GESTIÓN DE RIESGOS PARA LA SEGURIDAD DIGITAL EN COLOMBIA

Cubillos Ramos Johan Anderson
jcubillos79@gmail.com
Universidad Piloto de Colombia

***Abstract*—**This article is an analysis of the current situation in risk management for digital security at the national level and in the business sector, due to the increase in threats and incidents in the digital environment; a correct self-assessment will display the status of our policies and strategies anti-cybercriminal mechanism to minimize risks in Colombia.

***Resumen*—**Este artículo es un análisis de la situación actual en gestión de riesgos para la seguridad digital a nivel nacional y en el sector empresarial, debido al crecimiento de las amenazas e incidentes en el entorno digital, una correcta autoevaluación permitirá visualizar el estado actual de políticas y estrategias anti cibercriminal, mecanismo para minimizar los riesgos en Colombia.

***Índice de Términos*—** Compute security incident response (CSIRT), Forum of incident response and security teams (FIRST), cibercrimen, ciberterrorismo, gestión de riesgos, entorno digital, infraestructura crítica cibernética

I. INTRODUCCIÓN

Gestión de riesgos para la seguridad digital es un amplio enfoque que los Gobiernos de varios países han adoptado como una política nacional de seguridad digital, en un mundo globalizado, la tendencia cada vez, más fuerte hacia las tecnologías de comunicación y el incremento en la oferta de servicios disponibles en línea, incluye al ciudadano hacia una participación directa, donde la necesidad de garantizar los derechos fundamentales consagrados en la constitución política de Colombia pasa a ser un compromiso de obligatorio cumplimiento , ahora en otro escenario bastante conocido y poco protegido , el ciberespacio. Una responsabilidad de seguridad para el ciudadano no solo debe tener una fuerza disponible en las calles como es la policía, adicionalmente la conformación de grupos especializados de respuesta a incidentes en seguridad digital como los CSIRT, están dentro de las recomendaciones de países con un nivel alto de madurez en temas de ciberseguridad. La batalla ahora pasó a un entorno distinto, un lugar virtual pero real con diferentes tipos de peligros y amenazas sobre las cuales la mayoría de personas no están socializados o desconocen por su falta de capacidad técnica e investigativa. El Gobierno nacional consciente de los nuevos tipos de riesgos y amenazas en el entorno digital, genera una estrategia de defensa y prevención con la colaboración internacional de diferentes organismos e instituciones como la OEA (Organización de los Estados Americanos) que tiene como propósito principal promover y desarrollar la cooperación entre los estados miembros para prevenir, combatir y eliminar el terrorismo en todas sus formas pero con un amplio enfoque hacia la seguridad cibernética y protección de la infraestructura crítica.

La estrategia adoptada por Colombia está documentada en el CONPES (Consejo Nacional de Política Económica y Social) 3854. Con el objetivo de impulsar en el país una política nacional de seguridad digital, donde la directriz está basada en la oportuna identificación y prevención de riesgos en entornos digitales e infraestructuras críticas. Este documento surge como un plan de cambios y restructuración al anterior CONPES 3701 enfocado en contrarrestar el incremento de las amenazas cibernéticas, bajo los objetivos de defensa del país y lucha contra el cibercrímen dejando de lado la gestión del riesgo en el entorno digital. Enfoque esencial en un contexto en que el incremento en el

uso de las TIC para realizar actividades económicas y sociales ha traído consigo nuevas y más sofisticadas formas de afectar el desarrollo normal de estas en el entorno digital.

II. ANÁLISIS POLÍTICA NACIONAL DE SEGURIDAD DIGITAL PARA COLOMBIA CONPES 3854

Para Colombia el enfoque de la política de ciberseguridad y ciberdefensa en la actualidad se ha concentrado en contrarrestar el aumento de las amenazas cibernéticas bajo los objetivos de defensa nacional, dejando de lado la gestión del riesgo.
CONPES 3854 como estrategia de ciberseguridad nacional, quiere cambiar este enfoque tradicional al incluir la gestión del riesgo como uno de los elementos más importantes para abordar el plan de cambio adoptando los principios fundamentales: Identificar, gestionar, tratar y mitigar, la planeación de la política que por fases permitirá en el tiempo organizar y delimitar el cumplimiento. A continuación, se relacionan las principales actividades. Datos obtenidos, directamente del documento CONPES 3854.

1era fase: Se establecerá un marco institucional claro en torno a la seguridad digital. Para esto, se crearán las máximas instancias de coordinación y orientación superior en torno a la seguridad digital en el Gobierno, y se establecerán figuras de enlace sectorial en todas las entidades de la rama ejecutiva a nivel nacional. El Departamento Nacional de Planeación será el directo encargado de administrar y revisar el cumplimiento de la política.

2da fase: Se crearán las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, mediante mecanismos de participación permanente, la adecuación del marco legal y regulatorio de la materia y la capacitación para comportamientos responsables en el entorno digital.

3era fase: Se fortalecerá la defensa y seguridad nacional en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos.

4ta fase: Se generarán mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico.

A. Gestión económica:

Monto proyectado a tres años inversión total de 85.070 millones de pesos, el plan de acción se deberá ejecutar a partir del 2016 y finalizando en el 2019.

