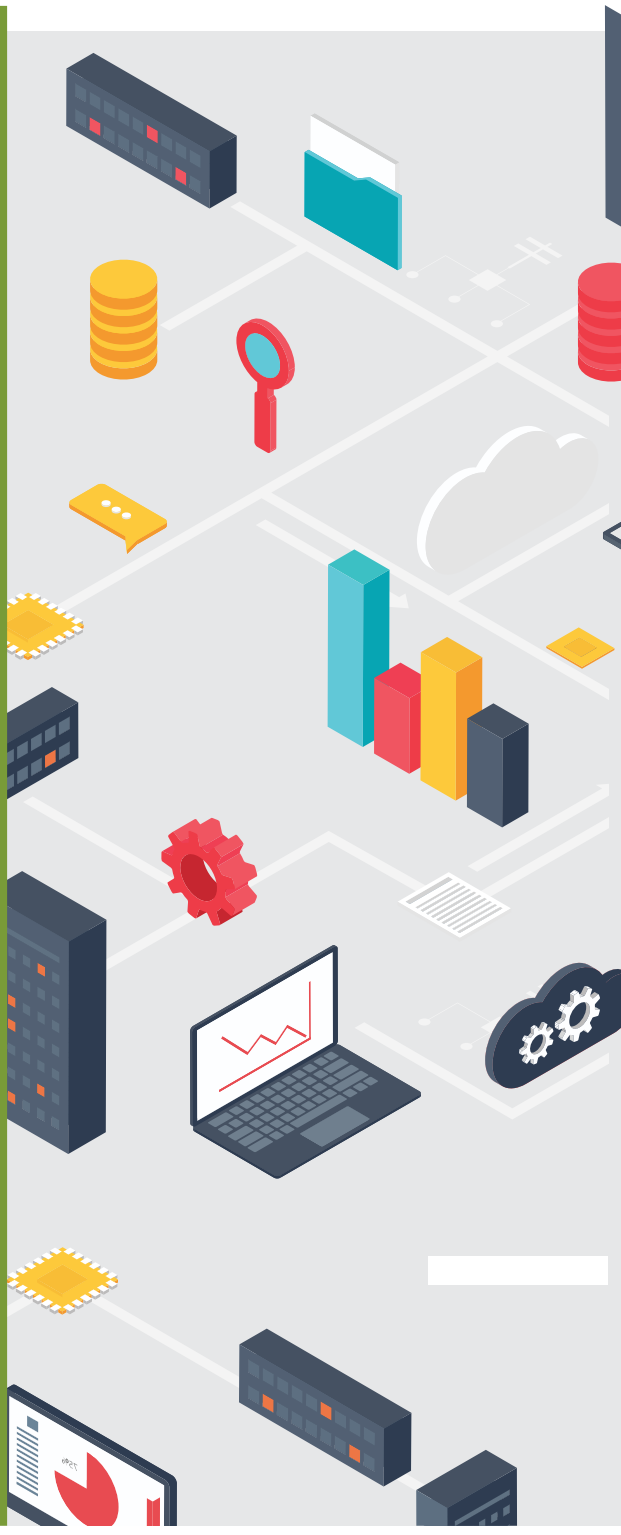
ASOCIACIÓN REGIONAL DE EMPRESAS DEL SECTOR
PETRÓLEO, GAS Y BIOCOMBUSTIBLES
EN LATINOAMÉRICA Y EL CARIBE.

Ruta estratégica de la ciberseguridad empresarial

Un marco de orientación directiva



Marzo 2017

PUBLICACIÓN ARPEL N° WP01 - 2017

WHITE PAPER

Tabla de contenido

1. Introducción

La vertiginosa evolución tecnológica y la acelerada digitalización de productos y servicios revelan nuevas oportunidades para las empresas y novedosas propuestas de valor para los individuos (Schwab, 2016).

En este escenario de inestabilidades tecnológicas, sumados a los cambios y ambigüedades geopolíticas, el incremento de los marcos normativos globales, las exigencias cambiarias y retos macroeconómicos de las naciones, establecen el nuevo territorio de operaciones de los negocios internacionales que demanda una mirada estratégica distinta, que permita identificar las nuevas asimetrías de información y sobremanera anticipe movimientos discontinuos que modifiquen el statu quo vigente (Paloalto – NYSE, 2015).

