Ciberseguridad de Gobierno

Lopez Mendez Edwin Javier
Edwinlopera76@gmail.com.
Universidad Piloto de Colombia

Resumen—. En el mundo actual las TIC se han convertido en un activo fundamental en las organizaciones que ven en las mismas el crecimiento y éxito no solo económico y empresarial, sino además se han convertido en un soporte indispensable de todas las áreas de la organización. Las diferentes herramientas han convertido a las TIC como un elemento principal para resguardar toda la información estableciendo una serie de pasos o procesos que permitan controlar el uso adecuado de la misma y brindando seguridad.

Con el paso de los años las organizaciones tanto públicas como privadas en el mundo están realizando una serie de esfuerzos en razón a minimizar el riesgo frente a las amenazas informáticas, la creación de grupos especializados y estrategias entre mecanismos e instrumentos que los gobiernos vienen adelantando para facilitar y coordinar el intercambio de información entre los diferentes organismos estatales, y en este mismo sentido sobre ciberamenazas y ciberincidentes entre los sectores públicos y privados, sin que el intercambio de información a través de medios electrónicos represente un grave riesgo, contrario a ello generando protocolos que permiten de alguna manera tener confianza entre ellos a la hora del intercambio de información.

Abstract—. In the current world the TIC they have turned into a fundamental assets into the organizations that see in the same ones the growth and not alone economic and managerial success, but in addition they have turned into one I support indispensably all the areas of the organization. The different tools have turned the TIC as a principal element to protect all the information establishing a series of steps or processes that allow to control the suitable use of the same one and offering safety.

As the years went by the organizations both public and deprived worldwide realize a series of efforts in a reason to minimize the risk opposite to the IT threats, the creation of specialized groups and strategies between mechanisms and instruments that the governments come improving to facilitate and to coordinate the exchange of information between the different state organisms, and in the same sense on cyberthreats and cyberincidents between the public and private sectors, without the exchange of information across electronic means represents a serious risk, I contradict to it generating protocols that allow to have somehow confidence between them at the moment of the exchange of information.

Índice de términos — CCOC, CCP, ciberataque, ColCERT, Conpes, hacker.

I. INTRODUCCIÓN.

En la actualidad las Organizaciones han incrementado el manejo de la información digital para todas sus actividades del negocio que recae en el uso desmedido de computadoras e internet; el envío y recepción por medio de correo electrónico es uno de los principales medios de intercambio de información que facilitan y agilizan su proceso. En cuanto a las organizaciones de trasporte, su principal medio son los sistemas de navegación aéreos; adicionalmente el entretenimiento con aplicaciones mantiene a las personas dependientes de este tipo de tecnología; por esa razón se hace necesario tener claro qué información estamos almacenando en los dispositivos móviles o en la computadora personal. Teniendo en cuenta que se han realizado estudios como el elaborado en el 2011 por Cisco[1]IBSG donde se calculó que para el 2020 habrá más de cincuenta mil millones de dispositivos

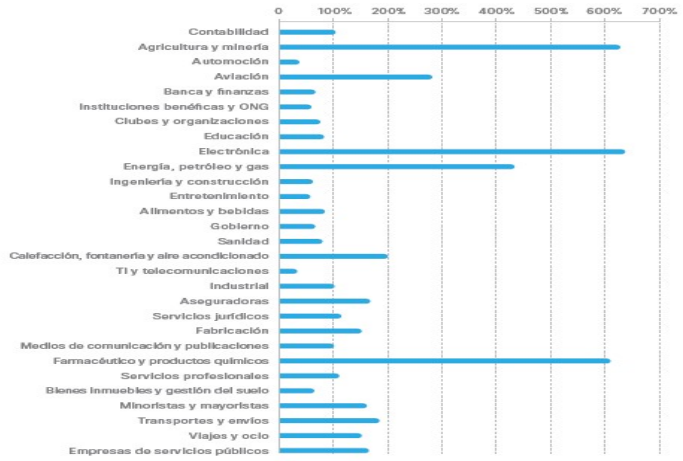
[1] Internet de las cosas - Cisco
http://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRT-CV%5D%20Informe-Internet_de_las_Cosas.pdf

conectados por internet, es decir, un promedio de 6.58 dispositivo por persona, esto nos lleva a concluir que la información se encuentra cada día más expuesta a posibles vulneraciones en la red. Otro informe realizado en Julio de 2014 por HP Fortify[2]reveló que estos dispositivos tienen un 80 % de fallas y con un mal uso, 6 de cada 10 cuentan con una interfaz vulnerable.