Principales entidades ejecutoras del presupuesto:

- Ministerio de Tecnologías de la Información y las Comunicaciones.
- Ministerio de Defensa Nacional.
- Dirección Nacional de Inteligencia.
- Departamento Nacional de Planeación.

Entidad	2016	2017	2018	2019	Total
Ministerio de Defensa Nacional	14.618	7.392	7.583	7.782	37.375
Ministerio de Tecnologías de la Información y las Comunicaciones	8.750	13.950	13.000	9.550	45.250
Dirección Nacional de Inteligencia	-	-	500	1.000	1.500
Ministerio de Justicia y del Derecho	-	200	250	-	450
Ministerio de Educación Nacional	-	75	150	120	345
Departamento Nacional de Planeación	75	75	-	-	150
Total	23.443	21.692	21.483	18.452	85.070

Tabla 1. Financiamiento estimado 2016-2019, fuente: documento CONPES 3854.

Como objetivos específicos para el cumplimiento de la política y asignación del presupuesto están los siguientes lineamientos:

- Establecer un marco institucional para la seguridad digital, creando conciencia hacia un enfoque de gestión de riesgos.

- Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital.

- Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y transnacional, con un enfoque de gestión de riesgos.

- Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos.

- Generar mecanismos permanentes y estratégicos para impulsar la cooperación, colaboración y asistencia en seguridad digital, a nivel nacional e internacional.

- Implementación de las estrategias: plan de acción.

- Establecer un marco institucional para la seguridad digital consistente con un enfoque de gestión de riesgos.

- Valoración de impacto económico de la política.

- El seguimiento a la ejecución física y presupuestal de las acciones propuestas para el cumplimiento de los objetivos del documento CONPES.

B. Estrategia de gestión de riesgos de seguridad digital.

Para el diseño de la estrategia de riesgos de seguridad digital, Colombia como país miembro reviso las recomendaciones formuladas en el estudio realizado año 2015(Perspectivas de la OCDE sobre la economía digital 2015) por la OCDE (Organización para la Cooperación y el Desarrollo Económico).

Recomendaciones OCDE:

- La seguridad digital debe tener un enfoque flexible y ágil para abordar las incertidumbres digitales.

- La estrategia nacional debe crear las condiciones para que las múltiples partes interesadas puedan gestionar la seguridad digital de sus actividades económicas y sociales.

- La estrategia nacional debe fomentar la confianza en el entorno digital y además debe estar apoyada desde el más alto nivel de Gobierno, incluyendo de manera directa a los principales ministerios y entidades de apoyo.

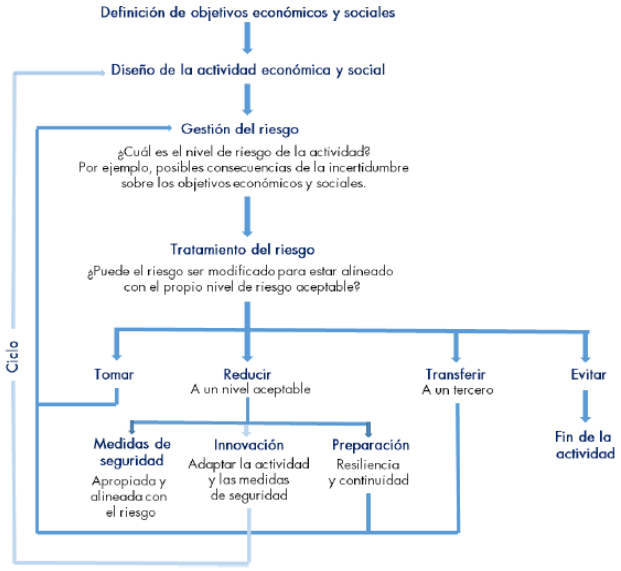

Figura 1. Modelo de gestión sistemática y cíclica de riesgo seguridad digital, fuente: documento CONPES 3854.

El modelo de gestión sistemática y cíclica de riesgo de seguridad digital refleja los principios operativos recomendados por la OCDE, se puede utilizar como un marco de referencia para iniciar un plan de gestión de riesgos corporativo, aunque no se refleja un detalle técnico ni de procedimiento se puede utilizar bajo un enfoque general.

Objetivos modelo de gestión sistemática y cíclica de riesgo de seguridad digital orientados a la política nacional:

- Adopción del modelo, gestión sistemática y cíclica del riesgo.

- El modelo debe ser liderado desde el alto nivel del Gobierno.

- Asegurar la defensa y seguridad nacional.

- Estimular la prosperidad económica y social.

- Adoptar un enfoque multidimensional, es decir, la seguridad digital será abordada tanto desde la dimensión técnica o jurídica, como desde la dimensión económica y social.

- Se deben tener en cuenta a las múltiples partes interesadas.

- Promoverá la responsabilidad compartida y salvaguardará los derechos humanos.

- Protegerá los valores nacionales y concientizará a todas las partes implicadas en el proceso de gestión de riesgos digitales.