Para la industria de petróleo y gas la situación no es diferente, como quiera que este segmento de negocio se encuentra en la mitad de las tensiones internacionales, por su valor estratégico en la generación de riqueza y como infraestructura crítica de las naciones que afecta su gobernabilidad. En este sentido, comprender la dinámica de las amenazas informáticas y los ataques cibernéticos por parte de los ejecutivos de esta industria, se vuelve relevante para comprender la incertidumbre que los impactos de este tipo de situaciones genera, para mantenerse informados sobre las acciones claves a realizar y particularmente contar con una monitorización activa de sus tendencias (Moraleda, 2014).

Bajo este contexto, el presente documento establece una ruta estratégica base para las compañías de petróleo y gas con el fin de movilizar los esfuerzos respecto de la ciberseguridad empresarial, que le permita establecer acciones concretas para evolucionar sus prácticas actuales de seguridad y control y desarrollar, en el mediano y largo plazo, capacidades claves que habiliten una postura de ciberseguridad proactiva que proteja y defienda el valor de los activos digitales críticos que la industria mantiene en el desarrollo de sus actividades de negocio.

Es importante anotar, que las propuestas detalladas en esta publicación responden a la dinámica de las buenas prácticas de ciberseguridad empresarial vigentes a la fecha y por lo tanto, no son sugerencia específica para las organizaciones del sector de petróleo y gas. En consecuencia, se entrega este aporte conceptual y práctico como una oportunidad para reflexionar y analizar los retos que enfrenta la industria en un entorno volátil, incierto, complejo y ambiguo (Johansen, 2009), y adicionalmente, digitalmente modificado.

Bienvenidos a explorar y refinar este mapa estratégico de la ciberseguridad empresarial, sabiendo que es sólo una excusa para detallar un territorio poco explorado y que aún se empieza descubrir y detallar.

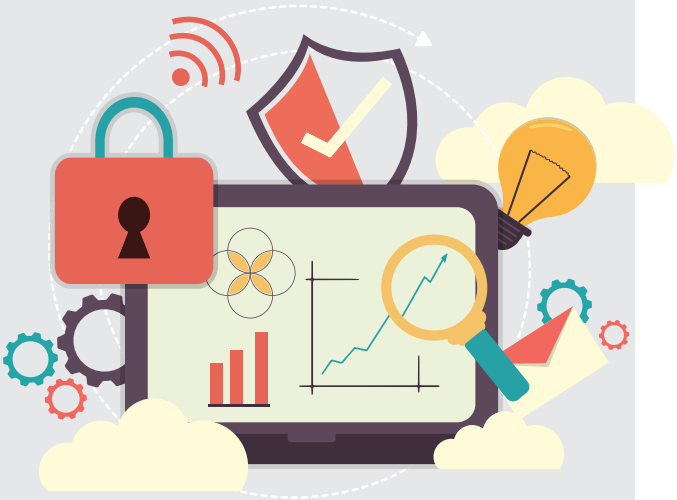
2. **Motivaciones estratégicas**

Movilizarse en los temas de ciberseguridad empresarial en el contexto de la industria de petróleo y gas, es entender la dinámica de la geopolítica global que afecta las diferentes variables económicas y sociales de los países con activos estratégicos como los hidrocarburos y productos conexos. La exigencia de mejores precios y la necesidad de mayores ingresos de las naciones, hacen de esta industria un eje fundamental para el mantenimiento de los equilibrios globales y los posicionamientos de las naciones y grupos económicos en el contexto internacional.

Bajo este contexto y la acelerada digitalización del mundo, se introducen aspectos novedosos en las operaciones de la industria petrolera, visibilizando infraestructura de operaciones que antes sólo era de dominio y control de redes cerradas y personal especializado en el uso y aseguramiento de sistemas de control industrial.

La hiperconectividad y la necesidad de contar con información en tiempo real, para toma de decisiones estratégicas, lleva a tender puentes de conexión entre el mundo de control de operaciones y los sistemas de información corporativos, abriendo la posibilidad de nuevos retos técnicos y administrativos tanto para proveer información, como para proteger el valor de los activos digitales de la organización (Cloutier, 2016).

