# ¿CÓMO ESTAMOS EN CIBERSEGURIDAD NACIONAL E INTERNACIONAL, SU GESTIÓN DE RIESGOS Y TENDENCIAS?

Linares Lizarazo, Yaneth

ingyanethlinares@hotmail.com
Universidad Piloto de Colombia

***Resumen*** — El contenido del artículo, se materializa desde la perspectiva de la importancia que tiene la Ciberseguridad, para proteger los activos de una organización. Hace un análisis global a cerca del rol actual de la Ciberseguridad, frente a los problemas del funcionamiento de la Infraestructura Crítica y de las tendencias en nuestros días.

Se ocupa de señalar la relevancia de la Tecnología Digital, en el desarrollo de los países y se plantean las causas, las consecuencias y las tendencias del problema que la afectan; las distintas maneras en que lo hacen y los variados procedimientos y métodos para evitarlos.

Se exponen las posiciones asumidas, por respetables organizaciones, como la NIST, ISO, INCIBE y otras en relación a sus resultados sobre sus investigaciones, relacionadas con el desarrollo y aplicación de la Gestión de Riesgos de Ciberseguridad, y se presenta el Modelo de Madurez de Capacidad -CMM-, creado para detectar la capacidad de los países, para prevenir y controlar los riesgos. Se presta atención especial, al análisis del marco conceptual de ciberseguridad de la NIST y presenta el desarrollo y aplicación de la gestión de riesgos de seguridad, y termina con la presentación y análisis sobre la Ciberseguridad en Colombia.

***Índice de Términos***— Ciberseguridad, Información, Gestión de Riesgos, Infraestructura Crítica, entorno, activos, resiliencia, estándares, vulnerabilidad, amenazas, riesgos, impacto, probabilidad, evaluación, tolerancia, mitigar, buenas prácticas, capacidad, organización, redes, contexto, implementación, ataques, ciberdelincuentes, Economía Digital, ámbito.

***Abstract***— The content of the article is materialized from the perspective of the importance of cybersecurity to protect the assets of an organization. It makes a global analysis about the current role of cybersecurity in the face of the problems of the operation of critical infrastructure and trends in our days.

It deals with pointing out the relevance of digital technology in the development of countries and the causes, consequences and trends of the problem that affect it are considered; the different ways in which they do it and the varied procedures and methods to avoid them.

The positions of some respected organizations such as NIST, ISO, INCIBE and others are exposed in relation to the results of their research related to the development and application of cybersecurity risk management, and the capacity maturity model -CMM- is presented. Created to detect the capacity of countries to prevent and control risks. Special attention is paid to the analysis of the cybersecurity conceptual framework of the NIST and presents the development and application of security risk management and ends with the presentation and analysis of cybersecurity in Colombia.

***Index Terms***— Cybersecurity, Information, risk management, critical infrastructure, environment, assets, resilience, standards, vulnerability, threats, risks, impact, probability, evaluation, tolerance, mitigation, good practices, capacity, organization, networks, context, implementation, attacks, cybercriminals, digital economy, scope.

## I. INTRODUCCIÓN

El avance de la Tecnología Digital, es lo que más profundamente y con mayor persistencia y éxito, ha contribuido a la consolidación y desarrollo del actual fenómeno de la globalización, convertido en motor de progreso económico y social.

En la era del Internet, el activo más importante para personas y organizaciones es la información digital, que ha de protegerse, en su confidencialidad, integridad y disponibilidad.

En este artículo, se busca una aproximación general a los problemas y tendencias que se han dado, en el escenario de la ciberseguridad, y la manera como se han tratado de superar.

La importancia del valor de la información “digital” y el aumento progresivo de la desconfianza en la utilización del internet, ha motivado a importantes organizaciones internacionales, como la ISO, NIST, ISACA entre otras, a trabajar en proyectos de investigación, que han conducido a disminuir la incertidumbre, utilizando un procedimiento de gestión de seguridad de la información, acogido a la normatividad internacional, a las leyes, a las buenas prácticas y con suficientes conocimientos para disponer de la mejor capacidad, para hacerlo.

El acceso a Internet y a la banda ancha, con objetivos diferentes al progreso general, y al bienestar, se ha interpretado como la búsqueda de beneficios fraudulentos, que al final se convierten en las amenazas y riesgos, que se traducen, en sucesos que proporcionan daños y perjuicios a organizaciones o empresas de diferentes tipos de actividades, sean publicas o

privadas. Esto lo podemos entender, como el costo de nuestro mundo conectado.

Se presenta, de manera muy general, la situación actual de la Ciberseguridad, considerando no solo el desarrollo y aplicación de la Gestión de Riesgos, de esta en el mundo, si no tratando también de mostrar sus tendencias, principios y normativas internacionales que la regulan; todo esto, con la señalización de un marco guía que será soporte, orientación y garantía para evitar los riesgos de la seguridad cibernética.

Estando en la Era de la Informática y de la ciber información, el mundo ha reconocido, categóricamente, que es esta era donde la humanidad globalizada ha tenido sus mayores y mejores progresos, y en la misma perspectiva, sobre el tema han reconocido la simultanea emergencia de riesgos y amenazas, que, al ser materializados, su impacto genera consecuencias que hacen daño y limitan el progreso de algunas organizaciones, impidiendo o limitando el cumplimiento de sus objetivos y misiones. Esta es la fuerza que se opone al progreso alcanzado y constituye el fundamento para resolver en la era de la informática y cuyos principales responsables son las organizaciones y la ciberseguridad.

En alguna forma, ya se ha enunciado anteriormente la presencia de un problema que afecta a la ciberseguridad. Por tanto, es adecuado hacer referencia al aspecto de la causalidad, consecuencias y tendencias del problema.

El acceso ilícito a sistemas y equipos de información y a infraestructuras críticas, corresponde a un ataque interno o externo. En el primer caso, (ISO 27032 9.4.2) puede tener su origen a través de personas con acceso físico a la red, en proveedores o ataques que han logrado acceso a la red interna, o con acceso físico o remoto no autorizado.

En el acceso de ataques externos (ISO 27032 9.4.3), estos ataques se dan a infraestructuras, aplicaciones, servicios o a cualquier activo. Los medios, gusanos, malware, o phishing, ataques de denegación de servicios o escaneos de puntos automatizados.

Los ciber riesgos y ciber amenazas se orientan a vulnerar la información “digital”, contenida en nuestros sistemas de información, dado que este es el activo principal de la organización; empero, se debe tener en cuenta que no es el activo de la información, el único amenazado, pues son susceptibles de ser perseguidos, también, la infraestructura informática, los equipos auxiliares, las redes de comunicaciones, las instalaciones y las personas.

Teniendo en cuenta que la característica de la Información Digital, de una organización, esta determinada por condiciones rigurosas, de confidencialidad, integridad y disponibilidad, estas tres dimensiones constituyen el enfoque, de los ciber atacantes, que pueden ser dirigidos a un hardware, a un software o al personal o a la propia organización, especialmente cuando algún tipo de vulnerabilidad la afecta.“El soborno, el robo, el secuestro o simplemente la destrucción de activos de la información, se han dado especialmente en los llamados riesgos mayores, como la delincuencia financiera, los de la estabilidad de los sistemas financieros, el robo de la información comercial, y el robo personal o la destrucción de activos, con el propósito de hacer daño a la Democracia, como es el caso de las Agendas Políticas”.

Las causales del problema, expuestas por ESET, en relación a las tendencias, han sido señaladas por autores de ESET e ISACA, quienes han hecho investigaciones en el año 2017, de las que han logrado concluir: que el índice de ciber amenazas ha crecido, especialmente, a nivel de las infraestructuras críticas, como la red eléctrica y los sectores de defensa y salud; procesos de fabricación cruciales y producción de alimentos, agua y transporte.

Los investigadores, han demostrado que ataques a la infraestructura crítica siguen creciendo, por la aparición generalizada de malwares que intentan provocar apagones, paralizar el transporte o detener procesos de fabricación. La capacidad de llevar a cabo ataques a redes eléctricas, tiende al aumento progresivo, especialmente en 2018, a menos que existan medidas preventivas.

Frente a estas perspectivas, hay una alternativa válida para la resolución del problema: desarrollar actividades de carácter continuo, en ámbitos en los que se tenga en cuenta, de manera integral, aspectos socioculturales, tecnocientíficos y económicos. Desarrollar una política orientada a capacitar a las empresas para que inicien o continúen realizando procedimientos y estrategias dirigidas a la protección de los activos empresariales, en el campo de la ciberseguridad. Esto, también, es una tendencia puesta de presente, en las inquietudes que han sido presentadas por el Modelo de Capacidad y Madurez (CMM).

La acentuada vulnerabilidad de la ciberseguridad en el mundo, ha conducido a la Organización de Estados Americanos, al Banco Interamericano de Desarrollo y a la Universidad de Oxford a crear un Modelo de Madurez de Capacidad (CMM) de seguridad cibernética, que ha sido utilizado para detectar la capacidad de los países para prevenir y controlar el riesgo. Se selecciono a Estonia, Israel, República de Corea y Estados Unidos como países más avanzados en cobertura de ciberseguridad, para ser evaluados con el CMM, y se detectó que la ciberseguridad está enfocada sustancialmente a delincuentes, pero también a adversarios.

David Harley, ha presentado a la comunidad Internacional las tendencias en ciberseguridad, en su aporte, sobre la evolución del Ransomware con finalidad de tipo malware, de

inmensa propagación en limpieza de discos y secuestro de datos con fines fraudulentos o la destrucción de estos, por motivos políticos. En virtud de que el activo a proteger es la Información Digital contenida en los sistemas de información, Harley ha recomendado las siguientes medidas, que disminuyen el riesgo en general:

Considera que en principio es mejor proteger los datos en forma proactiva que "confiar en la capacidad y buena fe de un delincuente", cuando se decide pagar rescate por los datos; asegura que el pago no implica recuperación de archivos; sostiene la necesidad de que policía e investigación trabajen unidos contra el cibercrimen y el Malware. Por otra parte, señala la importancia de realizar backups, en forma periódica, y mantener copias de seguridad offline en medios no expuestos habitualmente a ataques de ransomware u otro malware, principalmente en ubicaciones físicamente seguras, como discos ópticos y unidades flash. Aunque el almacenamiento esté fuera del sitio, si permanece "siempre encendido", su contenido puede ser vulnerable a las infecciones de ransomware, de la misma manera que el almacenamiento local. La recomendación es no permanecer en línea de manera habitual y proteger los datos almacenados cuando el centro remoto este on-line, de modo que un malware no pueda modificarlos o sobrescribirlos en forma automática o silenciosa.

