ACTUALIDAD DE COLOMBIA EN SEGURIDAD DE LA INFORMACIÓN

González Hernández, Mauricio.
mauriciogonzalezh@yahoo.com
Universidad Piloto de Colombia

***Abstract*— The objective of seeking this article is to learn more about the current status which crosses Colombia in terms of information security, taking into account the past, present and future, also controls applied to decrease statistical incidents caused by cybercrime and commitment of the various government agencies working jointly attacking threats and vulnerabilities of systems towards keep information secure.**

***Resumen*— El objetivo que busca este artículo es dar a conocer más a fondo el estado actual por el cual atraviesa Colombia, en cuanto a seguridad de la información, teniendo en cuenta el pasado, el presente y el futuro, así mismo los controles aplicados para disminuir la taza de incidentes causados por el cibercrimen y el compromiso de las diferentes entidades del gobierno que trabajan mancomunadamente atacando las amenazas y vulnerabilidades de los sistemas en pro de mantener la información segura.**

Índice de Términos— Amenazas, Ataque, Ciberdelincuencia Ciberdelito, Ciberespacio, Ciberseguridad, Delito, Estadísticas, Ingeniería Social, Políticas, Seguridad Informática.

I. INTRODUCCIÓN

El elevado incremento de los dispositivos tecnológicos en las últimas décadas a nivel mundial presenta una de las grandes fuentes de vulnerabilidad y amenaza sobre los sistemas de las organizaciones, sin importar si son de índole privado o público. El uso de diferentes plataformas de información y gran variedad de hardware inquieta bastante para que el cibercrimen se encuentre atento y a la expectativa de intentar nuevos ataques y explotar las vulnerabilidades encontradas en determinado sistema o dispositivo.

Colombia se encuentra en el top 5 de los países latinoamericanos con mayor número de incidentes de seguridad tales como: fraude electrónico, extorción, robo de información, denegación de servicio, malware, virus entre otros. *Solamente en Brasil, los costos de los delitos cibernéticos alcanzaron los USD 8,000 millones, seguidos por México con USD 3,000 millones y Colombia, con USD 464 millones [1]*.

Para SOPHOS [2] el uso de dispositivos móviles como herramienta de trabajo en el entorno empresarial hace que el control y la protección de los datos sea cada vez más difícil, pues la gran diversidad de tecnología móvil y de computadores personales aumenta de forma acelerada, que los entes encargados de dicho control no son suficientes para tener registro de cada dispositivo, propietario e información que puedan almacenar.

Según InfoSecurity[3] cerca de 700 profesionales de los diferentes sectores de la empresa colombiana, incluyendo empresa privada, sector gobierno, PYMES y empresas grandes, respondieron una encuesta generada para medir el nivel de seguridad de la información en ésta área.

Observamos los resultados, que dejan claro que en los empresarios, no existe conciencia de los pros y los contras que hay en el acceso a mejores tecnologías de la información y las comunicaciones.

Algunos resultados:

- 81 % de las empresas nunca ha implementado una herramienta para gestión de riesgos.

- 53% ha instalado antivirus en todas las tecnologías de su empresa incluyendo las móviles.
- 40% NO revisa el marco normativo de seguridad de la información implementando en la empresa
- 52% no ha implementado en su empresa ningún estándar internacional de Infosec
- 47% nunca hizo ningún test de seguridad de las redes (Ethical Hacking, Análisis De Vulnerabilidades y/o Pruebas De Penetración en su empresa)
- 47% no cuenta con un Plan de Continuidad del Negocio que le permita seguir con las operaciones en caso de un evento no deseado.

