del cumplimiento de su misión, garantizando que no se afecte la vigencia del régimen democrático, la seguridad o la defensa nacional. Cada lineamiento y parámetro de seguridad de la información que se genera preserva el derecho al uso de la información y garantía de los derechos humanos frente a la información personal de los funcionarios.

Tal como lo menciona Romero (2010), existen dos vertientes en el derecho al uso de la información "la pasiva, que alude al derecho a recibir información, y la activa, que indica al derecho a buscar e investigar la información que es de interés, accediendo directamente a las fuentes"; sin embargo, debe tenerse en cuenta que las restricciones al acceso a la información deben ser muy limitadas y sólo previstas por ley.

La implementación de políticas y directrices se realizan de forma física y/o mediante la utilización de herramientas tecnológicas, el sistema de acceso a la información tiene restricciones con capacidades de administración, monitoreo y control, con base en los cargos, perfiles y funciones determinadas en la estructura de cada unidad de la Policía Nacional, orientadas a la aplicación de controles y buenas prácticas de seguridad de la información en el contexto de las personas, procesos y tecnología.

La Institución continúa a la vanguardia del desarrollo tecnológico, con visión hacia la consolidación de la información en las unidades que integran la Policía Nacional, apoyado de una plataforma tecnológica robusta, susceptible de crecimiento y actualización, conforme a las necesidades propias de la institución: dinámica, proactiva, confiable y prospectiva, que se adapta a los cambios y permanece vigente como protagonista en el ámbito nacional e internacional.

Por consiguiente, la Policía Nacional de Colombia ha implementado programas académicos de posgrado para formar a sus integrantes en temas específicos, que apoyan el aseguramiento de la información e incrementa la efectividad policial frente a flagelos sensibles para la ciudadanía como delitos informáticos. Programas como la especialización en informática forense comprenden temas relevantes para el seguimiento, identificación y recolección de evidencias que permiten asegurar las condiciones de seguridad y convivencia en el ámbito del ciberespacio.

Así mismo la institución hace parte activa de la Comunidad de Policías de América – AMERIPOL, como una de sus estrategias para consolidar la seguridad de la información y la neutralización de la dinámica del cibercrimen, propendiendo por el control y tratamiento de la ciber-seguridad desde una perspectiva internacional, por cuanto la normatividad local de los estados resulta insuficiente para tratar este tipo de criminalidad. (Ballesteros & Hernández, 2014)

Conclusiones

La Policía Nacional de Colombia se ha convertido en la institución de vanguardia frente a la seguridad de la información, logrando impactar positivamente la sociedad, mediante el empleo de políticas, controles y actividades de formación y administración del talento humano.

Las organizaciones deben mantener estrategias continuas y dinámicas para minimizar el riesgo constante que se evidencia en los empleados frente a la seguridad de la información, vinculando métodos de formación, supervisión y control efectivos que impacten a sus integrantes.

Referencias bibliográficas

Ballesteros, M. C. R., & Hernández, J.,Antonio G. (2014). Cibercrimen: Particularidades en su investigación y enjuiciamiento/Cybercrime: Particularities in investigation and prosecution. Anuario Jurídico y Económico Escurialense, (47), 209-233. Retrieved from http://search.proquest.com/docview/1528550562?accountid=143348

Cabarique, W., Salazar, C. & Quintero, Y. (2015). Factores y causas de la fuga de información sensibles en el sector empresarial. Cuaderno Activa, 7, 67-73. Recuperado de http://ojs.tdea.edu.co/index.php/cuadernoactiva/article/view/263/253

Cáceres, M. B. A. (2015). Constitutional courts against "civil and political rights". A look from analytic theory of law. [Las Cortes Constituci onales frente a los «derechos ci vil es y polític os». Una mirada desde la teoría analític a del Derecho] *Revista Espanola De Derecho Constitucional,* 105, 105-136. doi:10.18042/cepc/redc.105.04

Congreso de la Republica de Colombia. (2012). Ley Estatutaria 1581 **"**Por la cual se dictan disposiciones generales para la protección de datos personales". Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Grueso, M. P. (2010). Implementación de buenas prácticas de promoción de personal y su relación con la cultura y el compromiso con la organización. Innovar, 20(36), 79-90. Recuperado de http://search.proquest.com/docview/1677604265?accountid=143348

Icontec Internacional. (2013). Norma Técnica Colombiana NTC-ISO-IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. Bogotá. Editada por el Instituto Colombiano de Normas Técnicas y Certificación.

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (2015). Modelo de Seguridad y Privacidad de la Información. Recuperado de http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_Seguridad.pdf

Palomino, P. R., & Amaya, C. R. (2011). Factores determinantes del comportamiento ético/no ético del empleado: una revisión de la literatura. Investigaciones Europeas de Dirección y Economía de la Empresa, 17(3), 29-45. Recuperado de http://search.proquest.com/docview/1323957164?accountid=143348

Policía Nacional de Colombia. (2012). Resolución N° 03049 el 24/08/2012 "Por la cual se adopta el Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional". Bogotá.

Policía Nacional de Colombia. (2016). Instructivo N°011 DIPON – COEST del 22/02/2016 "Parámetros para el correcto uso y administración de las redes sociales". Bogotá.

Romero, G. (2010). Implicaciones jurídicas del desarrollo del derecho de acceso a la información pública en el marco del derecho a la libertad de expresión y los derechos humanos. American University International Law Review, 26(1), 157-182. Recuperado de: http://search.proquest.com/docview/887907407?accountid=143348