Finalmente, muy importante, la recomendación del autor en relación con la necesidad de proteger de infecciones a las generaciones de datos anteriores. Esto con el objeto de recuperar, si ocurriera un ataque que afectara a los últimos backups, al menos algunos datos que incluyan las versiones anteriores de los datos actuales.

Desarrollar el tema de la ciberseguridad en el marco de un artículo como este, implica enormes limitaciones, dada la complejidad, multiplicidad y diversidad de interacciones e interconexiones que buscan no solo el logro de los objetivos de los diferentes activos (empresas), sino también la materialización de las amenazas crecientes a estructuras organizadas.

El propósito de la seguridad en todos los ámbitos en los que se aspira a aplicar, es reducir riesgos, hasta un nivel aceptable por gerencias y/o directivos. Sin embargo, la aspiración de lograr una seguridad libre de todo peligro, daño o riesgo, es utópica y por tanto, solo es una cuestión ideal, ya que fuera de lo teórico, en el terreno de la realidad no es posible tener certeza de que se pueden evitar todas las amenazas y riesgos.En este orden de ideas, la protección del patrimonio de activos, es un imperativo que hay que realizarse a través de una Gestión de Riesgos, que garantice la seguridad o al menos disminuya la posibilidad de la materialización de las amenazas.

## II. ENTORNOS Y ÁMBITOS DE CIBERSEGURIDAD

Parece recomendable, para facilitar la comprensión del concepto de Ciberseguridad, señalar algunos de los entornos o ámbitos del ciberespacio, en los que con las herramientas de la tecnología y con la presencia de una Red Informática (Internet), se puede disponer de todo tipo de información que navega por el ciberespacio. Es decir, al entorno de la seguridad de la información y de la seguridad informática, ilustrado en la figura 1, donde se han desarrollado los adelantos tecnológicos relacionados con la información y donde esta se comunica por Red Informática. Por encontrarse estos ámbitos en el ciberespacio, y desarrollar sus actividades en él, se comprende que la seguridad protegida en el mismo es la Ciberseguridad.

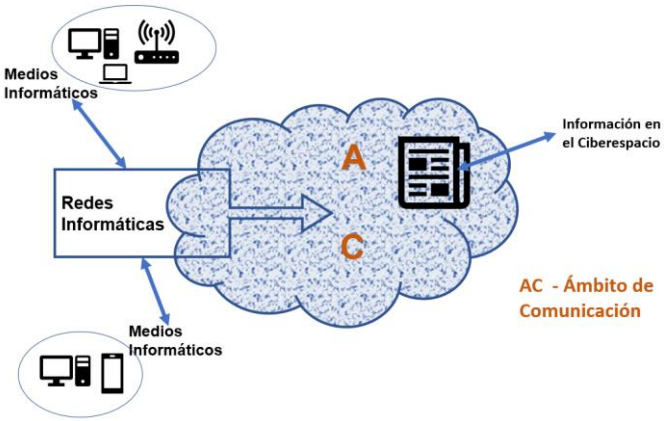


**Fig. 1**. Entornos y ámbitos de ciberseguridad
**Fuente**: Yaneth Linares Lizarazo

El prefijo ciber, comienza a generalizarse; se habla de ciber amenaza, y también de cibercriminal, ciberdelincuente, ciber riesgo, etc. Si observamos la figura, comprendemos que, para lograr la ciberseguridad en cualquiera de los ámbitos, se debe proteger el activo más importante de una organización, que es la información, lo que podría hacerse de forma correcta, dentro del proceso de la Gestión de Riesgos y buenas prácticas.

Consultando instituciones como ISACA, NIST, ISO, con su normatividad ISO 27001 e ISO 27032 se encuentra el aporte para desarrollar planes y proyectos encaminados a controlar y disminuir los riesgos que amenazan la ciberseguridad. Según ISACA Ciberseguridad es "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".

También se ha tomado como fuente de información, el Instituto Nacional de Estándares y Tecnología (NIST), de los Estados Unidos, Organización que recientemente, en abril del 2018 ha publicado el documento relacionado con el marco para mejorar la Ciberseguridad de la Infraestructura Crítica, y que es seleccionado como punto de referencia para desarrollar la Gestión de Riesgos de la Ciberseguridad.

La atención especial dada al documento referido, se debe no solamente a su actualización, (abril de 2018) sino, por la utilidad de sus aportes en el aspecto de la claridad con que son presentados. Igualmente, por la extensión de conocimientos, prácticas y metodologías que aportan, de una manera muy significativa la forma de desarrollar y llevar a cabo un buen procedimiento, para la gestión de riesgos por parte de una entidad u organización que quiera mantener las funciones de sus infraestructuras críticas, a la vez, que reconoce y recomienda la normatividad, las directrices y los estándares internacionales, reconocidos en el mundo y que han dado buenos resultados. Por lo anterior, es relevante, además, hacer una pequeña mención histórica acerca, de los antecedentes del NIST en relación con el tema que nos ocupa:

El Instituto Nacional de Estándares y Tecnologías de los EU da a conocer sus proyectos de Ciberseguridad en los años 2013-2014 y en abril del 2018 presenta un documento, en el que aporta el Marco de Ciberseguridad de la Infraestructura Crítica amenazada exponencialmente.

La Ley de mejora de la Ciberseguridad del año 2014 (CEA) actualizó el papel del Instituto Nacional de Estándares y Tecnologías, para "facilitar y apoyar el desarrollo de marcos de riesgo de ciberseguridad. A través de la CEA, el NIST debe identificar un enfoque priorizado, flexible, repetible, basado en el rendimiento y costo efectivo, que incluya medidas de seguridad de la información y controles que puedan ser adoptados voluntariamente por los propietarios y operadores de la infraestructura crítica, para ayudarlos a identificar, evaluar y administrar los riesgos cibernéticos". Posteriormente, la ley patriótica de los Estados Unidos del año 2015 define como infraestructura crítica, aquella conformada en "sistemas y activos, ya sean físicos o virtuales, tan importantes para los Estados Unidos, que la incapacidad o destrucción de dichos sistemas y activos, tendrá un impacto debilitador en la seguridad económica nacional, Salud Pública Nacional, seguridad o cualquier combinación de estos asuntos". Podría apreciarse lo anterior, en términos generales, como parte importante del contexto general del Marco de Referencia desde el cual el NIST se actualizó y se impulsó para concretar, en un documento trascendente, el Marco para mejorar la Ciberseguridad de la Infraestructura Crítica, versión 1.1 del 16 de abril del año 2018.

Los marcos de ciberseguridad construidos e identificados, pueden ser utilizados voluntariamente por propietarios y operadores de infraestructura crítica de la organización. Así mismo, su enfoque esta dirigido al uso de impulsores de negocios, con el objeto de guiar las actividades de ciberseguridad y considerar los riesgos de Seguridad Cibernética, como parte de los procesos de Gestión de Riesgos de la Organización.

El Marco de Ciberseguridad se desarrolló para mejorar la Gestión del Riesgo de Ciberseguridad en la Infraestructura Crítica, por tanto, el marco puede ser utilizado por organizaciones en cualquier sector o comunidad. La estructura del marco, posibilita a las organizaciones independiente de su tamaño, grado de ciberseguridad o sofisticación de ciberseguridad, aplicar los principios y mejores prácticas de gestión de riesgos, para mejorar la seguridad y la capacidad de recuperación. Proporciona, también una estructura de organización común para múltiples enfoques de ciberseguridad, mediante el ensamblaje de estándares, directrices y prácticas que funcionan de manera efectiva en la actualidad y hace referencia a normas reconocidas, mundialmente, para la ciberseguridad, por tanto, el marco puede servir como modelo para la cooperación Internacional, en el fortalecimiento de la ciberseguridad en infraestructura crítica, así como en otros sectores y comunidades.

Las partes que conforman el Marco, son el núcleo del marco, niveles de implementación y los perfiles del marco. Al Frame work core lo conforman un conjunto de actividades ligadas a la seguridad cibernética, a los resultados y referencias informáticas que son comunes en todos los sectores e infraestructuras críticas. Los elementos del núcleo que hacen parte de las actividades de seguridad, proporcionan una guía detallada para desarrollar perfiles organizacionales individuales. Por su uso, el marco tiene un significativo valor, al ayudar a una organización a priorizar y alinear sus actividades de seguridad cibernética, con sus seguimientos de negocios y misión, tolerancias de riesgos y recursos.

El marco es aplicable a organizaciones que dependen de la tecnología, ya sea que su enfoque de ciberseguridad sea principalmente en tecnología de la información (- TI, Sistemas de control industrial -ICS-, sistemas cibernéticos -CPS- sistemas ciber físicos) o dispositivos conectados en general, incluido el internet de las cosas.

En cuanto al vínculo del marco con las distintas organizaciones, tener en cuenta cómo las organizaciones continúan afrontando riesgos únicos, consistentes en diferentes amenazas, y diferentes vulnerabilidades, y diferentes tolerancias de riesgo, y cómo también varían en cómo personalizar las practicas descritas en el Marco. Por estas razones el Marco de Ciberseguridad no corresponde a un enfoque único para administrar el riesgo de seguridad cibernética. En última instancia, el objetivo principal del Marco consiste en reducir y gestionar mejor los riesgos de ciberseguridad.

Las organizaciones pueden voluntariamente utilizar el frame work de diferentes maneras, para tener en cuenta sus necesidades únicas de ciberseguridad. Es la organización implementadora, la que decide sobre cómo utilizarlo. Así, por ejemplo, una determinada organización, puede elegir utilizar

los niveles de implementación del marco para articular las prácticas de gestión de riesgos previstas, en tanto que otra organización puede utilizar las cinco funciones del marco para analizar toda su cartera de gestión de riesgos. El marco tiene utilidad como estructura e idioma para organizar y expresar los requisitos de ciberseguridad de una organización y está más allá de un simple cumplimiento.