Después de analizar las encuestas se llegó a la conclusión de que la empresa colombiana no distingue entre seguridad informática y seguridad de la información, inclusive conoce poco la legislación colombiana en materia de TICS: Todo esto no permite lograr una concientización en materia de seguridad de los actores que intervienen en la empresa colombiana, incluyendo clientes y proveedores.[3]

II. ACTUALIDAD EN COLOMBIA

Colombia es uno de los países suramericanos con mayor aceptación de la tecnología, observamos un porcentaje considerable de personas usando dispositivos móviles, computadoras personales, redes inalámbricas WiFi, redes sociales, correo electrónico, e-shopping, en fin una cantidad de servicios que a consecuencia de la tecnología están disponibles en el medio. Esta aceptación es favorable para el desarrollo tecnológico del país y de la misma economía, también para competir en el mercado mundial con las grandes potencias, pero veamos este avance tecnológico desde el punto de vista de la seguridad de la información y hagamos la pregunta: ¿con este avance nuestra información está segura?, ¿nuestros sistemas son confiables?, ¿tenemos privacidad en nuestras comunicaciones? En procura de responder estos interrogantes y otros más, el gobierno colombiano ha adoptado diferentes iniciativas para promover y dar cumplimiento a la Disponibilidad, la Confidencialidad y la Integridad, pilares de la seguridad de la información. Una de estas iniciativas está regida por el documento COMPES 3701 el cual define una política para la ciberseguridad y ciberdefensa.

El documento COMPES 3701 busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. Adicionalmente, recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema [4]. Si bien Colombia no es el país más fuerte en seguridad de la información, y basados en la definición anterior se observa un compromiso del gobierno nacional al incorporar estos mecanismos de acción, que ayudan a contrarrestar los continuos ataques de la ciberdelincuencia.

El robo de información, la estafa electrónica, la suplantación de identidad, la denegación de servicios, la extorción entre otros, es el diario vivir de la delincuencia cibernética, todos los días se presentan incidentes de esta índole los cuales generan pérdidas económicas millonarias, daños a la imagen corporativa de las empresas y hasta daños morales a causa del acoso cibernético. Estos delitos y consecuencias son cometidos por los delincuentes, aprovechándose de la confianza que las personas tenemos en el momento de usar cualquier medio y/o herramienta tecnológica. Somos muy confiados cuando usamos redes sociales, dejamos a vista pública información sensible y relevante, descubrimos nuestra intimidad al publicar fotos, ubicaciones y estados, no tenemos precaución con nuestras transacciones y pagos, los realizamos desde

cualquier computador en fin suministramos el insumo más importante para un atacante que es la información confidencial. Es así como la falta de capacitación y conciencia de la ciudadanía contribuye a que esta tarea sea más fácil para los delincuentes. *Como referencia, en el 2013 hubo 2 millones y medio de casos de robo de datos en dispositivos móviles, de acuerdo con cifras de la Unidad de Delitos Informáticos de la Policía Nacional de Colombia* [1].

La Policía Nacional por su parte en su compromiso con la seguridad de la información de la ciudadanía está dotada de un área especializada, conocida como la oficina de delitos informáticos que se encarga de la prevención, control e investigación de ciberdelitos [4]. Entidades como estas corroboran la importancia que está tomando el tema y brindan un parte mínimo de tranquilidad para un buen comienzo del aseguramiento de la información tanto de las empresas como de las persona.

Cabe anotar que a pesar del incansable trabajo que realizan los entes responsables de la seguridad informática y de los delitos cibernéticos, Colombia cuenta con debilidades importantes, que al ser atacadas por los ciberdelincuentes, pueden desestabilizar alguna organización del estado o en general la seguridad nacional.

III. COMBATIENDO LA CIBERDELINCUENCIA

El estado colombiano al presentar grandes debilidades en seguridad informática, toma medidas para mitigar y contrarrestar el riesgo que se está corriendo en la actualidad, es por eso, que realiza un trabajo constante e incansable, adoptando políticas, creando entes especializados y generando reglamentaciones que contribuyan a minimizar los riesgos y posicionarse en un nivel fuerte o al menos aceptable de seguridad de la Información.

Delitos informáticos de la Policía Nacional, asegura que los incidentes que se presentan con mayor frecuencia en el ciberespacio colombiano son: estafas a través de subastas en línea, pornografía infantil en internet, violación de los derechos de autor, divulgación indebida de contenidos, piratería en internet entre otros [5]. Para este fenómeno se toman medidas, inicialmente de prevención y concientización al ciudadano, dando a conocer la importancia que puede tener la información privada o corporativa que manejan las personas y mostrando el uso que pueden dar de esta cuando cae en manos de la ciberdelincuencia.