La ciberseguridad implica la protección de la información, previniendo, detectando y respondiendo a los ataques que a diario se presentan; debido a esto es que el aseguramiento de la información se ha convertido en un papel fundamental tanto para las organizaciones como para las personas a lo cual se detecta con más preocupación su activo más valioso. "La información" en donde se encuentra amenazada por agentes internos y externos que con el tiempo se han vuelto más expertos e inteligentes al momento de realizar un ciberataque, tomando el tiempo necesario para conseguirlo.

El propósito de la seguridad en todos sus ámbitos es reducir riesgos hasta un nivel que sea aceptable para los interesados en mitigar amenazas latentes. En este orden de ideas el enfoque al cual se ha llevado la ciberseguridad en los gobiernos es la creación de políticas tendientes a evolucionar junto con el creciente auge que tienen las organizaciones en las cuales se debe implementar modelos de programas para la seguridad informática que apoyen los objetivos de negocio y así poder dar cumplimiento a la misión y visión de la misma.

Gráfica 1 Riesgos de los sectores y encuentros con malware web (2013).



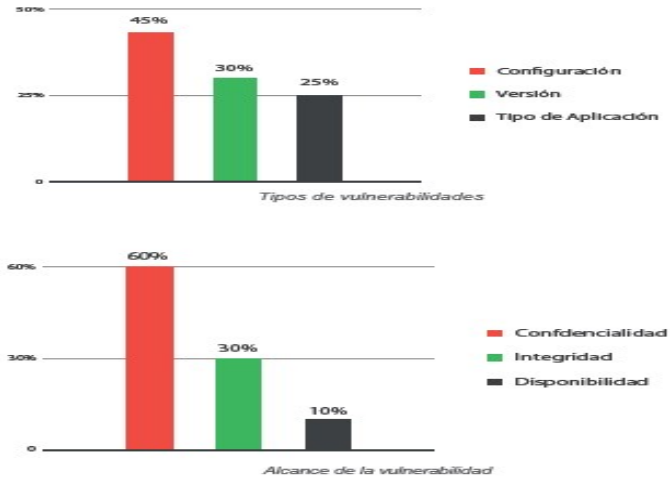
Informe anual de seguridad de Cisco 2014.[3]

II. CIBERSEGURIDAD EN EL MUNDO.

Para hablar de seguridad se hace necesario encontrar la diferencia entre ciberseguridad y seguridad en la información. Según Isaca define a la ciberseguridad como "Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados". Llamamos activos a todo dato que tiene algún tipo de valor para las organizaciones, estos datos se pueden presentar en varias formas como son electrónicas, físicas, virtuales. Por eso cuando hablamos de ciberseguridad no hablamos de toda la información, solo estamos hablando de los archivos digitales y todo lo que esto implica.

En un reciente estudio realizado por Trend Nicro Organización de los Estados Americanos presentó un informe de las principales vulnerabilidades en América y que están vinculados a la Organización de los Estados Americanos OEA, presentando un alto porcentaje en infraestructura, aplicaciones que por presentar falencias en las configuraciones se ven expuestas a los ataques, otra de las mayores vulnerabilidades es la utilización de versiones obsoletas o la instalación de aplicaciones inapropiadas, sin embargo, esos problemas se asocian con un nivel de riesgo más alto.

Gráfica 2. Vulnerabilidades.