Como quiera que el marco se ha creado para mejorar la Gestión de Riesgos de Ciberseguridad, en lo relacionado con la Infraestructura Crítica, puede ser utilizado por organizaciones de cualquier sector de la economía o de la sociedad. Así, su utilidad se puede dar en empresas, agencias gubernamentales, independientemente de un enfoque o tamaño.

La taxonomía común de estándares, directrices y practicas que proporciona, no es específica de un país. Las organizaciones de cualquier parte del mundo, también pueden usar el Marco para fortalecer sus propios esfuerzos de ciberseguridad y puede contribuir a desarrollar un lenguaje común para cooperar internacionalmente en infraestructura crítica de ciberseguridad.

## III. COMPONENTES Y DESCRIPCIÓN DEL MARCO

Los niveles de implementación del Marco – "Niveles" – determinan el contexto en el cual una organización tiene en cuenta el riesgo de seguridad cibernética y los procesos ya establecidos para gestionar el riesgo.

Los niveles describen los distintos grados de Ciberseguridad, que se pueden encontrar en las prácticas de Gestión de Riesgos y que las organizaciones podrían tener en cuenta, para desarrollar o mejorar su propio marco, cuyo nivel caracterizaría su práctica organizacional en un rango, desde parcial (nivel 1) hasta adaptativo (nivel 4).

Una organización debe considerar sus prácticas actuales de administración de riesgos, durante el proceso de selección de niveles; igualmente, hay que considerar el entorno de amenazas, los requisitos legales y reglamentos, así como los objetivos comerciales y de misión, y las limitaciones de la organización. Como conceptos básicos del marco tenemos:

Cuenta con un lenguaje común, que facilita comprender, gestionar y expresar el riesgo de seguridad cibernética, para las partes interesadas dentro y fuera de la organización. Su utilización, ayuda a la identificación, a la priorización de acciones encaminadas para reducir el riesgo de seguridad cibernética. El marco se convierte en una herramienta que permite alinear los enfoques, relacionados con políticas, negocios y tecnología, para darle manejo a ese riesgo.

También, puede ser utilizado el marco, con el objeto de administrar el riesgo de seguridad cibernética, en todas las organizaciones o bien, se puede enfocar en la entrega de los servicios críticos de una organización.

El Marco de Ciberseguridad, está construido con un lenguaje común, que puede ser comprendido en cualquier parte del mundo, y no solamente en los Estados Unidos. Significa esto, mejorar comunicación y por tanto mejor comprensión de su contenido, especialmente para comprender, gestionar y expresar el riesgo de seguridad cibernética.

El Marco se considera una herramienta global, específica, para alinear los enfoques políticos, de negocios y tecnológicos de una organización determinada, con el objeto de alcanzar metas con coordinación y coherencia.

Las funciones básicas del marco, deben realizarse concurrente y continuamente, para formar una cultura operativa que aborde el riesgo de ciberseguridad.

Las categorías son subdivisiones de una función, que se traducen en grupos de resultados de ciberseguridad, los cuales se encuentran adheridos a las necesidades y actividades de la misma. Ejemplo (Conciencia y entrenamiento, Seguridad de datos, Procesos y procedimientos de protección de la información, gestión de activos, evaluación de riesgos, etc.).

Las subcategorías permiten el logro de los resultados de cada una de las categorías, a través de actividades técnicas específicas, como establecer y comunicar las prioridades para la misión, los objetivos y las actividades de la organización.

Los roles y las responsabilidades, están coordinados y alineados con los roles internos y los socios externos, etc. En referencias informativas, se cuenta con unidades específicas, en donde se manejan una serie de normas, directrices y practicas comunes, en los sectores de Infraestructura Crítica, que revelan un método para lograr los resultados asociados con cada subcategoría.

## IV. PERFIL DEL MARCO

En el perfil del marco, están representados los resultados que se soportan en las necesidades comerciales que la organización ha escogido, de las categorías y subcategorías del marco. El perfil puede ser caracterizado como el enfoque de estándares o alineación, de estándares, directrices, y prácticas con el núcleo del marco en un escenario de implementación particular. Los perfiles pueden ser utilizados para identificar oportunidades, para mejorar la postura de ciberseguridad, comparando un perfil "Actual" (el estado "Tal cual") con un perfil de "objetivo" (el estado "a ser").

Para desarrollar un perfil, la organización en función de los impulsores de negocios / misión, puede revisar todas las categorías y subcategorías, y mediante una evaluación de riesgos, determinar cuáles son los más importantes para abordar los riesgos de la organización. Un perfil actual, se

puede usar para apoyar la priorización y la medición del progreso hacia el perfil objetivo.

## V. GESTIÓN DEL RIESGO Y MARCO DE CIBERSEGURIDAD

La Gestión del Riesgo se considera como un proceso continuo, que busca identificar, evaluar y dar respuesta al riesgo. Para desarrollar la Gestión de Riesgo, una organización debe comprender, para empezar, la probabilidad de ocurrencia de algún evento o suceso y los posibles impactos derivados del mismo; con la información de esta parte del proceso, se determinará el nivel aceptable de riesgo, para que la organización logre sus objetivos y esto, se puede expresar como tolerancia al riesgo. Si se tiene comprensión de la tolerancia al riesgo, hay la probabilidad de priorizar actividades de ciberseguridad, lo cual facilitará tomar decisiones sobre sus gastos. Por otra parte, la implementación de programas de Gestión de Riesgos aporta capacidad de cuantificar y comunicar los ajustes a sus programas de seguridad cibernética.

La organización puede manejar el riesgo de diferente manera: bien sea mitigando el riesgo, previniendo el riesgo, o la aceptación de este y según el impacto potencial en la prestación de los servicios críticos. El marco utiliza procesos de Gestión de Riesgos para permitir que las organizaciones informen y prioricen las decisiones relacionadas con la ciberseguridad.

## VI. FUNCIONES DEL MARCO

- Identificación: Busca una comprensión organizacional, que facilite entender los componentes reales y virtuales de una organización, para poder administrar con claridad y eficiencia, los riesgos de seguridad cibernética que puedan afectar sistemas, personas, activos, datos y capacidades que una organización posea.

  Las actividades en esta función son indispensables, para darle un uso efectivo al marco; es decir, que, con el buen uso de esta función, podemos comprender el contexto sobre el cual iremos a practicar las acciones respectivas, frente a los recursos que responden a las funciones críticas y los riesgos de seguridad cibernética que afectan o pueden afectar a la organización. Esto permite a la empresa enfocarse y priorizar sus esfuerzos de manera consistente y coherente, con su estrategia de gestión de riesgos y sus posibilidades comerciales. “La gestión de activos, ambiente de negocios, gobernanza y evaluación de riesgos constituyen ejemplos de categorías de resultados de esta función.”

- Proteger: se basa en el desarrollo y la implementación de medidas de seguridad, adecuadas, enfocadas a garantizar la entrega de servicios críticos y tener capacidad en determinadas circunstancias, de limitar o contener el impacto de un posible evento, o suceso de ciberseguridad.

  Para el logro de buenos resultados, con esta función, se debe incluir en su desarrollo, medidas de seguridad, como gestión de identidad y control de acceso, conciencia y entrenamiento; seguridad de datos, procesos y procedimientos de protección de la información, mantenimiento y tecnología de protección. Todo lo anterior, se puede traducir como resultados de diversas categorías, de prácticas y comportamientos.

- Detectar: Esta función permite el descubrimiento oportuno de eventos de ciberseguridad; para cumplir con sus objetivos, debe desarrollar e implementar actividades que sean necesarias, para identificar la ocurrencia de eventos de ciberseguridad. Los resultados de la función, los podemos categorizar, por ejemplo, con la detección de anomalías y eventos; con los efectos de un monitoreo continuo de seguridad y el desarrollo de procesos de seguridad.

- Responder: Esta función desarrolla e implementa actividades estratégicas, o planes adecuados de resiliencia que permitan restaurar cualquier capacidad o servicio que se haya visto afectado, debido a un incidente de ciberseguridad. Como categorías de resultados, en esta función, tenemos por ejemplo la planificación de recuperación, mejoras y comunicaciones.

### Niveles de Implementación del Marco

El nivel de implementación del marco ilustra, sobre el contexto desde el cual una organización, considera el riesgo de ciberseguridad y los procesos que se han establecido, para gestionarlo. Son múltiples los aspectos de ciberseguridad que se consideran en la Gestión de Riesgos, incluido el grado en que la consideración de privacidad y libertades civiles, se integran en la gestión de riesgos de ciberseguridad en una organización.

### Selección de Niveles del Marco de Ciberseguridad

Seleccionar el nivel del marco, es un proceso que debe tomar en cuenta las prácticas actuales de Gestión de Riesgos; el ámbito de amenazas y riesgos, los requisitos legales y la normatividad regional e internacional. El nivel deseado es determinado por la correspondiente organización, asegurando el cumplimiento de sus objetivos y que sea posible implementar y disminuir el riesgo de ciberseguridad a los activos y recursos críticos a niveles aceptables o tolerables para la empresa.

Un nivel de madurez, no esta representado en los niveles de un marco de ciberseguridad, ya que su finalidad, es respaldar la toma de decisiones con relación a cómo gestionar el riesgo de ciberseguridad. Cuando la relación costo - beneficio indica una reducción factible y económica del riesgo de

ciberseguridad, esta circunstancia fomenta la progresividad a un marco de ciberseguridad más alto.

**Definiciones de Niveles**

A continuación, se presentan solamente los niveles 1 y 4, los cuales podrían contrastar las condiciones de capacidad de una organización, para desarrollar de forma correcta la Gestión de Riesgos, ajustada a los principios y normas internacionales que garanticen, las mejores prácticas en estrategias de ciberseguridad; los niveles 2 y 3 son posiciones intermedias entre los niveles 1 y 4.

**Nivel 1 Parcial**

Proceso de Gestión de Riesgos: Las prácticas de gestión de riesgos de ciberseguridad, se realizan ad-hoc, puesto que no están formalizadas aún. Las priorizaciones de actividad cibernética pueden no estar directamente informada, por los objetivos de riesgo de la organización.

Programa Integrado de Gestión de Riesgos: el conocimiento sobre el riesgo de ciberseguridad en la organización, es muy limitado y la implementación del mismo, por tanto, es irregular.

Participación externa: la participación no existe, pues ni colabora, ni recibe información. Así, no hay probabilidad de recibir inteligencia sobre amenazas, mejores prácticas o tecnología.