C. Estado actual, política nacional de seguridad digital Colombia.

Para el establecimiento de una política nacional es importante tener como referencia la actualidad local sin obviar el escenario internacional, a continuación, se presentan datos estadísticos con relación a los incidentes presentados en seguridad digital y los principales sectores afectados, el orden establecido será, primero el escenario internacional y luego el nacional:

Organización afectada	Sector	Impacto
Snapchat	Red social	4,5 millones de nombres y números móviles comprometidos
Kickstarter	*Crowd funding*	5,6 millones de victimas
Korean Telecom	Telecomunicaciones	12 millones de suscriptores comprometidos
Heartbleed	*Software*	Primera de tres vulnerabilidades de fuente abierta
Ebay	Compras	Base de datos de 145 millones de compradores comprometida
PF chang´s	Comidas	Mas alta violación de información de alto nivel del mes
Energetic bear	Energía	Operación de ciberespionaje a la industria de energía
Cybervor	Tecnología	1,2 billones de credenciales comprometidas
iCloud	Entretenimiento	Cuentas de celebridades comprometidas
Sandworm	Tecnología	Ataque cibernetico a la vulnerabilidad de Windows
Sony Pictures	Entretenimiento	Mas alta violación de alto nivel del año
Inception Framework	Sector público	Operación de ciberespionaje a sector público

Tabla 2. Grandes casos de ataque cibernéticos en el mundo en el 2014, fuente: documento CONPES 3854.

¿Porque ninguna empresa colombiana está en el anterior informe?, una respuesta simple estaría en la ausencia de una legislación que obligue a cualquier empresa en el territorio colombiano a reportar cualquier ataque cibernético.

Legislaciones internacionales como la de Estados Unidos de América tiene un nivel de madurez en este sentido, lo cual ayuda a la concienciación de las partes interesadas o sectores productivos que estén en la capacidad de evidenciar y prevenir un futuro riesgo.

SECTORES	ATAQUES POR DÍA	PORCENTAJE	TENDENCIA A FUTURO
Financiero	6.600.000	75,29%	Aumentarán
Gobierno	925.600	10,56%	Aumentarán
Comunicaciones	737.200	8,41%	Se mantendrá
Energía	325.347	3,71%	Descenderán
Industria	173.900	1,98%	Aumentarán
Comercio	3.600	0,05%	Aumentarán
TOTAL	8.765.647	100%	

Figura 2. Panorama de los sectores en seguridad informática en LATAM (sectores afectados) cierre a 2015, fuente: cifras Digiware a 2015.

Los principales sectores atacados en Latinoamérica, bajo un interés determinado, el sector financiero sigue siendo el más apetecido por los ciberdelicuentes, el restante forma parte en su mayoría de la infraestructura crítica de un país como lo es: Comunicaciones energía y Gobierno.

Figura 3. Panorama de los sectores en seguridad informática en LATAM (ataques en la región) cierre a 2015, fuente: cifras Digiware a 2015

Colombia es el tercer país más atacado de Latinoamérica debido a la cantidad de población con acceso a Internet, siendo mayor esta cifra a la implementación de estrategias de defensa digital de usuarios y de empresa.

Revisando las cifras de manera general, se visualiza un riesgo alto de ciberseguridad para las partes interesadas, muy específicamente para la infraestructura crítica del país, objetivo primario del documento origen de estudio en este artículo CONPES 3854.

Se define como infraestructura crítica de un país cuyos activos, sistemas y redes, ya sean físicos o virtuales, son tan vitales para Colombia que su incapacidad o destrucción tendrían un efecto debilitante sobre la seguridad, la economía nacional, la salud, seguridad pública nacional, o cualquier combinación de éstas.

Principales tipos de infraestructura crítica para un país:

- Instalaciones químicas.
- Instalaciones comerciales.
- Comunicaciones.
- Fabricación crítica.
- Represas.
- Bases industriales de defensa.
- Servicios de emergencia.
- Energía.
- Servicios financieros.
- Alimentación y agricultura.
- Instalaciones gubernamentales.
- Salud pública.
- Tecnología de la información.
- Reactores, materiales y residuos nucleares.
- Sistemas de transporte.
- Sistemas de agua y agua residual.

Todos estos sectores dependen en cierta medida de la infraestructura digital conocida como Internet.
La tendencia probable para 2018 es que los atacantes sigan sondeando la infraestructura crítica a través de la infraestructura de Internet. Distintos tipos de atacantes seguirán buscando maneras de causar daño, denegar el servicio o secuestrar datos para pedir un rescate, colocando a Colombia en un panorama preocupante si no se toman las medidas correctas y enfocando los controles a una metodología de prevención de riesgos digitales.
El análisis sobre el estado actual de la política nacional de seguridad digital en Colombia se destaca lo siguiente:

- En materia de cooperación nacional el CCOC (Comando Conjunto Cibernético), integrantes comando general de las fuerzas militares de Colombia, viene adelantando el proceso de elaboración, catálogo de infraestructuras críticas cibernéticas nacionales en el país, el catálogo en mención permitirá a futuro coordinar y gestionar los planes y programas de protección y defensa a infraestructuras críticas cibernéticas nacionales, a 2015 el ministerio de defensa nacional había elaborado la guía para la identificación de la infraestructura crítica , la cual constituye el insumo principal de dicho catálogo y construido en coordinación con las múltiples partes interesadas.
La identificación de infraestructura crítica cibernética en Colombia se desarrolla actualmente como proceso para creación del catálogo final, documento que por su importancia estará clasificado como secreto, el levantamiento de información e identificación de la infraestructura está basado en el conjunto de buenas prácticas internacionales **Framework for improving critical infrastructure cibersecurity (NIST),** metodología adoptada por el Gobierno de los Estados Unidos de América como estrategia y marco de referencia para el tratamiento de los riesgos en la seguridad digital del país y de sus principales infraestructuras críticas, este marco de buenas prácticas está dividido en tres partes, Framework core, Framework implementación tiers, y Framework profiles.