En el proceso de combatir la delincuencia en el ciberespacio, Colombia crea el centro de información y respuesta técnica a incidentes de seguridad informática – CIRTISI con el cual busca servir de soporte a diferentes entidades del gobierno en: prevención, detección, manejo y recuperación en cuanto a amenazas de seguridad de la información [6]. Esto genera confianza al gobierno nacional pues el proyecto abarca la creación de laboratorios para la investigación, la estandarización de procesos basándose en reglamentación internacional, la generación de redes de apoyo, la interacción con otros gobiernos, entre otros objetivos del CIRTISI.

El gobierno colombiano dentro de sus medidas de choque para combatir la ciberdelincuencia recientemente invito una delegación internacional de expertos para realizar un estudio minucioso de la ciberseguridad en el país. Dicho estudio fue dirigido a revisar políticas de ciberseguridad, gestión y respuesta a incidentes, marcos normativos, cooperación internacional y la investigación de los delitos de cibernéticos y ciberdefensa.

Pero no solo el gobierno muestra preocupación por la seguridad de la información, la empresa privada también marca tendencia en adoptar medidas de mitigación de los riesgos que conlleven a exponer su información confidencia o de negocio, cada vez son más las empresas que tienen un Sistema de Gestión

de Seguridad de la Información – SGSI y adicional una certificación ISO 27001.

IV. FUTURO DE COLOMBIA EN SEGURIDAD INFORMÁTICA

El futuro del gobierno colombiano, en el campo de la Seguridad de la Informaciones es favorable en comparación con la evolución tecnológica que se desarrolla en el país, teniendo en cuenta el crecimiento acelerado de los diferentes dispositivos móviles, personales, plataformas de comunicaciones entre otros es de resaltar la gestión que se realiza por parte del estado incorporando mecanismos para estar a la expectativa de cualquier amenaza que pretenda desestabilizar alguna organización o algún sistema.

La academia juega un papel muy importante, pues en los últimos años se ha incrementado la oferta de programas especializados en seguridad informática en los diferentes niveles de educación: técnico, profesional, especialista, master etc. Este incremento augura un buen futuro para el territorio colombiano pues cada vez más tendremos personal capacitado y experto en la lucha de proteger el activo más preciado de las organizaciones y de las personas, la información.

Por su parte la Policía Nacional de la mano del ministerio de las TICs y las entidades financieras, adelantan programas de concientización y sensibilización ciudadana para crear cultura de seguridad desde los mismos hogares y desde la infancia y adolescencia, todo esto soportado en conferencias, charlas, informes, estadísticas y publicidad de la importancia de la seguridad de la información.

Para dar cumplimiento y que las iniciativas en torno sean exitosas, el estado colombiano incorpora una serie de normativas, legislaciones y decretos para fortalecer las posibles vulnerabilidades que tienen sus entidades y a la vez castigar o penalizar los posibles ciberdelincuentes que intentan lanzar algún ataque perjudicando el buen funcionamiento de los sistema. A continuación se mencionan algunas leyes y decretos que está utilizando el estado en temas de Seguridad de la información:

- Ley 527 de 1999 – COMERCIO ELECTRÓNICO
- Ley 599 DE 2000
- Ley 962 de 2005
- Ley 1150 de 2007
- Ley 1273 de 2009
- Ley 1341 de 2009
- Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009
- Circular 052 de 2007 (Superintendencia Financiera de Colombia)

Entre otras, con esta normatividad los entes encargados de la seguridad de la información del país y las empresas en general afrontan la ciberseguridad y la ciberdefensa. Pues al ver en detalle se encuentra legislación para los diferentes crímenes realizados en los sectores financieros, bancarios, de comercio electrónico, sistemas de información, tecnologías de información y comunicación.