**Nivel 4 Adaptable**

Proceso de Gestión de Riesgos: La organización gestiona sus practicas de ciberseguridad, soportadas en actividades de ciberseguridad anteriores y actuales, incluidas las lecciones aprendidas y los indicadores predictivos. A través de un proceso, de mejora continua, que incorpora prácticas y tecnologías avanzadas de ciberseguridad, la organización se adapta activamente a un panorama cambiante, de amenazas y tecnología, y responde de manera oportuna y efectiva a las amenazas cambiantes y sofisticadas.

Programa Integrado de Gestión de Riesgos: Existe un enfoque de toda la organización para gestionar el riesgo de ciberseguridad que se vale de políticas, procesos y procedimientos informados, sobre riesgos, para afrontar posibles eventos de ciberseguridad. La relación entre los objetivos o fines de la organización y el riesgo de ciberseguridad, se entiende y se tiene en cuenta, con claridad, al tomar decisiones.

Los ejecutivos de alto nivel de la empresa, monitorean el riesgo de ciberseguridad, en el mismo contexto que el riesgo financiero y otros riesgos organizacionales. El presupuesto de la organización se basa en la comprensión del entorno del riesgo actual, y previsto, y la tolerancia al riesgo. Por otra parte, las unidades de negocios implementan la visión ejecutiva y analizan los riesgos a nivel del sistema en el contexto de las tolerancias de riesgo organizacional.

La gestión de riesgos de ciberseguridad es parte de la cultura organizacional, y evoluciona a partir de la conciencia de las actividades previas y la conciencia continua de las actividades en sus sistemas y redes. La organización puede dar cuenta de forma rápida y eficiente, de los cambios en los objetivos empresariales y de misión, y en la forma en que se aborda y comunica el riesgo.

- Participación externa: La organización entiende su función, sus dependencias y sus dependientes, en un ecosistema más amplio y contribuye a una mayor comprensión de los riesgos, por parte de la comunidad. Recibe, genera y revisa información priorizada que informa el análisis continuo de sus riesgos a medida que evolucionan los paisajes de amenazas y tecnología. La organización comparte esa información interna, externamente, con otros colaboradores. Igualmente, la organización utiliza información en tiempo real o casi tiempo real, para comprender y actuar de forma coherente, sobre los riesgos de la cadena de suministro cibernética asociados, con los productos y servicios que proporciona y que utiliza.

Además, se comunica de forma proactiva, utilizando mecanismos formales (acuerdos) e informales para desarrollar y mantener relaciones solidas en la cadena de suministros.

**Coordinación de la Implementación del Marco**

La administración del riesgo se desarrolla, mediante un flujo común de información y decisiones en los niveles ejecutivo, procesos de negocios e implementación y operaciones de una organización, de acuerdo con lo ilustrado en la figura 2.

El nivel ejecutivo decide y comunica las prioridades de la misión; los recursos disponibles y la tolerancia al riesgo general al nivel de negocio y proceso. Este nivel de negocio utiliza la información como entradas en el proceso de gestión de riesgos, y luego colabora con el nivel de implementación y operaciones del negocio y crea un perfil. Enseguida, el nivel implementación y operaciones comunica el progreso de la implementación del perfil al nivel de negocio y proceso. Ahora, el nivel de negocio y proceso utiliza esta información para realizar una evaluación de impacto.

Finalmente, la administración de nivel de negocios y procesos, informa los resultados de esa evaluación del impacto, al nivel ejecutivo, para informar el proceso general de gestión de riesgos de la organización y el nivel de implementación y operaciones para la conciencia del impacto comercial. (fig. 2)

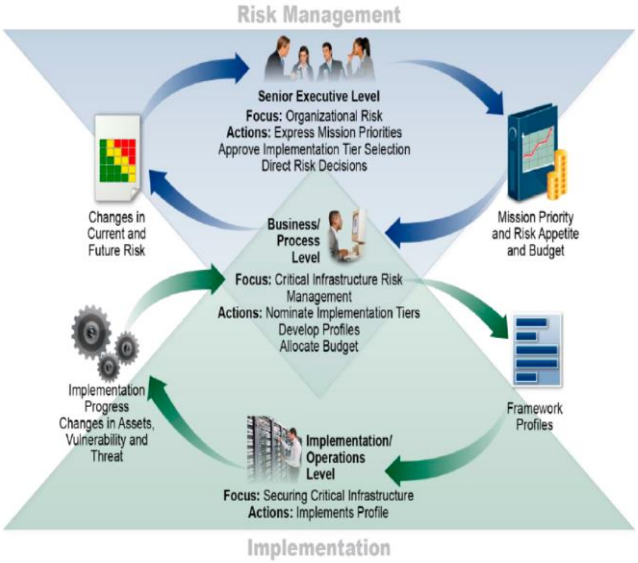


**Fig. 2**. Información nocional y flujos de decisión dentro de una organización.
**Fuente**: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 National Institute of Standards and Technology April 16, 2018

## VII. COMO USAR EL MARCO

El Marco de Ciberseguridad proporciona un medio para expresar los requisitos de ciberseguridad a los socios comerciales y clientes. Está diseñado para complementar las operaciones comerciales y de ciberseguridad existentes. Puede ser utilizado como una parte clave o esencial de su proceso sistemático para identificar, evaluar y administrar el Riesgo de Ciberseguridad. El Marco no esta diseñado para reemplazar los procesos existentes; una organización puede usar su proceso actual y superponerlo en el marco. Para determinar las brechas en su enfoque actual de Riesgo de Ciberseguridad y desarrollar una hoja de ruta hacia la mejora. El marco puede servir como base de un nuevo Programa de Seguridad Cibernética o un mecanismo para mejorar un programa existente; utilizándolo como una herramienta de Gestión de Riesgo de seguridad cibernética, puede ayudar a identificar lagunas en la práctica de ciberseguridad de una organización. Además, el marco proporciona un conjunto general de consideraciones y procesos para considerar las implicaciones de privacidad y libertad civil en el contexto de un Programa de Seguridad Cibernética, y puede ser aplicado en las fases del ciclo de vida del plan representadas en el diseño, construcción y compra, implementación, operación y desmantelamiento.

Las consideraciones generales de Seguridad Cibernética, deben ser declaradas y descritas con la mayor claridad posible. Por otra parte, el plan debe reconocer que es probable que esas consideraciones y requisitos evolucionen durante el resto del ciclo de vida.

La fase del plan de diseño, inicia el ciclo de cualquier sistema y sienta las bases para todo lo que sigue; por otra parte, debe tenerse en cuenta los requisitos de ciberseguridad, como parte de un proceso de Ingeniería de Sistemas multidisciplinario, más grande.

Una red compleja de dependencias (por ejemplo, controles comunes y de compensación), entre sistemas, significa que los resultados documentados, en los perfiles de objetivos de los sistemas relacionados, deben considerarse cuidadosamente, a medida que los sistemas se desmontan. Un hito clave, de la fase de diseño, es la validación de las especificaciones de ciberseguridad, para que coincidan con las necesidades y la disposición de riesgo del perfil de la organización. Los resultados deseados de ciberseguridad priorizados en un perfil objetivo, deben incorporarse cuando se desarrolle el sistema durante la fase de construcción o cuando se compre o externalice un sistema durante la fase de compra. Ese mismo perfil de destino (objetivo), sirve como una lista de características de ciberseguridad y determinadas mediante el uso del marco, y que deberían servir como base para la operación continua del sistema; esto incluye, reevaluaciones ocasionales, captura de resultados en un perfil actual, para verificar que los requisitos de ciberseguridad aún se cumplan.

Las organizaciones pueden utilizar el marco, mediante la revisión básica de las prácticas de ciberseguridad, el establecimiento o mejora de un Programa de Ciberseguridad o mediante la comunicación de los requisitos de ciberseguridad con los interesados.

### Revisión básica de las Prácticas de Ciberseguridad

El Marco de Ciberseguridad puede ser utilizado, para hacer una comparación de las actuales actividades de ciberseguridad, de una organización, con aquellas delineadas en el marco de ciberseguridad y el marco actual de la organización. Las organizaciones que quieran saber en qué medida están logrando los resultados descritos, en las categorías principales y subcategorías alineadas con las cinco funciones de alto nivel, deben crear un perfil actual. Para tener claridad sobre este aspecto, se tiene en cuenta, las funciones de alto nivel, que son: identificar, proteger, detectar, responder, y recuperar; la organización puede descubrir que ya esta logrando el objetivo deseado, de los resultados. De acuerdo con lo anterior, la organización puede usar esa información para desarrollar un plan de acción, que fortalezca las prácticas existentes, de ciberseguridad, y reduzca, por tanto, el riesgo de la misma.

Por otra parte, las cinco funciones de alto nivel, no reemplazan un Proceso de Gestión de Riesgos, pero si tienen capacidad para proporcionar información, de forma concisa, para que los altos ejecutivos y otros, estén en capacidad de emitir los conceptos fundamentales del Riesgo de Ciberseguridad, y para que puedan evaluar comó se gestionan los riesgos identificados y cómo se acumula su organización, de alto nivel, en comparación con los estándares, directrices y prácticas de ciberseguridad existentes a nivel mundial.

### Establecimiento o mejoras de un Programa de Ciberseguridad

Las organizaciones pueden utilizar el marco para crear un nuevo programa de ciberseguridad, o mejorar el existente o actual. Para eso, ha de seguir los siguientes pasos:

**Paso 1.** Prioridad y alcance: La organización toma decisiones estratégicas en relación con las implementaciones de ciberseguridad y determina el alcance de los sistemas y activos que respaldan la línea o proceso comercial seleccionado. Para lo anterior, la organización identifica sus objetivos de negocio, misión y las prioridades organizacionales de alto nivel.

**Paso 2. Orientar:** Determinado el alcance, del Programa de Seguridad Cibernética y alineado en negocios o en el proceso, la organización identifica los sistemas y activos relacionados, los requisitos reglamentarios y el enfoque del riesgo general. Luego consulta las fuentes para identificar las amenazas y las vulnerabilidades aplicables a esos sistemas y activos.

**Paso 3. Crear un perfil actual:** Al indicar qué resultados de categoría y subcategoría del núcleo del marco se están logrando actualmente, la organización desarrolla un perfil actual. Si se logra parcialmente un resultado, tomar nota de este hecho, ayudará a respaldar los pasos posteriores, al proporcionar información de referencia.