- Framework core: es un conjunto de actividades de seguridad cibernética, resultados deseados y referencias aplicables que son comunes en los sectores de infraestructura crítica. El core presenta las normas, directrices y prácticas de la industria de manera que permita una comunicación de las actividades y los resultados de la seguridad cibernética aplicado a nivel ejecutivo y a nivel de implementación de las operaciones. Framework core consta de cinco funciones simultáneas y continuas: identificar, proteger, detectar, responder, recuperar, consideradas conjuntamente, funciones que proporcionan una visión estratégica de alto nivel del ciclo de vida en la gestión de una organización basada en el riesgo de seguridad cibernética. Framework core identifica las categorías y subcategorías clave subyacente para cada función, comparándolos con base en referencias informativas tales como estándares

existentes, directrices y prácticas para cada subcategoría.

- Framework implementation tiers: proporciona un contexto sobre cómo una organización considera el riesgo para la seguridad cibernética y los procesos existentes para manejar ese riesgo. Los niveles (tiers) describen el grado en que las prácticas de gestión de riesgo de ciberseguridad de una organización son características definidas en el Framework (por ejemplo, riesgo, amenaza, repetible y adaptado). Los niveles (tiers) caracterizan las prácticas de una organización en un rango, desde parcial (nivel 1) a adaptable (nivel 4). Estos niveles (tiers) reflejan la progresión desde la informalidad, las respuestas a enfoques que sean ágiles y estén informados sobre el riesgo. Durante la selección del nivel (tier) de proceso una organización debe considerar sus prácticas actuales de gestión de riesgos, medio ambiente, requisitos legales y reglamentarios, objetivos de negocio, misión, y restricciones organizacionales.

- Framework profiles: representa los resultados basados en las necesidades del negocio en la cual la organización ha seleccionado las categorías del Framework y sub categorías. El perfil se puede caracterizar como alineación de normas, directrices y prácticas sobre el Framework core, en un escenario de implementación particular. Los perfiles pueden utilizarse para oportunidades de mejorar la postura de la seguridad cibernética mediante la comparación de un ("tal cual") con un perfil de "objetivo" (el estado "ser"). Para desarrollar un perfil, la organización puede revisar todas las categorías y sub categorías sobre la base de los conductos y una evaluación del riesgo, determinando cuáles son los más importantes; ellos pueden agregar categorías y sub categorías según sea necesario para abordar los riesgos de la organización.

El perfil puede utilizarse para apoyar la priorización y la medición del progreso hacia el perfil objetivo, teniendo en cuenta otras necesidades empresariales, incluida la eficacia de innovación.
Los perfiles pueden utilizarse para llevar a cabo autoevaluaciones y comunicarse a la organización o entre diferentes organizaciones.

Figura 4. Estructura del Framework core, fuente: Documento, Framework for improving critical infrastructure cyber security versión 1.0, National Institute of Standards and Technology, february 12, 2014.

Framework core, proporciona un conjunto de actividades para lograr resultados específicos hacia la seguridad cibernética, referenciando ejemplos de orientación para lograr óptimos resultados. Framework core no es una lista de acciones a realizar presenta los resultados clave de ciberseguridad identificados por la industria, como gestión del riesgo para ciberseguridad. Framework core consta de cuatro elementos: **funciones, categorías, sub categorías y referencias informativas,** a continuación, se explicarán de manera general cada una de ellas.

- Funciones: Organizar actividades básicas de ciberseguridad en su nivel más alto. Estas funciones son: Identificar, proteger, detectar, responder y recuperar. Ayudan a una organización expresando su gestión del riesgo de seguridad cibernética organizando información, las decisiones de gestión, abordando las amenazas y mejorando mediante el aprendizaje de eventos e incidentes previos. Las funciones también se alinean con las metodologías existentes para la gestión de incidentes y ayudan a mostrar el impacto en las inversiones de ciberseguridad. Por ejemplo, las inversiones en planificación y ejercicios de apoyo a las acciones de respuesta y recuperación oportunas, reduciendo el impacto en la prestación de servicios.
- Categorías: Especifica las subdivisiones de una función en grupos de resultados para seguridad

cibernética están estrechamente ligados a necesidades programáticas y a actividades particulares. Ejemplos de categorías incluye "gestión de activos", "control de acceso" y "procesos de detección".

- Sub categorías: son la división de una categoría en resultados específicos de las actividades de gestión. Proporcionan un conjunto de resultados que, aunque no exhaustivos, apoyan el logro de los resultados en cada categoría. Ejemplos de sub categorías "los sistemas de información externos están catalogados, "los datos en reposo están protegidos" y "se investigan las notificaciones de los sistemas de detección".

- Referencias informativas: Son secciones específicas de normas, directrices y prácticas comunes entre los sectores de infraestructura crítica que ilustran un método para lograr los resultados asociados con cada sub categoría. Las referencias informativas presentadas en el Framework core, son ilustrativas y no exhaustivas. Se basan en orientaciones intersectoriales que se mencionan con mayor frecuencia durante el proceso de desarrollo del Framework core.