V. CONCLUSIONES

Después de conocer la realidad actual por la que atraviesa el estado colombiano, el panorama no es del todo devastador, encontramos que el gobierno presenta debilidades informáticas y cibernéticas, pero también se observa que se están creando y existen bastantes mecanismos para contrarrestar este tipo de debilidades, además que se trabaja constantemente en el desarrollo de nuevas prácticas para fortalecer la seguridad de la información.

La confianza de las personas es una de las causas más importantes para que un ciberdelincuente aproveche y vulnere cualquier sistema, no protegemos nuestras contraseñas, las compartimos,

no cerramos sesiones en los equipos, publicamos información confidencial, descuidamos nuestros dispositivos móviles, en fin tenemos el pensamiento que no cumplimos con el perfil que le puede interesar a un atacante.

Conociendo que una de las causas por las que la ciberdelincuencia vulnera tantos sistemas y organizaciones es el aumento acelerados de equipos tecnológicos (dispositivos móviles, computadores personales, tabletas etc.) lo importante es realizar prevención para que las vulnerabilidades sean minimizadas, esto se logra a través de campañas de sensibilización y capacitación a todos los usuarios de las entidades gubernamentales y porque no del área privada.

RECOMENDACIONES

Realizar prevención y capacitación a todos los usuarios que de una u otra manera tengan acceso a información sensible, que en dado caso de robo pueda generar trastornos en una organización.

Crear conciencia y cultura de seguridad en todos los campos en los que nos movemos ya sea en la casa, en la oficina, en sitios públicos, etc, para de esta manera minimizar los riesgos de fuga o robo de información y evitar costos innecesarios que generan los incidentes de seguridad.

Conocer y aplicar las políticas de Seguridad de la Información que rigen las organizaciones para las cuales laboramos y colaborar con la mejora continua de los procesos.

Evitar el uso de dispositivos de almacenamiento en sitios no seguros protegiendo de esta forma la información que nos pertenece.

REFERENCIAS

[1] Symantec Corporation, Reporte Norton 2013 (Colombia). Disponible en: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

[2] (2013) Web site SHOPOS. [Online]. Available: http://www.sophos.com/en-us/security-news-trends.aspx

[3] Web site INSEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA COLOMBIANA [Online]. Available:http://www.infosecurityvip.com/newsletter/estadisticas_ago11.html

[4] *Documento COMPES*, 3701, 14 de Julio de 2011.

[5] Web site OFICINA DE DELITOS INFORMÁTICOS DE LA POLICÍA NACIONAL [Online]. Available: http://www.policia.gov.co/portal/page/portal/UNIDADES_POLICIALES/Direcciones_tipo_Operativas/Direccion_Seguridad_Ciudadana/Planes_de_Seguridad/Recomendaciones_de_seguridad/delitos_informaticos

[6] Web site CENTRO DE INFORMACIÓN Y RESPUESTA TÉCNICA A INCIDENTES DE SEGURIDAD INFORMÁTICA – CIRTISI [Online]. Available: http://programa.gobiernoenlinea.gov.co/apcaafiles/5854534aee4eee4102f0bd5ca294791f/CIRTISI_COLOMBIA_aprobado_24_de_mayo_de_2007_2.pdf

[7] Web site UNIVERSIDAD INDUSTRIAL DE SANTANDER [Online]. Available: http://revistas.uis.edu.co/index.php/revistagti/article/view/1259

[8] Web site CAMPUS-PARTY INNOVACION SEGURIDAD Y REDES [Online]. Available: http://www.campus-party.com.co/2012/seguridad-y-redes.html

[9] Web site EL TIEMPO [Online]. Available: http://www.eltiempo.com/tecnologia/actualidad/ARTICULO-WEBNEW_NOTA_INTERIOR-12493603.html

[10] *Information Security Management System*, ISO/IEC 27001, 2013

[11] D. Kosutic, *9 Steps to Cybersecurity*, EPPS Services Ltd, 2012.

Autor
Mauricio González Hernández
Ingeniero de Sistemas
Auditor Interno –SGSI ISO/IEC 27001:13
Especialista en Seguridad Informática (En curso)