Así las cosas, la tendencia de lo “digital por defecto” es una condición necesaria de las organizaciones actuales. En este escenario, las empresas deben avanzar en un proceso de transformación digital (Rogers, 2016) donde deben repensar la manera como operan, la forma como exceden las expectativas de los clientes y sobre manera como crean y comunican el valor de los nuevos productos y/o servicios digitalmente modificados.



Por tanto, las empresas de petróleo y gas como pieza angular de la dinámica geopolítica actual y dueña de parte de las infraestructuras críticas de un país, requiere comprender y estudiar en detalles los riesgos conocidos, latentes, focales y emergentes que esta nueva realidad le pone de manifiesto, para darle respuesta a los ejecutivos de primer nivel respecto del nivel de aseguramiento y resiliencia disponible frente a la inevitabilidad de la falla.

Las empresas del siglo XXI deben pasar de una vista operacional y táctica de la tecnología de información y comunicaciones, a una estrategia digital que reconecta los intereses de los grupos de interés con los retos empresariales, con el fin de reinventar la forma como se alcanzan los objetivos corporativos y cómo los clientes se convierten en el insumo fundamental de la acción estratégica (Rowsell-Jones, 2013).

Lo anterior demanda de los cuerpos de dirección actuales tomar riesgos inteligentes, que permitan la mayor flexibilidad con la menor exposición; una ecuación que sólo es posible balancear cuando la organización entiende la falla como una inversión en el aprendizaje corporativo, como la capitalización de lecciones aprendidas y como una forma de hacer cosas distintas en el futuro (Scholtz, 2016; Scholtz, 2016b).

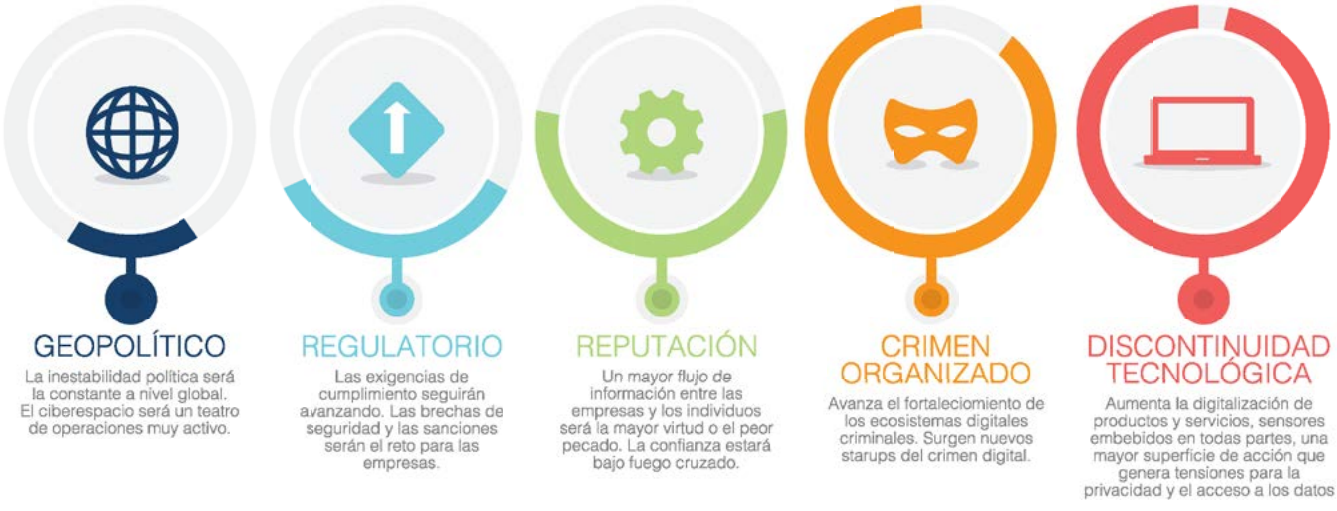
3. Ciberseguridad empresarial:
Una ruta estratégica para avanzar

3.1 Introducción

Cuando se habla de *ciberseguridad empresarial* se entiende como un conjunto de "nuevas prácticas de defensa y anticipación antes desconocidas y poco nombradas" con el fin de concretar la responsabilidad ejecutiva de los miembros de la junta directiva para entender y construir una estrategia corporativa que permita proteger y asegurar la resiliencia de las operaciones y la reputación de la empresa en el contexto de las amenazas digitales propias del ecosistema donde opera (Adaptado de Cano, 2015).