Como resultado de la política nacional de seguridad digital y enmarcada a nivel de indicador de gestión, la institucionalidad ha permitido la creación de los siguientes grupos y equipos de trabajo como plan estratégico y de respuesta ante incidentes cibernéticos.

- Grupos de respuesta ante incidentes cibernéticos:

1. **ColCert:** Grupo de respuesta a emergencias cibernéticas en Colombia, integrantes Ministerio de Defensa Nacional.
2. **CCOC:** Comando Conjunto Cibernético, integrantes comando general de las fuerzas militares de Colombia.
3. **CCP:** Centro Cibernético Policial, integrantes policía nacional de Colombia.
4. **CSIRT PONAL:** Equipo de respuesta a incidentes de seguridad informática de la policía nacional.
5. **Delegataria de protección de datos,** entidad encargada Superintendencia de Industria y Comercio.
6. **Subdirección técnica de seguridad y privacidad de tecnologías de información,** entidad encargada Ministerio de Tecnologías de la Información y las Comunicaciones.
7. **Comité de ciberdefensa,** entidad encargada Fuerzas militares.
8. **Unidades cibernéticas,** entidades encargadas: Ejército nacional, Armada nacional y la Fuerza Aérea Colombiana.
9. **Comisión nacional digital y de información estatal,** se creó mediante el decreto 32 de 2013 del Ministerio de Tecnologías de la Información y las Comunicaciones.

Colombia cuenta con 8 CSIRT (Equipo de respuesta frente a incidencias de seguridad informática) con membrecía en el foro de equipos de seguridad y respuesta de incidentes FIRST (Foro internacional equipos de respuesta a incidentes de seguridad) esto le permite responder de manera eficaz a incidentes de seguridad al tener acceso a información acerca de las mejores prácticas, ser invitados a eventos, capacitaciones y cursos relacionados con la seguridad digital.

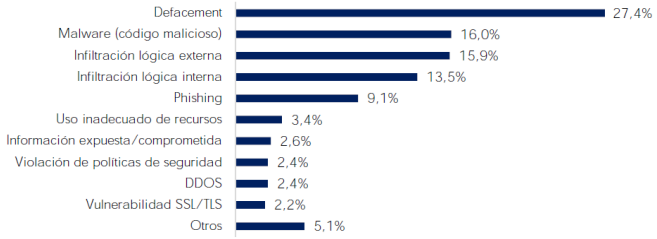

Figura 5. Incidentes digitales gestionados por el CCOC y el colCERT en el entorno digital en Colombia, 2015, fuente: Documento CONPES 3854.

- Enfoque de múltiples partes interesadas y responsabilidad compartida. Cada actor que depende del entorno digital para desarrollar algunas o todas sus actividades económicas y sociales debe ser vinculado representando un papel particular en el enfoque orientado a gestión de riesgos, partiendo de la premisa donde el Gobierno establece de manera estandarizada una metodología para gestionar los riesgos digitales, todas las partes

interesadas tendrían un enfoque para analizar y tratar los riesgos expuestos en un entorno digital, de esta manera el impacto podría reducirse a niveles aceptables o de rápida recuperación. La política además debe incorporar de manera diferenciada el objetivo de prosperidad económica y social, en lugar de continuar tratando el riesgo de seguridad digital como un problema técnico que necesita soluciones técnicas, este también debería abordarse como un riesgo económico que debe gestionarse en cualquier proceso de toma de decisiones.

- La política nacional de seguridad digital se regirá por cuatro principios fundamentales (PF):

1. Salvaguardar los derechos humanos y valores fundamentales.
2. Adoptar un enfoque incluyente y colaborativo.
3. Asegurar una responsabilidad compartida.
4. Adoptar un enfoque basado en la gestión de riesgos.

- Nivel de madurez.

BID (Banco Interamericano de Desarrollo) y la OEA (Organización de los Estados Americanos) a través de su modelo de madurez de capacidad de seguridad cibernética, asigna una clasificación en diferentes aspectos a continuación, se detallan los principales:
Clasificación: inicial, formativo, establecido, estratégico, dinámico.

1. Capacidad de respuesta a incidentes clasificación asignada = formativo
2. Las múltiples partes interesadas no maximizan sus oportunidades al desarrollar actividades socio económicas en el entorno digital, los problemas no se abordan al más alto nivel de Gobierno, el Gobierno no cuenta con una evaluación exhaustiva de la situación de riesgo a nivel nacional y por tanto no puede tomar decisiones basadas en la gestión del riesgo.
3. Marco jurídico y reglamentario clasificación asignada = establecido.

Se establece el marco jurico y reglamentario en aspectos como privacidad, protección de datos y otros derechos humanos.

D. América Latina y la ciberseguridad en infraestructuras críticas.

La evolución de los incidentes ha permitido que la mitad de las compañías de América Latina y del Caribe sufrieran ataques en los años recientes, al igual que las instituciones gubernamentales, las administraciones y las organizaciones políticas. Los ataques siguen al alza. Argentina es uno de los países con la actividad criminal cibernética más alta del mundo. Las amenazas cibernéticas en Colombia también son numerosas pues casi la mitad de los ataques de phishing en América Latina ocurren en este país. Estos ciberataques incluyen los fraudes, los ataques dirigidos, el secuestro de computadoras, el hacktivismo, el robo de información pública, privada y de identidad (especialmente en el sector financiero), el terrorismo, la guerra y el espionaje militar. Los ciberataques en la región incluyen también ataques de alto perfil y robo de identidad, similar a lo que sucedió con el correo electrónico del presidente Santos, que tuvo una gran repercusión en los medios. A escala global, las dos principales tendencias en el crimen cibernético son el fraude con motivaciones económicas, y los ataques contra la confidencialidad, la integridad y la disponibilidad.