**Paso 4. Realizar una evaluación de riesgos:** El proceso de gestión de riesgos general, de la organización, podría ser guía de esta evaluación o por actividades previas de la evaluación de riesgos. Para que la organización discierna la probabilidad de un evento de ciberseguridad y el impacto que el evento podría tener en la organización, debe analizar el entorno operativo. Es importante, que las organizaciones identifiquen los riesgos emergentes y utilicen la información de amenazas de ciberseguridad, de fuentes tanto internas como externas, para obtener una mejor comprensión de la probabilidad y el impacto de los eventos de ciberseguridad.

**Paso 5. Crear un perfil de destino (objetivo):** Ese perfil objetivo, creado por la organización, se centra en la evaluación de las categorías y subcategorías del marco, que describen los resultados deseados de ciberseguridad de la organización.

Igualmente, las organizaciones pueden desarrollar sus propias categorías adicionales y subcategorías lo que le permitirán tener en cuenta los riesgos únicos de la organización. También puede considerar las influencias y requisitos de las partes internas y externas, como las entidades del sector, los clientes y los socios comerciales, al crear un perfil objetivo.

**Paso 6. Determinar, analizar y priorizar brechas:** Para determinar las brechas, la organización debe hacer una comparación entre el perfil actual y el perfil objetivo. A continuación, crea un plan de acción priorizado, para abordar las lagunas que reflejan los impulsores, los costos y los beneficios de la misión, y los riesgos, para lograr los resultados en el perfil objetivo. Después, la organización debe determinar los recursos, incluidos los fondos y la fuerza laboral, necesarios para abordar las lagunas.

**Paso 7. Implementar un plan de acción:** La organización debe abordar las brechas si las hay, y luego ajustar sus prácticas actuales de ciberseguridad para lograr el perfil objetivo. Para obtener más orientación, el marco identifica ejemplos de referencias informativas, sobre las categorías y subcategorías, pero las organizaciones deben determinar qué normas, directrices y prácticas, incluidas aquellas que son específicas del sector, y que funcionan mejor para sus necesidades.

Según sea necesario, para evaluar y mejorar continuamente su ciberseguridad, la organización repetirá los pasos. Así, las organizaciones, pueden encontrar que una repetición más frecuente del paso orientar, mejora la calidad de las evaluaciones de riesgos. También, las organizaciones pueden monitorear el proceso a través de actualizaciones iterativas al perfil actual, y luego comparar el perfil actual, con el perfil objetivo. Igualmente pueden utilizar este proceso, para alinear su Programa de Ciberseguridad con su nivel de implementación del Marco de Ciberseguridad.

### Comunicar los Requisitos de Ciberseguridad con los Interesados

Los requisitos de la ciberseguridad son proporcionados por el marco, mediante un lenguaje común, con el cual se comunica con las partes interesadas interdependientes, responsables de la entrega de productos y servicios esenciales, de la Infraestructura Crítica. Algunos ejemplos relacionados con lo anterior incluyen:

El que una organización pueda utilizar el perfil de destino, para expresar los requisitos de gestión del riesgo de ciberseguridad a un proveedor de servicios externo, o la posibilidad de utilizar de igual manera un perfil actual, para expresar su estado de ciberseguridad, informando resultados o comparando con los requisitos de adquisición. Igualmente, el propietario y operador de una infraestructura crítica, al haber identificado un socio externo del que depende esa infraestructura crítica; igualmente puede usar un perfil de destino que se puede establecer dentro de sus componentes, como un perfil de referencia, para construir sus perfiles de destino personalizados.

Un ejemplo final, de la comunicación de requisitos de ciberseguridad, es que las organizaciones pueden gestionar mejor el riesgo de ciberseguridad, entre las partes interesadas, mediante la evaluación de su posición en la Infraestructura

Crítica y la Economía Digital más amplia.

Las cadenas de suministro, comienzan con el suministro de productos y servicios; y se extienden desde el diseño, desarrollo, fabricación, procesamiento, manejo y entrega de productos y servicios, hasta el usuario final. Dadas estas relaciones complejas e interconectadas, la Gestión del Riesgo de la Cadena de Suministros (SCRM) es una función organizativa crítica. La comunicación es fundamentalmente importante entre las partes interesadas hacia arriba y hacia abajo de las cadenas de suministro.

El ciber SCRM aborda tanto el efecto de ciberseguridad que una organización tiene en las partes externas, como el efecto de ciberseguridad que las partes externas tienen en una organización; y en términos generales el Ciber SCRM es el conjunto de actividades necesarias para gestionar el riesgo de ciberseguridad asociado con partes externas. También, un objetivo principal del Ciber SCRM es identificar, evaluar y mitigar, "productos y servicios, que pueden contener funcionalidad potencialmente maliciosa, que sean falsificados o sean vulnerables, debido a malas prácticas de fabricación y desarrollo dentro de la cadena de suministro cibernético". (publicación especial NIST 800-161).

Entre las actividades del Ciber SCRM se pueden incluir:

Determinar los requisitos de ciberseguridad para los proveedores, luego promulgarlos mediante un acuerdo formal (por ejemplo, contratos); de la misma manera, comunicarles la forma de verificar y validar esos requisitos de ciberseguridad; Así, mismo, se deberá verificar el cumplimiento de los mismos, a través de una metodología de evaluación, y finalmente, realizar acciones concernientes a gobernar y administrar las actividades anteriores.

Para ampliar la comprensión del Ciber SCRM, hay que señalar que este abarca proveedores y compradores de la tecnología, así como proveedores y compradores no tecnológicos, en donde la tecnología se compone mínimamente, de Tecnología de la Información (TI), Sistemas de Control Industrial (ICS), Sistemas Ciber Físicos (CPS) y dispositivos conectados en general, incluido el Internet de las Cosas (IOT).

Las partes descritas anteriormente, hacen parte del Ecosistema de Ciberseguridad de una organización. Sus relaciones hacen sobresalir, el papel crucial del Ciber SCRM para abordar el Riesgo de Ciberseguridad en la Infraestructura Crítica y la Economía Digital más amplia. Las mismas relaciones anteriores, los productos y servicios que brindan y los riesgos que presentan, deben identificarse y tenerse en cuenta en las capacidades de protección y detección de las organizaciones, así como sus protocolos de respuesta y recuperación.

El significado de "comprador", se refiere a las personas u organizaciones descendentes, que consumen un determinado producto o servicio de una organización, con o sin fines de lucro. El "proveedor", incluye proveedores de productos y servicios, en sentido ascendente, que se utilizan para los objetivos internos de una organización (infraestructura de TI) o integrados en los productos o servicios proporcionados al comprador. Estos términos pueden ser aplicados para productos y servicios basados en tecnología, como no basados en tecnología.

El marco ofrece a las organizaciones y sus socios, un método para ayudar a garantizar que el nuevo producto o servicio cumplan los resultados críticos de ciberseguridad. Los anteriores requisitos se ilustran en la fig. 3.

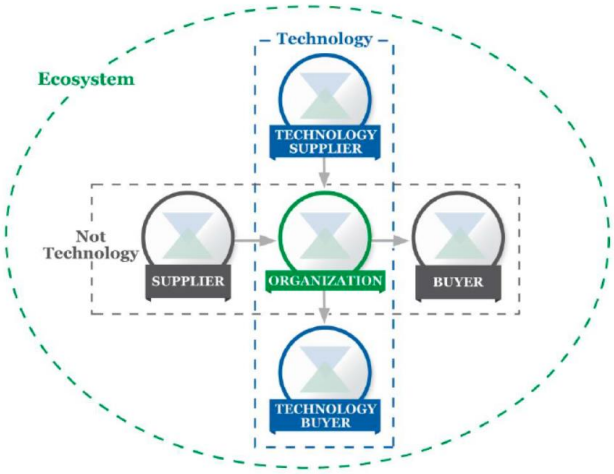


**Fig. 3**. Relaciones de ciber Cadena de Suministro
**Fuente**: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 National Institute of Standards and Technology April 16, 2018

**Decisiones de Compra**

Los perfiles objetivo de una organización pueden ser utilizados para informar las decisiones, sobre la compra de productos y servicios. La comunicación de los requisitos de ciberseguridad a las partes interesadas, varían, ya que no es posible imponer un conjunto de requisitos de ciberseguridad al proveedor. Entre múltiples proveedores, el objetivo de la organización debe ser el de tomar la decisión de compra, teniendo en cuenta una lista cuidadosamente determinada de requisitos de ciberseguridad; esto significa, con frecuencia, un determinado grado de compensación al comprar múltiples servicios o productos con vacíos conocidos en el perfil objetivo.

Comprado un producto o servicio, el perfil también se puede utilizar para rastrear y abordar el riesgo de ciberseguridad residual, por ejemplo, si el servicio o producto adquirido no cumplió con todos los objetivos descritos. En el perfil de objetivos, la organización puede abordar el riesgo residual a través de otras acciones de gestión. Adicionalmente, el perfil

brinda a la organización un método, para evaluar si el producto cumple con los resultados de ciberseguridad, mediante revisiones y pruebas periódicas.

**Autoevaluación del Riesgo de Ciberseguridad con el Marco**

El Marco de Ciberseguridad se ha diseñado para mejorar la Gestión de Riesgo de Ciberseguridad. Con esto, se busca reducir riesgos para los objetivos de la organización. Cuando esta utiliza el marco, podrán medir y asignar valores a su riesgo junto con el costo y beneficios de los pasos tomados para reducir el riesgo a niveles adaptados. En cuanto mayor capacidad tenga una organización para medir sus riesgos, costos y beneficios de las estrategias y pasos de ciberseguridad, más racional, eficaz y valioso será su enfoque e inversiones en Ciberseguridad.

En relación a la efectividad de las inversiones, la organización, para examinarla, debe comprender con claridad, sus objetivos organizacionales; la relación entre dichos objetivos y los resultados de ciberseguridad de apoyo y de los administrativos.

## VIII. GESTIÓN DE RIESGOS DE LA CIBERSEGURIDAD

Para terminar de considerar los aspectos generales de la ciberseguridad, fuera del país, se busca una aproximación a la forma de desarrollar una Gestión de Riesgos, teniendo como base, para ello, el aporte dado por el Instituto Nacional de Ciberseguridad de España (INCIBE), el cual basa sus orientaciones generales en la ISO 27005 e ISO 31000 y que también se han tenido en cuenta como fuente de información en este artículo.