En este sentido, trazar una ruta estratégica que sirva de guía para la organización y su cuerpo de gobierno (Calleja y Rovira, 2015), requiere establecer un modelo base de **prerrequisitos, fases y capacidades** que permitan orientar las acciones pertinentes en las empresas respecto del reto de las amenazas digitales (Mcafee, 2016) que se advierten en el entorno considerando al menos cinco (5) riesgos estratégicos:

Riesgos claves en la ciberseguridad empresarial[1]



(1) Autoría: Jeimy J. Cano M., Ph.D, CFE

3.2 Marco de orientación directiva para la ciberseguridad empresarial

A continuación, se detalla el marco de acción directiva que desarrolla una agenda estratégica para concretar las capacidades requeridas para enfrentar las amenazas digitales propias de las empresas, en el escenario de un ecosistema digital y el aumento de los productos y servicios digitalmente modificados (Porter y Heppelmann, 2015).

Ruta estratégica para la ciberseguridad empresarial[2]

FASES	INTELIGENCIA	INTEGRACIÓN	CUMPLIMIENTO	VALOR
CONSOLIDACIÓN	**Planeación y análisis de escenarios** (Anticipiar posibles y probables entornos empresariales)	**Simulación y pruebas de escenarios** (Validación de amenazas emergentes)	**Responsabilidad digital corporativa** (Confianza digital en los clientes)	**Defender y anticipar** (Gobierno corporativo de activos digitales)
INCORPORACIÓN	**Analítica de datos y pronósticos** (Relevar patrones y tendencias emergentes)	**Centro de operaciones de seguridad (SOC)** (Detección y prevención frente a amenazas conocidas y latentes)	**Responsabilidad digital demostrada** (Aseguramiento de prácticas de seguridad y privacidad)	**Proteger y asegurar** (Gestión de riesgos de Infosec)
INICIALIZACIÓN	**Correlación de eventos** (Identificar y relacionar eventos no estándar)	**Defensa en profundidad** (Seguridad centrada en los datos y las operaciones)	**Gestión de controles de TI** (Uso de buenas prácticas y estándares internacionales en infosec)	**Proteger** (Efectividad de controles de TI)
PRERREQUISITOS	**Datos e información de calidad**	**Competencias técnicas y analíticas**	**Cultura de seguridad y control**	**Visibilidad y reconocimiento ejecutivo**

(2) Modelo adaptado de las ideas de: Dubois, D. (2016) The building blocks of digital transformation: Intelligence, Integration and Impact. European Business Review. Septiembre. Recuperado de: http://www.europeanbusinessreview.com/the-building-blocks-of-digital-transformation-intelligence-integration-and-impact/

CAPACIDADES

Una capacidad es una habilidad para coordinar diferentes actividades que la organización sabe hacer muy bien y en la cual aprovecha un aprendizaje colectivo, que permite generar valor a sus grupos de interés. Por lo tanto, no es estática y evoluciona conforme la dinámica del entorno donde hace realidad (Adaptado de Prahalad y Hamel, 1990).

Particularmente en el contexto de la ciberseguridad empresarial una capacidad permite aumentar el nivel de proactividad y anticipación de una corporación frente a las amenazas digitales, así como su resiliencia frente a eventos inesperados o inciertos que afecten la imagen y las operaciones de una organización.

Bajo este enfoque se definen tres (3) capacidades básicas asociadas con la ciberseguridad empresarial: **inteligencia, integración y cumplimiento,** cada una de ellas interrelacionadas con el fin de brindar una ruta integrada de acciones que son requeridas para aumentar el nivel de preparación y anticipación requerido frente al escenario asimétrico de riesgos previamente comentado.

La **inteligencia** es una capacidad que busca desarrollar habilidades en la organización para explorar el entorno, detectar patrones de amenazas, anticipar eventos inesperados e influir en su ambiente para generar disuasión frente a posibles terceros no autorizados que quisieran comprometer la infraestructura tecnológica y de seguridad tecnológica disponible, así como el desarrollo de campañas que puedan generar acciones adversas contra la imagen y operaciones de la empresa. Para avanzar en la evolución de esta competencia clave es necesario tener como prerrequisito *datos e información de calidad*. Es decir, se debe asegurar un ejercicio de depuración de los datos disponibles para motivar una correlación de eventos, que sea base para la analítica de datos y pronósticos, y así finalmente plantear el análisis de escenario claves que la empresa debe mantener en foco para anticipar sus movimientos en su entorno de negocios y en el contexto del ecosistema digital donde participa.