Todo sistema informático basado en plataformas digitales contiene vulnerabilidades inherentes, América Latina no es la excepción gracias a esta condición inevitable se ha producido un aumento significativo en los ataques dirigidos, en particular los ataques dirigidos a los sectores o infraestructuras que brindan servicios críticos para la sociedad y el estado, fomentando el crecimiento de los servicios de detección de vulnerabilidades. Se hace esto para ayudar a establecer prioridades, solucionar los problemas de seguridad y cumplimiento para prevenir ataques, y facilitar la implementación de políticas y estrategias adecuadas
En cada caso. Los datos de Brasil, Chile y México revelan que la mayoría de las vulnerabilidades se relacionan con las configuraciones erróneas de los sistemas, seguidas por versiones obsoletas y problemas con las aplicaciones. Sin embargo, esos problemas se asocian con un nivel de riesgo más alto. 60% de las vulnerabilidades que dejan al

descubierto los agujeros podrían afectar a la confidencialidad de la información. En tanto, 30% de las vulnerabilidades representan una amenaza para la integridad, mientras que 10% de las vulnerabilidades son debilidades que pueden aprovechar los ataques contra la disponibilidad de la información y de los servicios.

Ataques más utilizados en América Latina en infraestructuras críticas:

- Distributed Denial of Service (DDoS).

Los ataques "DDoS-for-hire" y los ataques de reflexión y de múltiples vectores son una tendencia que aumenta en cuanto al número y volumen de los incidentes. Las víctimas de estos ataques incluyen a proveedores de servicios financieros, compañías de comercio electrónico, instituciones gubernamentales, medios digitales, centros de datos, etc. En Chile, una sola víctima sufrió hasta 35 ataques DDoS en un mes durante 2014. 50% de los ataques observados tuvieron un ancho de banda menor a los 5Gbps; mientras que 25% de los ataques tuvieron anchos de banda entre 5 y 10Gbps; y el 25% restante incluyó accidentes con volúmenes entre 10 y 20Gbps. Los ataques más frecuentes tuvieron anchos de banda superiores a 20Gbps. Los ataques de 50Gbps son cada vez más comunes. La información es similar al resto de los países de la región.

La mayoría de los ataques con un volumen más alto que utilizaron el protocolo UDP se dirigieron a los puertos NTP, DNS, SNMP, HTTP y HTTPS, lo que implica el uso potencial de mecanismos de reflexión/amplificación para crear tráfico. También se ha observado un aumento importante en el volumen de ataques contra SSL/TLS.

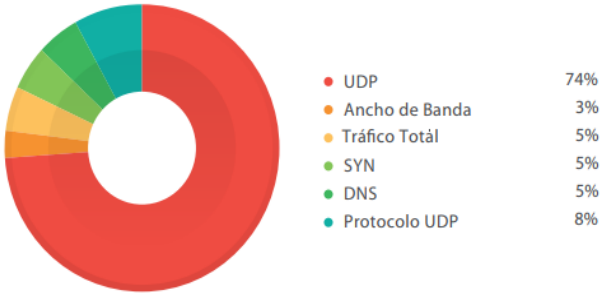

Figura 5. Tipos de ataques del "protocolo UDP": ataques que utilizan las anomalías del protocolo UDP, fuente: Reporte de seguridad cibernética e infraestructura crítica de las américas Trend Micro 2015.

- Spam y malware.

El robo de información confidencial sigue siendo la principal motivación para quienes utilizan el correo electrónico para propagar amenazas, también los medios sociales siguen siendo el medio perfecto para esta categoría de cibercrimen.

Por su parte, el fraude contra las instituciones financieras utiliza el spam para ocultar el phishing, el malware y el robo de datos. De acuerdo con los proveedores de servicios y contenido brasileños, cerca de dos millones de correos electrónicos basura son enviados diariamente, de los cuales un porcentaje importante se hacen pasar por notificaciones de tarjetas de crédito.

De acuerdo con información acerca del malware en la región de habla hispana, se reportan alrededor de 1.5 millones de intentos de conexión desde las computadoras infectadas a sus respectivos C&Cs. De igual manera, se identifican alrededor de 10,000 IPs diariamente, y se infectan 7,000 diferentes IPs a la semana con malware, lo que corresponde a la actividad de cerca de 50 botnets diferentes, incluyendo a DOWNAD/Conficker12, ZACCESS/ZeroAccess13 y la familia de malware B10614.