Las grandes revoluciones que se han dado, especialmente en la segunda mitad del siglo veinte y que tienen que ver con la progresiva transformación del mundo, en especial en el área económica, científica y tecnológica, se ha debido especialmente a la utilización de la ultima en el campo de la información digital. No obstante, lo anterior, que es reflejo del beneficio recibido por las organizaciones mundiales, se debe reconocer, que hay aspectos negativos que las amenazan, especialmente en los últimos tres a cinco años y que tienen que ver con los riesgos y amenazas, a que han sido sometidos los activos de la información, con lo cual disminuyen el desarrollo de las metas y objetivos de dichos activos.

Organizaciones Internacionales, de reconocida autoridad, han aportado para evitar o disminuir esos riesgos o amenazas, la metodología para desarrollar un proceso de carácter continuo y de permanente revisión, que sea capaz de dar protección a los activos que tengan la posibilidad de sufrir sucesos o acontecimientos que conlleven grandes consecuencias para dichas organizaciones. Tal proceso se ha denominado la Gestión de Riesgos para la seguridad o Gestión de Riesgos para la Ciberseguridad.

Dentro de este contexto general, el activo principal de la empresa es el activo de la información digital, el cual, a través del proceso enunciado, será protegido en sus dimensiones de la seguridad de la información, es decir, en su confidencialidad, su integridad y su disponibilidad, que son los elementos esenciales a proteger por parte de la seguridad, incluyendo, además, la infraestructura informática, las redes de comunicaciones, equipos auxiliares, instalaciones y personas.

Es importante observar que cuando hablamos de la ciber información, esta puede encontrarse en diferentes ámbitos o entornos; así, por ejemplo, si buscamos proteger el software, nos estamos refiriendo básicamente al medio por el cual fluye la información; y si nos referimos al hardware, estaríamos refiriéndonos a la infraestructura tecnológica o servicios y nos encontraríamos entonces, en el ámbito de la seguridad informática o ciberseguridad. Por su parte, actividades de seguridad de personas y seguridad física, cumplimiento o comercialización nos referimos a seguridad de la información.Todo esto, significa que tratándose de la seguridad o de la ciberseguridad de la información, no se puede contar con un lugar específico y único, donde esta se desarrolla y puede ser gestionada.

**Acciones de Comunicación**

La gestión del riesgo, se caracteriza por la necesidad de desarrollar una serie de acciones, tanto internas como externas, que permitan la mejor comunicación tanto vertical como horizontal; entre estas se encuentran la necesidad de identificar riesgos, de valorarlos en función de consecuencias y su probabilidad de ocurrencia. Seleccionar prioridades del tratamiento de los riesgos y monitorizarlos, para confrontar su efectividad; el proceso mismo debe ser revisado, regularmente y monitorizado y la gestión del proceso de gestión ha de ser informada a la gerencia de la dirección.

**Contexto de la Seguridad de la Información**

Definido el contexto o ámbito en el que va a actuar la Ciberseguridad, se han de desarrollar, una serie de actividades, sujetas al cumplimiento de normas o principios, entre ellas la necesidad de definir criterios básicos, para la Gestión de Riesgos de la seguridad de la información o de la ciberseguridad; otro aspecto importante, es la valoración de las posibles consecuencias de los riesgos.

**Criterios para Evaluación de Riesgos**

Se recomienda determinar cuales son los activos de información críticos; su importancia en cuanto a confidencialidad, integridad y disponibilidad. El valor estratégico de procesos de información de la organización, niveles de clasificación de los impactos, escala de afectación de los riesgos y a que parte de la organización afectan preferencialmente.

**Valoración de los Riesgos de la Ciberseguridad**

Se considera, esta la fase central o medular del Proceso de Gestión de Riesgos. Se considera en esta fase, la identificación, el análisis y la evaluación. Los riesgos se identifican para ser evaluados, en seguridad de la información:

Lo primero que se debe hacer, es identificar los activos de la información; en seguida, conocer las amenazas que pueden llegar a materializarse y producir daños en la información, en los procesos y en los soportes. Para valorar los daños que puedan producirse, es necesario identificar activos con ayuda de preguntas como las siguientes:

¿Qué valor tiene este activo para la organización?, ¿Cuánto cuesta su mantenimiento, y como repercute en los beneficios?, ¿Cuánto costaría recuperarlo o volverlo a generar?, ¿Cuánto costó adquirirlo?. Con el listado de activos, con sus amenazas y con las medidas tomadas se pasará luego a revisar las vulnerabilidades.

**Vulnerabilidades**

Amenazas más vulnerabilidades, nos da un resultado matemático que es igual al daño. En cada amenaza, hay que identificar y analizar vulnerabilidades. La norma ISO 27005 incluye anexo con ejemplo de vulnerabilidades y amenazas.

Finalmente, se deben conocer las consecuencias, es decir, cómo estas amenazas y vulnerabilidades afectan a la disponibilidad, integridad y confidencialidad de los activos de información.

**Evaluación de los Riesgos**

Dadas las consecuencias o impacto y las probabilidades de los sucesos para los activos del ámbito elegido, se debe realizar el producto de ambos para calcular los riesgos.

**Tratamiento y Aceptación de Riesgos de Ciberseguridad**

Con el conocimiento de los riesgos, se debe situar la "línea roja" del umbral o nivel de tolerancia al riesgo. En esta fase se selecciona la opción de tratamiento: evitar, reducir o mitigar, transferir o aceptar; para cada uno de los riesgos de la lista, tendrá que haber una elección de opciones, o una combinación de ellas. Se considera no solo la valoración obtenida para cada riesgo, sino también, el costo de tratamiento; nos preguntaríamos, por ejemplo, si será mejor evitar un riesgo, que mitigarlo; si el costo es muy alto, se consideran como opciones preferidas, aquellas que aportan reducción considerable del riesgo de la manera más económica.

**Nivel de Tolerancia del Riesgo**

El nivel de la tolerancia del riesgo, se establece en base de criterios costo – beneficio. Si el costo es mayor que el beneficio la recomendación es evitar el riesgo, y si el costo del tratamiento es adecuado, se debería reducir o mitigar el riesgo, seleccionando o implementando los controles o medios adecuados que hagan reducir la probabilidad o el impacto.

Se ha considerado que el tratamiento hecho por terceros es más beneficioso; ejemplo de este caso se puede encontrar, si hay transferencia, contratando, por ejemplo, un seguro, o subcontratando el servicio. Si el nivel del riesgo esta muy alejado del nivel de tolerancia, el tratamiento sería, retenerlo o aceptarlo, sin implementar controles adicionales, pero seria recomendable monitorizarlo para confrontar que no se incremente.

**Reducir o mitigar el riesgo**

En esta circunstancia, para ello, hay que desarrollar acciones, como las siguientes: Instalar productos o contratar servicios; establecer controles de seguridad, mejorar procedimientos, cambiar el entorno o incluir métodos de detección temprana.

La implantación, de un plan de contingencia y continuidad, y la realización de formaciones y sensibilidades, son de gran importancia; la estabilización de controles se convierte en medidas de protección para reducir el riesgo. La norma ISO 27000:2013 incluye lista de controles de aplicación a la mayoría de las organizaciones. El resultado de esta fase, se conecta a un plan de tratamiento de riesgos o sea la selección y justificación de una o varias opciones, para cada riesgo justificado. A este plan se agregará una relación de riesgos residuales, entendiendo por tales, aquellos que siguen existiendo a pesar de las medidas tomadas.

**Los Riesgos**

Es importante señalar, que los riesgos no son estáticos y por tanto pueden cambiar de forma radical e imprevisible; de ahí la necesidad de supervisión continua, que detecte: nuevos activos o modificación de su valor; nuevas amenazas, cambios o aparición de nuevas vulnerabilidades. También el aumento de las consecuencias o impactos e incidentes de la seguridad de la información, son situaciones que representan cambios.

**Revisar el propio Sistema de Gestión**

De manera análoga, se revisa el propio sistema de gestión: las categorías de activos, los criterios de evolución de riesgos y los niveles de clasificación de los impactos; junto con las escalas de aceptación de riesgos, y los recursos necesarios constituyen una forma de revisión del mismo proceso de gestión.

**Resultado de la Gestión de Riesgos**

La identificación de los riesgos y su manera de tratarlos, se convierte en un buen comienzo para gestionar la Ciberseguridad de la información, en el ámbito de las organizaciones. Instituto Nacional de Ciberseguridad España (INCIBE).

## IX. LA CIBERSEGURIDAD EN COLOMBIA

El enfoque principal que tienen en cuenta las instituciones en Colombia, se relaciona con la Gestión de Riesgos de Ciberseguridad, desde la perspectiva de la protección de los activos, objetivos y misión de las organizaciones, que han estado amenazados y que constituyen la incertidumbre de las mismas. Sus ciudadanos y organizaciones nacionales están inmersos en el entorno del progreso digital; pero esta circunstancia, igualmente, la han colocado frente a las amenazas y riesgos derivados de las actividades de los cibercriminales o ciberdelincuentes.

Colombia ha sido considerada, como uno de los países líderes en el ámbito de la ciberseguridad en Latinoamérica.

Recientemente, la Política Nacional de Ciberseguridad, ha tenido como estrategia el desarrollo de actividades centralizadas, básicamente, en las fuerzas del Estado, para la protección del país, con énfasis en la Defensa Nacional, pero sin justificación para no dar la importancia debida a las múltiples partes interesadas, que son las promotoras del progreso en el Marco de la Economía Digital.

Las amenazas, riesgos, vulnerabilidades y el riesgo de seguridad digital, han aumentado paralelamente con el desarrollo del progreso. Como en otras partes del mundo, también han aumentado los malware en todos los sectores, lo que implica altos costos de las actividades maliciosas y con afectación de la Infraestructura Crítica. Los lineamientos de políticas para ciberseguridad y ciber defensa de 2011 al 2015 fueron determinados por la Comisión Nacional Digital y de Infraestructura Estatal (Decreto 32 de 2013).