La **integración** es otra capacidad que busca motivar la coordinación de actividades en la dinámica de los procesos de la empresa. Para ello se requiere tener como prerrequisito *personas con competencias (entendidas como saberes disponibles en las personas) técnicas y analíticas*, que permitan desarrollar las prácticas de seguridad y control situadas en la dinámica de las relaciones de negocio y las actividades que la soportan.

La evolución de esta capacidad clave demanda una implementación base del concepto de *defensa en profundidad centrada en los datos y las operaciones* de la empresa, con el fin de mantener un control de acceso definido y verificado frente a lo que la organización ha decidido es importante. Una vez consolidado este ejercicio, se debe incorporar la vista de un servicio de un centro operaciones de seguridad (conocido por sus siglas en inglés SOC – *Security Operation Center*) con el fin de aumentar la plataforma de monitorización disponible con el fin de detectar y prevenir amenazas conocidas y latentes.

Finalmente, esta habilidad llega a su nivel más elevado cuando es posible adelantar simulación y pruebas de escenarios (Phadnis, Caplice y Sheffi, 2016), que lo que buscan es validar las amenazas emergentes y crear las acciones preventivas que

anticipen los posibles impactos de la materialización de las mismas. Este ejercicio como el mencionado en la capacidad anterior, relacionado con el análisis de escenarios, requiere la participación clave del cuerpo de gobierno corporativo para que pueda visualizar la preparación resiliente de la empresa y sus responsabilidades frente a eventos inesperados que se pueden presentar en el futuro.

El **cumplimiento** como capacidad clave en la ciberseguridad empresarial es un compromiso de la empresa con la ética de los datos de los grupos de interés, un conjunto de acciones coordinadas disponibles en las regulaciones nacionales e internacionales que exigen de la organización una práctica homogénea asociada con estándares internacionales de seguridad y control, así como con la protección de datos personales, que aumentan la confianza de los terceros relacionados frente a las operaciones y negocios de la empresa.

Esta capacidad clave requiere como prerrequisito *una cultura de seguridad y control* claramente establecida, con el fin de que el desarrollo de las actividades en cada una de las fases de evolución prevista se puedan alcanzar los resultados esperados. Esto es, una adecuada gestión de controles de tecnología de información que respondan a las exigencias de supervisores nacionales e internacionales, que permita habilitar un marco de responsabilidad digital demostrada en el aseguramiento de prácticas de seguridad y privacidad, para finalmente alcanzar esa confianza digital (PwC, 2013) enraizada en los grupos de interés.

El cumplimiento más que ajustarse a una norma o regulación particular, debe ser una declaración empresarial frente al cuidado de los datos e información de sus grupos de interés, que permita tanto un control como uso adecuado en el ejercicio de los procesos de negocio de la empresa, así como oportunidades para las personas en compensación por compartir dichos datos con la organización.

FASES

Las fases son niveles de desarrollo que se van alcanzando de las capacidades previamente anunciadas. Las fases establecen tendencias de madurez alcanzadas en el desarrollo de las habilidades comentadas, con el fin de advertir cómo se debe ir avanzando en la consolidación de una capacidad particular. De esta forma, la inicialización será el nivel de desarrollo básico, la incorporación el intermedio y la consolidación el más avanzado.

Es importante anotar, que cada fase exige una sostenibilidad específica, pues sobre la anterior se basa el desarrollo de la siguiente. Así las cosas, no tener aseguradas las prácticas y resultados del nivel anterior implica un debilitamiento tanto de las capacidades claves como del valor previsto en el desarrollo del modelo.

Con la fase de inicialización podemos indicar que las empresas deben tener un nivel básico de prácticas en cada una de las capacidades. Es un ejercicio de revisión particular que busca validar el nivel de evolución actual de la organización frente a las capacidades. Si la corporación no logra tener los resultados establecidos para cada capacidad planteada, la promesa de valor prevista en la columna valor no será alcanzada de forma homogénea y habrá inestabilidades que comprometan los resultados previstos.