Reporte de seguridad cibernética e infraestructura crítica de las Américas.[4]

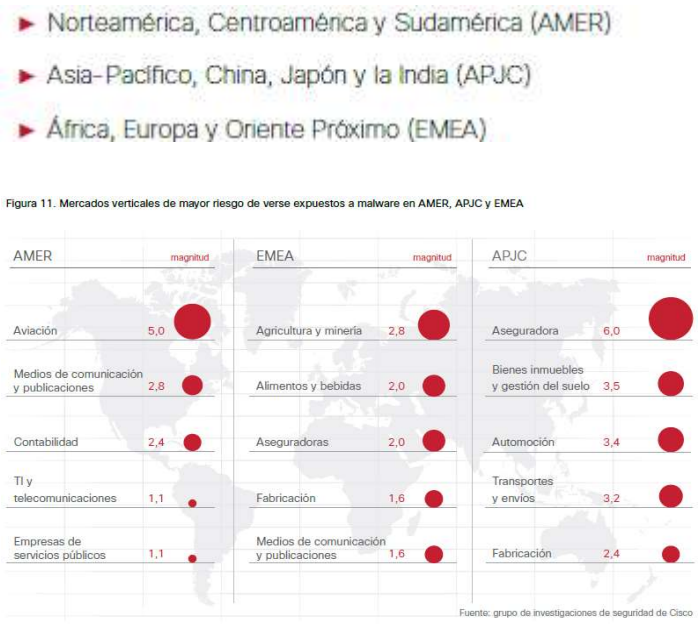
[2]http://www.csirtcv.gva.es/sites/all/files/downloads/%5BCSIRT-CV%5D%20Informe-Internet_de_las_Cosas.pdf

[3] http://www.cisco.com/ Informe anual de seguridad de Cisco 2014.

[4]https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf

Como se puede observar este tipo de problemas no solo afecta a las aplicaciones o infraestructura, estos ataques van dirigidos a uno de los tres pilares de la seguridad en la información (Disponibilidad, Confidencialidad, Integridad) siendo la más crítica la confidencialidad.
Una de las modalidades más frecuentes que se presenta son los spam y malware, estos métodos son utilizados para el robo de información confidencial que sigue siendo el principal método para vulnerar información utilizando diferentes medios como el correo electrónico para propagar amenazas. También las redes sociales siguen siendo el medio perfecto para esta categoría de cibercriminal.
Por otra parte, si hablamos de las entidades financieras su modalidad como el spam para ocultarse, el phishing, el malware y el robo de datos son los más utilizados.
Ahora bien, no podemos dejar a un lado los espionajes entre gobiernos, como se ha observado en los últimos años.
La falta de regulación por parte de las Entidades Estatales (Gobiernos), encargadas de elaborar las políticas públicas sobre este aspecto, impulsa a los ciberdelincuentes a trasmitir virus a través de una serie de países utilizando sus servidores para realizar la trasferencia de datos por canales que no cuentan con una buena seguridad del remitente al destinatario. Todos estos actos se realizan desde países en los que la legislación es muy laxa, lo que permite por no contar con la cooperación internacional para mitigar este riesgo. Incluso en los países con acuerdos, los procesos de intercambio de información suelen ser formales y requerir mucho tiempo, por eso hasta que no exista una política efectiva y marcos internacionales capaces de investigar, enjuiciar y castigar los ciberdelitos, este tipo de flagelos no disminuirá, por esa razón países como Estado Unidos ya está promoviendo un proyecto de ley CISPA el cual les da herramientas a las autoridades para realizar la judicialización y poner en cintura a estos delincuentes.
En la actualidad la ciberseguridad es un tema amplio y complejo que afecta en gran medida a las empresas, gobiernos y organizaciones que han invertido muy poco en proyectos de seguridad poniendo en riesgo su negocio realizando transacciones u otro tipo de actividades en la red abriendo puertas a estos delincuentes.

Gráfica 3 Mercados de mayor riesgo de verse expuestos a malware en AMER, APJC y EMEA.



Informe anual de seguridad de Cisco 2014[5].