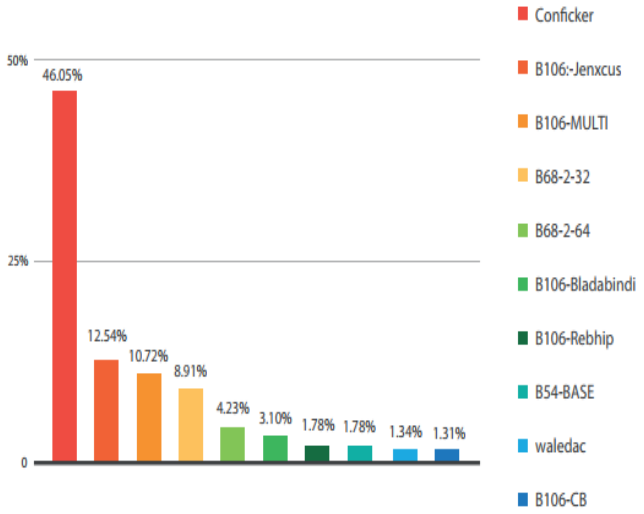

Figura 6. Información sobre la principal actividad del malware a febrero de 2015, fuente: Reporte de seguridad cibernética e infraestructura crítica de las américas Trend Micro 2015.

Conficker: Gusano botnet, B106: Robo de identidad/ fraude financiero/invasión de la privacidad**, B68: ZeroAccess:** publicidad/ fraude de clics, **B54: Citadel:** robo de identidad/ fraude financiero, **Waledac:** Spam.

- Capacidades y retos (Colombia):

Los ingresos del sector de las ITC de Colombia alcanzaron los €14,000 millones en 2012, 6% del PIB con un crecimiento anual de 9%. La industria de las ITC creó 110,000 empleos directos y reporta un crecimiento superior al de otros sectores. La inversión en el sector de las ITC alcanzó los €5,900 millones de euros en 2013, por lo que Colombia se coloca como el cuarto país de América Latina después de Brasil, México y Argentina. El plan de ciberseguridad será la hoja de ruta para la administración y se aplicará a las infraestructuras críticas y al sector privado, sus aspectos más importantes incluyen: una estructura de doble defensa y ciberseguridad contra las amenazas externas e internas, el crecimiento de los recursos tecnológicos; revisión y endurecimiento del actual marco regulatorio y el reforzamiento de las capacidades de inteligencia, tanto técnicas como humanas. Colombia enfrenta varios desafíos educativos, para promover y consolidar una cultura de la ciberseguridad en todos los ámbitos regulatorios, para establecer un marco claro que se adecue a la realidad del país y sus recursos críticos, con la capacidad de verificar el cumplimiento.

E. Diferencias de la ciberseguridad en el entorno industrial.

Los ataques con software malicioso tipo Malware en sistemas industriales, tienen como objetivo los sistemas de control industrial (ICS) y los sistemas de adquisición de datos y control de supervisión (SCADA) , como referencia se tiene el famoso caso Stuxnet que infecto en 2010 una planta de enriquecimiento de uranio en Natanz, Irán y logro entrar a través de una memoria usb ,logrando infectar en promedio 1000 máquinas que manejaban las centrifugadoras, el objetivo era destruir este tipo de sistemas y generar un daño irreversible en la planta, al parecer la cooperación entre países para generar este ataque genera un nuevo concepto de ciberguerra, puede haber cierta superposición en las amenazas y sus diferentes vectores pero hay diferencias significativas entre los requerimientos de ciberseguridad en los ecosistemas industriales y las corporaciones de negocios generales .

Los ambientes corporativos están enfocados en salvaguardar los datos confidenciales, cuando se tratan de sistemas industriales cada minuto de tiempo en inactividad o error tiene un costo, las operaciones ininterrumpidas son la máxima prioridad. Esta característica es lo que distingue a la ciberseguridad industrial de otras empresas.

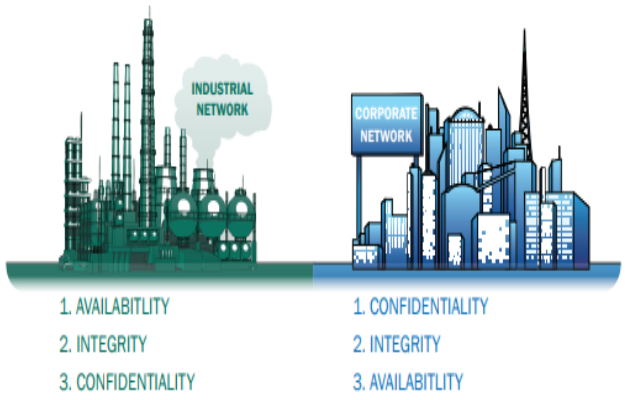

Figura 7. Diferencias de ciberseguridad industrial, Fuente: Documento Empowering industrial cyber security_web.pdf, autor Kaspersky Lab.

Se debe considerar 3 pilares en el momento de implementar una solución dirigida a los ecosistemas industriales, en el mundo de la seguridad informática es conocido como un enfoque holístico, a continuación, son relacionados:

- Procesos basados y enfocados a la implementación segura (procesos).

- Concienciación de los empleados en temas de ciberseguridad (personas).

- Tecnologías creadas específicamente para entornos industriales (tecnologías).

En un reciente reporte (ics-report-2017) del fabricante Kaspersky se encuentran los siguientes datos:

- 83% de los encuestados creen estar bien preparados para enfrentar incidentes de ciberseguridad en sectores ICS, al mismo tiempo la mitad de las empresas encuestadas experimentaron de uno a cinco incidentes de seguridad digital en los pasados 12 meses y 4% experimentaron mayor a seis meses.