La incorporación se consolida como un ejercicio de coordinación entre las prácticas y los procesos de negocio de la empresa. No es suficiente tener una efectividad de controles de tecnología de información, si en la dinámica de los procesos no se entiende y conecta la necesidad de protección de la información, como un ejercicio de confianza imperfecta (Cano, 2016b), donde tanto personas, como procesos y tecnología tienen limitaciones y por tanto, se requiere el concurso de los tres para establecer el nivel de protección que la información demanda frente a los retos de la empresa y su entorno.

La consolidación implica una declaración y visibilidad de ejecutiva de la protección de los activos digitales de la empresa, de tal forma que la planeación y visualización estratégica del negocio cuenta con las lecturas de las amenazas digitales,

los escenarios y sus simulaciones, así como el compromiso con los clientes y sus datos, denominado responsabilidad digital corporativa (Cooper, Siu y Wei, 2015). En este punto, no sólo se han afinado y asegurado las prácticas previamente comentadas, sino que se hace parte de la agenda y capital político de los miembros de junta la exigencias y retos de la ciberseguridad empresarial.

Es importante anotar que las organizaciones podrán avanzar más rápido en una u otra capacidad y esto hará menos concreta la promesa de valor que se advierte al llegar a un nivel homogéneo de evolución o logro de la fase. Por tanto, se requiere que al menos dos (2) de las tres capacidades se encuentren desarrolladas en un nivel particular en el modelo para poder validar la percepción de valor sugerida en el mismo.

Finalmente es importante tener en cuenta que la percepción del valor estará íntimamente ligada tanto a los resultados que se tienen en cada fase, para cada capacidad, así como el nivel de visibilidad y reconocimiento ejecutivo que se le haya brindado a la ciberseguridad empresarial en el cuerpo colegiado de gobierno.

PRERREQUISITOS

Los prerrequisitos que se establecen en modelo son los fundamentos base que se requieren en cada una de las capacidades claves declaradas para desarrollar la agenda estratégica de la ciberseguridad empresarial. Es decir, aquellos aspectos que afectan el desarrollo y fortalecimiento de la capacidad a la que hacen referencia, pues de no contar con este aspecto no se advertirá un desarrollo homogéneo para concretar los resultados que se pretenden con el cumplimiento de la agenda detallada en el modelo.

4. Ciberseguridad empresarial: **Un llamado a la acción del gobierno corporativo**

En un mundo digitalmente modificado el flujo de la información empresarial y personal se imponen como una realidad que no puede ser ignorada por las organizaciones ni los individuos. En este sentido, los cuerpos de gobierno corporativo deben comprender que se advierte una dinámica de negocios que necesariamente pasa por el contexto de lo digital, de lo tecnológicamente modificado y que demanda servicios novedosos todos ellos basados en información (Kaplan, Bailey, O'Halloran, Marcus y Rezek, 2015).

La nueva era digital establece para las organizaciones una comprensión dinámica de las expectativas de los clientes, una acelerada convergencia tecnológica y sobre manera una postura resiliente que le permitan sobreponerse a las inesperadas olas de discontinuidad de cambios en el entorno que repiensan y destronan paradigmas previamente aceptados y probados (Porter y Heppelmann, 2014).

En este escenario, los cuerpos de gobierno deben asegurar la incorporación de nuevos miembros que comprendan y revelen las inestabilidades actuales o sugieran alteraciones futuras del entorno que afecten los planes corporativos en el mediano y largo plazo, o motivar espacios para concretar una "alfabetización digital" que confronte los modelos de negocio y percepciones del mundo de los directores actuales, con el fin de abrir las reflexiones a escenarios no sólo probables, sino posibles (KPMG, 2015).

La nueva realidad de las empresas, ahora participantes de un ecosistema digital de negocios, demanda replantear las responsabilidades de los miembros de la junta directiva, no sólo frente a los riesgos propios del negocio del cual hacen parte, sino frente a las amenazas digitales que son fruto de la inevitabilidad de la falla, de la confianza imperfecta en las relaciones dentro y fuera de la organización y sobre manera del flujo masivo de información entre las empresas y las personas (Ernst & Young, 2013).

En consecuencia, tres (3) condiciones son necesarias para configurar un postura concreta y relevante de las juntas directivas frente a la ciberseguridad empresarial: **deben ser confiables, vigilantes y resilientes** (Deloitte, 2016). A continuación, se detallan de forma sencilla cada una de ellas y cómo hacerlas realidad en la dinámica del cuerpo colegiado.