Como podemos observar un reporte generado por el grupo de seguridad de Cisco (gráfica 3) nos muestra los mercados de mayor riesgo en ciberataques en el mundo. Esto nos lleva a que tenemos que crear conciencia en las organizaciones y las instituciones de gobierno, esta se debe realizar a cada uno de personas. Hoy podríamos hacer la pregunta en cada una de ellas y decirles si saben ¿Qué es ciberseguridad?
Se puede asegurar que un gran porcentaje de las personas no tendrá la más remota idea de su significado y lo que este término puede significar en el momento de algún tipo de ataque a sus sistemas o las posibles vulnerabilidades que puedan presentar algún tipo de pérdida o robo de información, todo esto por la mala manipulación en sus aplicaciones entre otros, teniendo en cuenta estas consideraciones, los delincuentes que pueden ser individuos u organizaciones, permanecen atentos a todo tipo de vulnerabilidades que en ocasiones les toma a estas personas todo el tiempo que necesiten para poder realizar un ataque.
La seguridad en las empresas de América Latina son muy distintas a las de Estados Unidos o Europa con relación a la seguridad, siempre los norte americanos o europeos están invirtiendo en seguridad, la razón más importante es que son los continentes con mayor índice de ataques por cracker de diferentes países.

[5] http://www.cisco.com/ Informe anual de seguridad de Cisco 2014

Se han realizado estudios en las principales multinacionales americanas, donde ya han podido establecer que estos ataques pueden durar más o menos 170 días promedio en detectarlo y 45 días en resolverlo.
Durante los últimos años, hemos sido testigos de la ocupación que el internet ha tenido en cada uno de nuestros dispositivos esto es llamado (Internet of things – Internet de las cosas).
Podemos listar algunas tendencias de ciberseguridad para el 2015, de acuerdo con ICbeat es una publicación digital independiente especializada en tecnología e innovación.

- ✓ Crecimiento de las tácticas de guerra cibernética y el ciberespionaje.
- ✓ Más ataques y más fuertes al Internet de las Cosas.
- ✓ El 'ransomware' salta a la nube.
- ✓ Más ataques a móviles.
- ✓ Explotación de los fallos de software.
- ✓ Nuevas técnicas de evasión del sandboxing.

Estas tendencias se están presentando debido al crecimiento de los ciberataques que pondrán en graves problemas a las grandes organizaciones principalmente a los dispositivos móviles.
Ahora bien las organizaciones de América Latina nunca muestran las falencias o principales vulnerabilidades a sus sistemas, siempre son reportadas solo cuando ya han sido atacadas, todas ellas siempre están siendo reactivas, hasta este momento se comienza a generar cultura con la nueva normatividad en la que se encuentra ISO 27000 y su familia, Cobit 5 entre otras.
Si sabemos que estas organizaciones no cuentan con el personal idóneo para detectar o minimizar el riesgo de ciberataques y tampoco cuenta con un debido soporte de compañías especializadas que lo hagan, por eso es por lo que la primera entrada de ataques empieza por las personas que no cuentan con una debida capacitación o formación en los riesgos y el impacto de los actos que realice.
Según encuesta realizada por Trend Micro Incorporated en este año a diferentes organizaciones en América han tenido algún tipo de ataque, este de diferentes formas y dirigidos a un objetivo específico, es así que ahora los delincuentes no se dedican a enviar ataques a diferentes organizaciones en busca de algún usuario que le dé la oportunidad de ingresas a sus sistemas, por lo contrario ahora se dedican a objetivo específico sin importar el tiempo que puedan gastar, estos ataques pueden ser también de diferentes maneras para lograr ese objetivo.
La mayoría de las regiones en América en las que se aplicó la encuesta indicaron que su equipo ICS/SCADA estaba siendo atacado, lo que revela una gran cantidad de amenazas, en la (gráfica 4) podemos identificar los gobiernos que se sienten listos a un ciberataque.

Gráfica 4. Percepción de la Preparación para los Incidentes Cibernéticos.