En 2014 y 2015 se realizaron mesas de trabajo con expertos Nacionales e Internacionales, para analizar el estado de la política vigente. En el momento, la política vigente en Colombia, con relación a la Ciberseguridad, se ha estructurado teniendo en cuenta las recomendaciones hechas por la (OCDE) Organización para la Cooperación y el Desarrollo Económico, el 17 de septiembre del 2015 y con las cuales la república de Francia actualizó su Política de Seguridad Nacional en octubre del mismo año. Por la anterior razón, el Marco de Seguridad Digital de Colombia tiene en cuenta entre las mejores prácticas, adoptar el enfoque de Gestión de Riesgos, estimular la prosperidad económica y social, adoptando una posición que tenga en cuenta la dimensión de lo técnico, lo jurídico, lo económico y social, y salvaguardando los derechos humanos, y protegiendo valores nacionales. También adopta enfoques relacionados con las múltiples partes interesadas. Podemos entonces establecer, que las políticas y estrategias nacionales, se han basado en las recomendaciones hechas no solamente por la OCDE, sino también, por las directrices emanadas de otras organizaciones internacionales, como la Organización de Estados Americanos OEA, la Organización del Tratado del Atlántico Norte - OTAN, la International Telecommunication Union y la Information Technology Industry Council, que en su conjunto puede considerarse que sus directrices han consensuado la importancia de la economía digital, en el mundo actual, y la necesidad de plantear estrategias y políticas orientadas a protegerlas. La OCDE plantea la necesidad de abordar la problemática, bajo la óptica de la seguridad digital, desde la perspectiva de la "prosperidad económica y social", bajo un enfoque multi stakeholder, que implemente un conjunto de principios y adopte una estrategia nacional, de gestión de riesgos.

En la figura 4, se ilustra las recomendaciones de la OCDE.

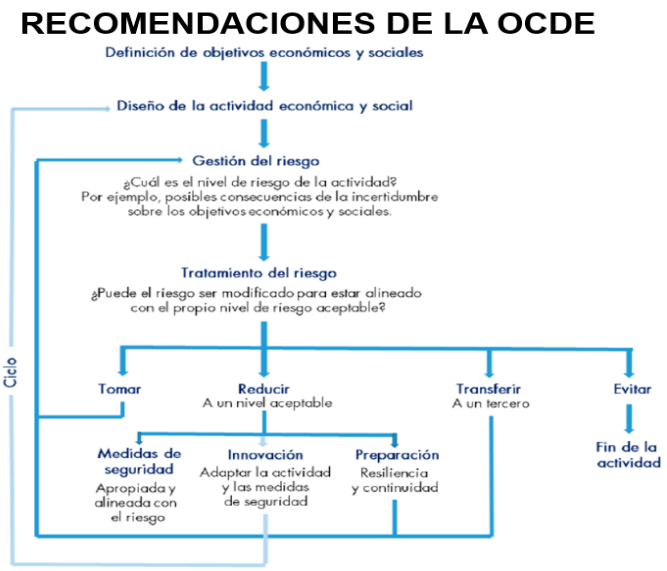


**Fig. 4**. Recomendaciones de la OCDE
**Fuente**: Impacto de los incidentes de seguridad digital en Colombia 2017.

Es necesario, ir más allá de las apreciaciones anteriores, para valorar de mejor manera lo que ilustra la figura 4, ya que de alguna forma representa la interpretación de los aspectos generales que se han tratado antes en este artículo, y que tienen que ver fundamentalmente con los aspectos relacionados con el riesgo de seguridad y la protección de los activos de una organización.

De acuerdo con la posición asumida por las anteriores organizaciones internacionales, especialmente la OCDE, respecto a la seguridad digital, concerniente, a que debe ser desarrollada en forma continua e integral en el ciberespacio, han planteado posiciones claras respecto a los aspectos más importantes, que afectan el buen desempeño y funcionamiento de dicha seguridad en el entorno planteado. Para empezar, en primer lugar, la OCDE plantea uno de los objetivos principales que se debe lograr en el entorno digital, para alcanzar la prosperidad económica y social, que un país debe obtener a través del desarrollo progresivo de la economía digital, que juega un papel importante en el desarrollo socioeconómico de todos los países.

Además, dan un enfoque especial a la utilización de la seguridad digital, en sectores distintos a los estrictamente relacionados con la defensa nacional, estimulando así, la inclusión al tener en cuenta a todas las partes interesadas en la ciberseguridad, como el Gobierno Nacional y los territorios (Departamentos, municipios y comisarias en Colombia), las organizaciones públicas y privadas, la fuerza pública (fuerzas militares, policía, etc.), los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil; y quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales. Finalmente, la Organización de referencia, recomienda adoptar una gestión de riesgos, consistente, fundamentada en principios de orden operativo, implementados para todos los integrantes del stake-holder y para todas las actividades económicas y sociales.

Recomienda entre los principios generales, un empoderamiento en el desarrollo de la ciber economía, con responsabilidad y con respeto a los derechos humanos y valores fundamentales del país. Entre los operativos recomienda que la gestión de riesgos sea cíclica, que se practiquen medidas de seguridad y se tenga en cuenta los factores de innovación y preparación que puedan traducirse en capacidad para gestionar los riesgos de ciberseguridad.

En el caso concreto de Colombia, hay que anotar, que es limitado el enfoque del gobierno nacional, en relación con la protección de la infraestructura crítica cibernética del país, y que el marco jurídico actual, no tiene en cuenta los aspectos necesarios para facilitar la protección y defensa de las infraestructuras críticas cibernéticas nacionales. Por otra parte, no existen mecanismos para generar el conocimiento necesario, que permita tener las capacidades para desarrollar las mejores prácticas, por parte de los responsables de la defensa nacional y protección de la infraestructura crítica cibernética del país; se requiere, entonces, desarrollar capacidades que se adapten a la dinámica de este entorno. Se ha recomendado, entonces, fortalecer la defensa de la soberanía nacional en el entorno digital, con un enfoque de gestión de riesgos. También, la creación de un plan de fortalecimiento de las capacidades operativas, administrativas, humanas, científicas, de infraestructura física y tecnológica del Comando Conjunto Cibernético del Comando General de las Fuerzas Militares (CCOC) y de las unidades cibernéticas de las fuerzas militares (MDN a octubre de 2016 y ejecutarlo a diciembre de 2019).

Bien vale la pena, señalar que, al contar con una política de seguridad digital, centrada en algún sector del país, con ausencia o déficit importante de coordinación con los demás sectores interesados en la ciberseguridad, se traduce en una limitación relevante de la detección y respuesta a incidentes o amenazas digitales. Así lo ha planteado la OCDE y lo ha confirmado el (BID) Banco Interamericano de Desarrollo y la (OEA) Organización de los Estados Americanos en el año 2016 a través de su Modelo de Madurez de Capacidad (CMM) de seguridad cibernética, al darle a Colombia una clasificación de “formativo”.

En el aspecto de “capacidad de respuesta a incidentes”, reconoce que el país ha trabajado en el establecimiento de un grupo de respuestas a incidentes nacionales “Colcert” pero que tiene un alcance limitado en cuanto a la detección y respuesta.

En relación con lo anterior, es necesario recordar, que una de las condiciones para llevar a cabo el procedimiento de gestión de riesgos, dentro de las condiciones exigidas internacionalmente, es la de contar con la capacidad de ejecutar acciones con pleno conocimiento y experiencia de las mismas; que sean capaces de detectar oportunamente las amenazas y riesgos, y en general la incertidumbre que afecta a las organizaciones o infraestructuras críticas bien sea públicas o privadas.

En el caso concreto de Colombia, a pesar de haber incluido en su Política Nacional las recomendaciones ya expuestas y las buenas prácticas internacionales, seguidas en la actualidad, hay que anotar que las autoridades encargadas de la Ciberseguridad en Colombia, han encontrado algunas inconsistencias del plan de Seguridad Nacional, entre otras las siguientes:

- Cooperación, colaboración y asistencia nacional e internacional, insuficientes y desarticuladas.
- No se cuenta con una instancia de coordinación nacional, desde el alto nivel del gobierno en materia de seguridad digital; tampoco, se cuenta con instancias de orientación superior, que emita lineamientos generales a nivel nacional.
- El marco legal y regulatorio, que permita maximizar las oportunidades de la economía digital, no es adecuado y es disperso.
- No hay suficientes recursos técnicos, humanos, ni financieros, para enfrentar nuevos tipos de crimen delincuencial y fenómenos, en el entorno digital, bajo un enfoque de gestión de riesgos.
- El marco jurídico para contrarrestar el delito cibernético y para gestionar los delitos, con evidencias electrónicas no es adecuado.
- Los jueces, fiscales y policías, no tienen capacidades suficientes en materia de delitos informáticos, ni en los aspectos técnicos y jurídicos de la obtención de la evidencia digital.

Se podría concluir, parcialmente, que las preocupaciones dadas en la ciberseguridad nacional, tienen que ver básicamente con la capacidad con que debe contar una infraestructura u organización, para gestionar una Ciberseguridad Nacional enfocada a la gestión de riesgos, y con capacidad, también, para proteger a las múltiples partes de la cibercriminalidad creciente; por otra parte, también hay una preocupación central, en relación a incluir en la gestión de

riesgo a todas las partes interesadas, según ya se ha planteado y para lo cual se lanzó en el mes de agosto del 2018 un modelo de gestión riesgos de seguridad digital (MGRSD) dirigido a las entidades del sector público y el cual fue incluido como anexo 4 en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, como se evidencia, no fue orientado a las partes interesadas (organizaciones privadas, entre otras), y que debe ser adoptado y aplicado, evaluándolo periódicamente e implementándolo y promoviéndolo en las múltiples partes interesadas.

Esto constituye una señal, acerca del direccionamiento de la política nacional de ciberseguridad, que está tomando para mejorar sus practicas y consolidarse como líder regional en el desarrollo de la ciberseguridad. Un ejemplo reciente que confluye a lo anterior, es la fundación del Centro de Capacidades para la Ciberseguridad de Colombia (C4), llevado a cabo el 6 de agosto de 2018, el cual se constituye, según los proyectos con que cuenta y sus capacidades, en el complejo más grande de Latinoamérica, para combatir los crímenes cibernéticos. Sin embargo, hay que puntualizar que ninguno de sus (4) cuatro enfoques, esta dirigido a la Gestión de Riesgos de Ciberseguridad.