- Los profesionales de seguridad orientada a sistemas industriales ICS tienen un optimismo acerca de la realidad, pero no están convencidos que este optimismo sea compartido: 31% dicen que la ciberseguridad de ICS es una prioridad baja para la alta gerencia.

- La ciberseguridad ineficaz cuesta a las organizaciones industriales $ 497K por año en promedio.

- Las principales consecuencias de los incidentes de ciberseguridad incluyen: daño a la calidad del producto y del servicio, pérdida de información confidencial o de propiedad, reducción o carencia en la producción para alguno de los sitios.

- La mitad de las compañías ICS encuestadas admiten que los proveedores externos tienen acceso a redes de control industrial en su organización, ampliando el perímetro de amenaza.

- 81% de las empresas informan de un mayor uso de las conexiones inalámbricas a la red industrial, señal de la ausencia de una correcta estrategia de seguridad inalámbrica.

- El top tres para tipo de soluciones orientadas a la ciberseguridad en entornos industriales son: Monitoreo de red antimalware, control de acceso para dispositivos de la misma manera el 54 % es considerado el escaneo de vulnerabilidades y gestión de actualizaciones.

III. CONCLUSIONES

La política nacional de seguridad digital en Colombia fue planeada desde su inicio, bajo un enfoque defensivo, con direccionamientos reactivos, los cuales solo permitían atender los incidentes de seguridad digital desde la perspectiva de remediación , la colaboración internacional en estos últimos años han permitido visualizar los problemas de la actual política, lo cual genera un nuevo documento CONPES con una directriz en particular, implementar el enfoque de gestión de riesgos de seguridad digital .

La política actual de seguridad digital en Colombia está centrada en el sector de defensa , sin coordinación de las partes interesadas , el personal capacitado en temas técnicos es una de las principales tareas a mejorar en los entes militares, siendo un tema de interés militar ya que tiene que ver con aspectos de la seguridad nacional, falta programas de formación, personal con experiencia y certificaciones internacionales, que permitan el planeamiento de una correcta estrategia en seguridad de la información e informática.

Las pequeñas y medianas empresas no están visualizando la necesidad de invertir en proyectos de seguridad de la información e informática, la falta de presupuesto y de conocimiento en el tema son los principales problemas, el Gobierno debe involucrar a estos sectores productivos, como partes interesadas donde los planes de capacitación y concienciación lleguen a los principales tomadores de decisión, para que puedan articular estrategias de mitigación ante posibles riesgos de seguridad digital, en un entorno que cada vez tiende hacia la comunicación global e Internet.

REFERENCIAS

[1] Antecedentes y justificación (Documento CONPES 3854 Versión aprobada Bogotá, D.C., 11 de abril de 2016), Política nacional de seguridad digital, Consejo Nacional de Política Económica y Social república de Colombia departamento nacional de planeación.

[2] Mejores prácticas internacionales (Documento CONPES 3854 Versión aprobada Bogotá, D.C., 11 de abril de 2016), Política nacional de seguridad digital, Consejo Nacional de Política Económica y Social república de Colombia departamento nacional de planeación.

[3] Diagnostico (Documento CONPES 3854 Versión aprobada Bogotá, D.C., 11 de abril de 2016), Política nacional de seguridad digital, Consejo Nacional de Política Económica y Social república de Colombia departamento nacional de planeación.

[4] Definición de la política (Documento CONPES 3854 Versión aprobada Bogotá, D.C., 11 de abril de 2016), Política nacional de seguridad digital, Consejo Nacional de Política Económica y Social república de Colombia departamento nacional de planeación.

[5] Colombia es el tercer país de la región con más ataques cibernéticos (Nota de prensa publicada en Pagina web http://www.eltiempo.com/archivo/documento/CMS-16383752), El Tiempo- tecnosfera.

[6] Amenazas para infraestructuras críticas la dimensión de Internet (Documento La seguridad como rehén Tendencias 2017), ESET, spol. s r.o., Cameron Camp Malware Researcher, Stephen Cobb, Senior Security Researcher.

[7] Digiware ataques en la región (Nota de prensa publicada en Pagina web http://gadgerss.com/wp-content/uploads/2015/10/digiware-ataques-en-la-region-1024x728.jpg), Digiware.

[8] Framework Introduction (Documento Framework for Improving Critical Infrastructure Cybersecurity Version 1.0), National Institute of Standards and Technology.

[9] América Latina y la Ciberseguridad Industrial (Documento Reporte Seguridad Cibernética y Protección de la Infraestructura Crítica), 2015 - OEA Trend Micro.

[10] Ciberseguridad en entornos industriales datos y estadísticas a https://www.kaspersky.com/blog/ics-report-2017/16967/.

Autor: Johan Cubillos R.

Ingeniero de sistemas especializado en seguridad informática y networking, amplio criterio en manejo de proyectos para gestión de riesgos, amenazas y vulnerabilidades en ambientes tecnológicos de alta disponibilidad, implementación y transición de servicios de infraestructura para el área de tecnología, liderazgo comprobado de equipos multidisciplinarios y personal de apoyo técnico, conocimiento norma internacional para gestión de la seguridad de la información ISO/IEC 27001:2013, metodología de análisis y gestión de riesgos de los sistemas de información MAGERIT v.3