Reporte de seguridad cibernética e infraestructura crítica de las Américas.[6]

Como lo vemos la gran mayoría no está preparada para este tipo de ataques y esto se debe a la falta de concientización por parte de las organizaciones al no enfrentar las deficiencias en sus infraestructuras, esto no lleva a trabajar de forma mancomunada en las organizaciones por adoptar estándares y crear regulaciones que nos permita utilizarla para hacer frente a estos delincuentes. Esto no lo podríamos hacer sin la ayuda de los gobiernos apoyando a las organizaciones tanto públicas como privadas lo cual significaría un avance para realizar acuerdos que inicien procesos de normalizar y reglamentar estos tipos de nuevos delitos que se vienen presentando en todo el mundo.

[6]http://www.cisco.com/assets/global/ES/pdfs/executive_security/sc-01casr2014_cte_lig_es_35330.pdf

III. CIBERSEGURIDAD EN EL COLOMBIA.

A diferencia de otros países en Colombia, se cuenta con la ley 1273 de 2009 la cual creo nuevas sanciones penales y a su vez elevo a rango de derecho fundamental la información privada que se almacena tanto en dispositivos como en computadoras; así mismo ya se viene trabajando en iniciativas en materia de seguridad y delitos cibernéticos **CONPES** 3701 de 2001 "Este documento 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.".
Esta política nacional que se ha utilizado durante varios años y que en el 2014 se basó para realizar una nueva estructura de gobierno en donde participan entidades estatales y privadas, allí se plasmó el plan nacional de ciberseguridad y ciberdefensa definiendo, principios rectores, roles y responsabilidades, así mismo se debía fortalecer a las oficinas de seguridad, acordar convenios internacionales y articular al empresariado, la academia y la ciudadanía en torno a una política pública. Para lograrlo se hizo necesario la creación de grupos como:

- ✓ Centro Cibernético Policial (CCP) especializado dentro de la policía nacional de Colombia, bajo la Dirección de Investigación Criminal e Interpol (Dijín). es la principal unidad designada en Colombia para investigar delitos cibernéticos en todo el país.
- ✓ Grupo de respuesta a emergencias cibernéticas (ColCERT), organismo nacional a cargo de la respuesta a incidentes cibernéticos.
- ✓ El Comando Cibernético Conjunto (CCOC).

Es importante tener en cuenta que estos grupos no pueden lograr una buena acción frente a delitos como (hackers, infecciones con virus, ataques, etc.) tanto a nivel público como privado se creó nuevo esquema de reporte y monitoreo obligatorio de incidentes de seguridad informática, esto nos obliga a todas los organismos y entidades como a la ciudadanía en general reportar este tipo de ataques que se nos presenten teniendo en cuenta que a todas y cada uno de nosotros se nos debe realizar una buena capacitación frente al tema.

Gráfica 5 Modelo de Coordinación.

Ministerio de Defensa Nacional.[7]

El Gobierno colombiano invitó a una comisión internacional de expertos de diferentes países y organizaciones especializadas en ciberseguridad para que se realizara un análisis profundo en cuanto a la seguridad cibernética, las principales recomendaciones de los expertos fueron:

- ✓ Fortalecimiento de las capacidades institucionales de ciberseguridad y ciberdefensa.
- ✓ Política para la protección de infraestructura crítica.
- ✓ Crear un órgano de coordinación permanente.
- ✓ Establecimiento y mejora de los marcos legales en ciberseguridad.
- ✓ Generación de capacidades de ciberdefensa.
- ✓ Capacidad analítica y técnica - tendencias de la amenaza.
- ✓ Academia de cibernética profesional.
- ✓ Establecer centros de innovación /excelencia.
- ✓ Cooperación internacional y cooperación entre múltiples partes interesadas.
- ✓ Estrategia para la cooperación internacional.
- ✓ Ampliar el papel del ministerio de relaciones exteriores.

[7] http://es.slideshare.net/Derechotics/3701

- ✓ Coordinador de política cibernética internacional.
- ✓ Invertir en un plan de capacitación internacional.

Las autoridades colombianas identificaron tres tendencias específicas del delito cibernético.

- ✓ Phishing (suplantación de identidad).
- ✓ La denegación de servicio (DoS).
- ✓ La delincuencia a redes sociales en general.