Para terminar, hay que decir, que en realidad la Política Nacional de Ciberseguridad en Colombia, apenas acaba de incluir la Política Internacional de Gestión de Riesgos, que se viene desarrollando con éxito en el mundo y cuyo objetivo principal es la protección de los activos de ciberseguridad, utilizando una estrategia que consolide la economía digital, mediante un procedimiento continuo e integral de seguridad, que este enfocado en la gestión de riesgos. Así, lo ha entendido Colombia, y su Política Nacional de Seguridad en el entorno digital, que al centrarse en ese aspecto y estimular el conocimiento y las capacidades para desarrollar las mejores prácticas aceptadas en el mundo. Inmersa, Colombia, en este escenario, puede aspirar a que se siga teniendo en cuenta como uno de los países líderes en Ciberseguridad.

Teniendo en cuenta la relevancia que se le ha dado a la gestión de riesgos, en la economía de una organización, y por tanto, a la de un país, es oportuno hacer una breve sintesís sobre cómo se ha entendido la Economía Digital: se la interpreta como un Gran sistema, en el que funcionan conjuntamente la infraestructura de las redes de comunicación, el procesamiento de información – servicios-, las tecnologías web y las multiples partes interesadas. Es el grado de desarrollo y complementación de estos componentes, lo que define el nivel de avance de cada país.

En el terreno organizacional, sus componentes y los recursos que soportan el negocio, como la tecnología, el hardware, el software, las telecomunicaciones y el personal especializado; todo lo cual constituye su estructura de negocio. Esta estructura, será alineada al comercio electrónico referido a la generación de negocios y compraventa de bienes utilizando internet como medio de comunicaciones. Es en este escenario, donde se activan las amenazas o ataques cibernéticos y en el cual debe hacer continua presencia la ciberseguridad, para proteger los activos principales, objetivos y finalidades de las organizaciones, para impedir o mitigar el deterioro económico.

En nuestro país, a pesar de contar en la actualidad con una política de ciberseguridad aceptable, según ya lo hemos anotado, los ataques de los ciberdelincuentes tienen una tendencia de aumento y últimamente, hace más o menos cinco años se han centralizado en sectores directamente vinculados a la democracia política. En este sentido, hay que anotar lo sucedido en el año 2014 cuando se invadio por expertos hackers la información digital confidencial de algunos activistas democráticos, y por lo cual hoy se encuentra en prisión el delincuente material. En la actualidad esta ocurriendo algo similar, en donde se encuentran comprometidas personas que recientemente habían tenido desempeño oficial, en el área de la infórmática. Estos dos casos ilustran, que nuestra ciberseguridad tiene capacidad para defender nuestras infraestructuras y también para castigar a los ciberdelincuentes. No obstante, hay que anotar que los supuestos autores intelectuales han gozado plenamente de total impunidad.

Como quiera que los ciberdelincuentes materiales, podrán ser castigados efectivamente en esta área de su actuación, hacia el futuro avisoraran otras áreas que les sean de mayor favoravilidad, para sus actos delictivos, como son las organizaciones o empresas privadas.

Por lo anterior, es pertinente insinuar algunas recomendaciones a nuestras organizaciones, para que con criterio preventivo, desarrollen algunas estrategias que les permitan superar adecuadamente las consecuencias, de algún ataque futuro a sus empresas. Parte de una buena estrategia, en primer lugar, una vez, se haya dado el ataque cibernético, la organización debe informar a los medios de comunicación y a las partes múltiples interesadas, qué información confidencial fue robada mediante el ataque digital, y quién debe divulgar esa información, que debe tramitarse a través de un guión claro y exacto que revele los efectos que se están mitigando después del ataque y qué deben hacer las multiples partes para impedir que sus datos confidenciales, como tarjetas de crédito, números de cédulas,etc, sean utilizadas en contra de sus intereses. Es importante, también, que antes del ataque de ciberseguridad la organización tenga identificada la información que tenga mayor valor para el hacker. Como también se ha dicho anteriormente, en este artículo, hay estudios que han revelado que los datos en la nube o en centros de datos pueden ser los objetivos del futuro ciberdelincuente, ya que en ellos se almacena cada día más información.

Finalmente, es imperativo tomar medidas para evitar que se produzca un ataque digital; ello implica contar con software y hardware especializados. Se recomienda, mantener siempre actualizadas las aplicaciones y los sistemas usados en los

computadores y servidores; impedir que los empleados usen en sus equipos memorias usb que no hayan sido vacunadas por el antivirus y por encima de todo no escatimar en el presupuesto que exige tener una buena seguridad digital.

## X. CONCLUSIONES

Las investigaciones más recientes sobre Ciberseguridad, han concluido que las amenazas y ataques que se vienen haciendo a las organizaciones ya sean públicas o privadas han aumentado en los últimos años, y que en la actualidad hay una tendencia exponencial de seguir creciendo en el futuro inmediato.

Se ha concluido igualmente que las amenazas a la infraestructura crítica a nivel mundial constituyen el problema de los objetivos y misiones de las organizaciones privadas, de las propias del Estado, y de la ciberseguridad.

Se puede concluir, que existen organizaciones Internacionales como la NIST, ISO, ISACA, INCIBE, entre otras, que han venido trabajando para solucionar el problema central de la ciberseguridad a través de estándares, directrices, y normas con la ayuda de las cuales se ha venido desarrollando una metodología enfocada a evitar o tratar los riesgos.

Que, en tal metodología aplicada, mediante el procedimiento de gestión de riesgos que se caracteriza por su continuidad y que ha de ser monitoreado permanentemente, debe contar con una buena comunicación entre los ejecutivos, nivel de procesos y negocios y el nivel de implementación y operaciones de una organización.

Una conclusión importante, es la necesidad de comprender la estrecha interrelación que existe entre los conceptos de vulnerabilidad, probabilidad y consecuencias en el proceso de la materialización del riesgo. Por esta razón, se debe concluir que cuanto mayor vulnerabilidad tengan los activos de una organización, mayor es la probabilidad que se materialice la amenaza, y que, al efectuar el producto de la mayor probabilidad por consecuencias, esto se traduce en el nivel del riesgo.

También hay material suficiente para concluir, que la tecnología de la información ha permitido el desarrollo económico a nivel mundial, y que esa misma tecnología también, esta amenazada por la materialización de riesgos que pueden traer grandes consecuencias.

También podemos entender como conclusión que el buen funcionamiento de la infraestructura crítica, depende de la capacidad organizacional para comprender e identificar, y evaluar las amenazas y riesgos, y que las organizaciones deben desarrollar la gestión de riesgos conjuntamente con la ciberseguridad, contando siempre, con la mejor comunicación posible tanto interna como externa.

Colombia en la actualidad esta en un proceso de transición que busca consolidarse en las mejores prácticas de ciberseguridad que actualmente existen en el mundo.

Colombia fue evaluada en su capacidad de ciberseguridad con el Modelo de Madurez de Capacidad (CMM), y se le dio la clasificación de “formativo” (alcance limitado en detección y respuesta).

En la actualidad, la ciberseguridad se orienta no solo a la ciber defensa, sino también a la ciberseguridad de las entidades públicas.

## REFERENCIAS


[1] «Conpes 3701,» (2011 julio) Ministerio de las TIC. http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf. [Último acceso: Agosto 2018].

[2] David Harley, ESET Senior Research Fellow «ESET,» Tendencias En Ciberseguridad 2018: El Costo De Nuestro Mundo Conectado, Diciembre 2017. [En línea]. Available: https://www.welivesecurity.com/wp-content/uploads/2017/12/Tendencias_2018_ESET.pdf. [Último acceso: Septiembre 2018].

[3] «Min Tic,» 2014. [En línea]. Available: https://www.mintic.gov.co/portal/604/w3-article-6120.html. [Último acceso: Julio 2018]

[4] Camilo Gutiérrez, ESET Head of Awareness and Research «ESET,» Tendencias En Ciberseguridad 2018: El Costo De Nuestro Mundo Conectado, Diciembre 2017. [En línea]. Available: https://www.welivesecurity.com/wp-content/uploads/2017/12/Tendencias_2018_ESET.pdf. [Último acceso: Septiembre 2018].

[5] «Colcert» Grupo de respuesta a emergencias en cibernéticas de Colombia[En línea].Junio 2017 Available: http://www.colcert.gov.co/?q=contenido/el-gobierno-de-colombia-liderado-por-la-presidencia-de-la-rep%C3%BAblica-comienza-una-campa%C3%B1a. [Último acceso: Agosto 2018].

[6] «CONPES 3854» 11 Abril 2016. [En línea]. Available: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf. [Último acceso: Julio 2018]

[7] «CCIT» 2016. [En línea]. Available: http://www.ccit.org.co/memorias-del-iii-foro-seguridad-digital-2016/. [Último acceso: Agosto 2018]

[8] «snti» 2018. [En línea]. Available: http://www.snti.ru/cd/ISO310002018.pdf. [Último acceso: Julio 2018]

[9] «NIST» abril 2018. [En línea]. Available: https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework. [Último acceso: Junio 2018]

[10] «NIST» 2014. [En línea]. Available: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf. [Último acceso: Junio 2018]

[11] «ISACA» 2018. [En línea]. Available: https://cybersecurity.isaca.org/state-of-cybersecurity. [Último acceso: Agosto 2018]

[12] «INCIBE» INCIBE_PTE_AproxEmpresario_002_GestionRiesgos-2015-v1. [En línea]. Available: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf. [Último acceso: Junio 2018]

[13] «Icontec» Norma Técnica Colombiana NTC-ISO31000-2011. [En línea]. Available: https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf. [Último acceso: Julio 2018]

[14] « NIST » Publicación especial NIST 800-160 Volumen 1, Ingeniería de seguridad del sistema, Consideraciones para un enfoque multidisciplinario en la ingeniería de sistemas seguros confiables, Ross et al, noviembre de 2016 actualizado del 21 de marzo del 2018) https://doi.org.110.6028/NIST.SP.800-160v1. [Último acceso: Agosto 2018]

**AUTOR**

Yaneth Linares Lizarazo, se graduó como Ingeniero de Sistemas, con Énfasis en software en la Universidad Antonio Nariño, actualmente se encuentra culminando una especialización en Seguridad Informática, en la Universidad Piloto de Colombia.

En la actualidad se desempeña como Web máster de una entidad del Distrito. Cuenta con habilidades para llevar a cabo proyectos bajo presión y con una responsabilidad grande al estar a cargo de la administración del Sitio Web, el cual presta un servicio a la ciudadanía.