La comisión la unión internacional de telecomunicaciones (UIT) publica el índice mundial de ciberseguridad (IMC) que evalúa el grado de desarrollo de la ciberseguridad en cada país, del más reciente estudio, realizado durante 2014, participaron 104 países del mundo. En los que Colombia ocupó el quinto lugar en América entre los mejores del mundo en manejo de ciberseguridad y a nivel mundial ocupó el noveno lugar compartiendo con Francia una de las potencias.

Los aspectos que se tuvieron en cuenta para la evaluación fueron:

- ✓ Medidas legales.
- ✓ Técnicas.
- ✓ Organizacional.
- ✓ Generación de capacidades y cooperación.

Cada tema daba una puntuación y ubicaba a los países en el ranking.
Según Jorge Bejarano, director de estándares y arquitectura de TI de Min TIC, "…la participación y los excelentes resultados de Colombia en el estudio confirman que las estrategias para proteger a los colombianos en el ciberespacio están dando resultado y que ante posibles incidentes de robo de información, suplantación de identidad, ataques cibernéticos, entre otros, el país podría tiene un nivel de preparación para responder a la altura de países como Francia y España. nuestro país obtuvo muy buenas calificaciones en aspectos como el legal, que se refiere a las regulaciones que se tienen para prevención y promoción de la seguridad en los sistemas, protección de datos personales y judicialización de delitos informáticos; el organizacional…".

IV. CONCLUSIONES.

El tema de ciberseguridad y sus características son objetivas que las empresas estatales como privadas debe promover como una cultura en todos los niveles desde la persona de la recepción hasta la alta gerencia teniendo en cuenta que hay estadísticas en donde la primera fuente a que los atacantes buscan como objetivos son las asistentes de la alta gerencia, es un deber de todos conocer los riesgos y métodos que utilizan los delincuentes para atacar y conseguir el objetivo. Esto solo se puede lograr diseñando y ejecutando planes de capacitación especializada en ciberseguridad y ciberdefensa en todas o cada una de las áreas en las organizaciones, realizando concientización por medio de mensajes que pueden ir desde volantes hasta juegos interactivos o encuestas que las personas podrían realizar.

Otra de las estrategias debería ser la colaboración Internacional y nacional entre los sectores público y privado desempeña un papel vital para el fortalecimiento de los marcos de ciberseguridad nacionales, teniendo en cuenta que la gran mayoría ya está realizando planes de ciberseguridad y ciberdefensa, que al poder unificar se tendría un buen intercambio de información a nivel mundial.

Al lograr fortalecer el cuerpo normativo y de cumplimiento en la materia con miras a desarrollar las herramientas jurídicas necesarias para una efectiva y eficiente prevención, investigación y judicialización de los delitos cibernéticos.

Cualquier momento judicializar la persona u organización limitándolo a que cumpla con una sola regla.
Se identifica que la ciberdefensa es una realidad emergente que deben considerar las naciones como un elemento estratégico de gobernabilidad en el siglo XXI.

BIBLIOGRAFÍA.

Fuentes académicas.

[1] Dejan Kosutic (2014). Ciberseguridad en 9 pasos.

Fuentes institucionales.

[2] Documento Conpes 3701, lineamientos de política para ciberseguridad y ciberdefensa (2011).

[3] Comisión de regulación de comunicaciones diciembre (2014).

Fuentes electrónicas.

[4] [www.sites.oas.org/cyber/Certs_Web/OEA-Trend] Micro] (2015) en línea consultado el 10, 08-15.

[5] ww.symantec.com/es/mx/page.jsp?id=cybersecurity-trends] (junio 2014) en línea consultado el 10, 08-15.

[6] [www.cisco.com/web/ES/offers/lp/2015-annual-security-report/index.html] (2015) en línea consultado el 10, 08-15.

[7] [www.mintic.gov.co/portal/604/articles-6120_recurso_2.pdfwww.cisco.com/web/ES/offers/lp/2015-annual-security-report/index.html] (marzo 2014) en línea consultado el 10, 08-15.

[8] ww.cisco.com/web/ES/ciberseguridad/index.html] (octubre 2014) en línea consultado el 10, 08-15.