La **confiabilidad**, implica establecer y mantener las capacidades fundamentales de la gestión de la seguridad, privacidad y control en la organización. Esto es, adelantar la gestión de riesgos, mantener una revisión y prueba de controles, así como motivar el cumplimiento de los estándares y regulaciones asociados con el tratamiento del ciber riesgo (Frappolli, 2015).

Esta confiabilidad en términos concretos en la junta directiva significa: (Adaptado de Deloitte, 2016)

- La junta directiva y los ejecutivos empresariales (el nivel presidencias y vicepresidencia) se mantienen informados de los riesgos potenciales identificados en su sector de negocio y los potenciales impactos para la organización.
- La junta directiva cuenta con asesores o personal especializado, que conoce, entiende y comunica los retos de las tecnologías de información y los ciber riesgos.
- La junta directiva es responsable directa de la gestión de ciber amenazas, así como del seguimiento al desarrollo e implementación del programa de ciber riesgos de la empresa.

La **vigilancia**, implica reconocerse como parte de un ecosistema digital empresarial, con el fin de detectar violaciones y anomalías en el flujo de la información, a través de una mayor consciencia de sus relaciones con su entorno, esto es, cómo la empresa y sus operaciones afecta su ambiente y viceversa.

La vigilancia revisada en términos prácticos en el contexto de las juntas directivas implica: (Adaptado de Deloitte, 2016)

- La junta directiva evalúa y monitoriza el valor del ciber seguro contratado, con el fin de asegurar las mejores prácticas que disminuyan su exposición.
- La junta directiva y su equipo ejecutivo, asistido de personal especializado identifica posibles "cisnes negros" o situaciones inciertas de riesgo, que permitan anticipar y evitar momentos no deseados, con potencial catastrófico.
- La junta directiva desarrolla de forma periódica una referenciación externa respecto del programa de gestión del ciber riesgo.

La **resiliencia**, es la habilidad para retornar rápidamente a la normalidad de las operaciones y reparar los daños ocasionados, luego de un inevitable ciber ataque. Esto es, hacer de la inevitabilidad de la falla, una oportunidad para asumir los efectos de un ciber ataque y construir una vista mejorada de la defensa activa de la empresa desde el negocio hacia las tecnologías de información.

La resiliencia practicada de forma específica por la junta directiva exige: (Adaptado de Deloitte, 2016)

- Compartir información con el sector de su industria, centros de análisis independientes, agencias del gobierno, instituciones académicas y firmas de investigación, para mantener una vista global de cooperación y resistencia conjunta con los actores del ecosistema digital empresarial.
- La junta directiva motiva la participación activa de la empresa en las simulaciones y entrenamientos frente a ciber ataques, promovidos por su sector de negocio y agencias del gobierno.
- Asegurar que las terceras partes que hacen parte de su cadena de operaciones, han sido entrenadas en los ciber riesgos de la empresa y han incorporado estas prácticas en su operación diaria.

Si bien pueden existir muchas más declaraciones específicas para cada una de las condiciones claves enunciadas, al menos las detalladas, establecen un punto base de reflexión, que le permita ahondar a cada cuerpo colegiado la realidad de ciber riesgo y la amenaza real de un inevitable ciber ataque (Deloitte, 2016).

En la medida que estas condiciones se desarrollen armónicamente en la junta directiva y su práctica se vuelva parte de la agenda de estos ejecutivos, la madurez y preparación de la empresa frente a un eventual ciber ataque será mayor, particularmente porque desde la vista directiva comparten un lenguaje común frente a esta realidad, que les permite hablar honesta y abiertamente generando un entendimiento común que se integra al ejercicio estratégico de la empresa (Cano, 2016).

En este sentido, las juntas directivas deben mantener una vista sistémica de los impactos de un posible ciber ataque, pues sólo así es posible identificar, aprender y entender desde la inevitabilidad de la falla, los ciber riesgos como fundamento de la práctica directiva moderna.

5. **Referencias**

Calleja, L. y Rovira, M. (2015) *Gobierno institucional. La dirección colegiada.* Navarra, España: EUNSA.

Cano, J. (2015) Ciberseguridad empresarial. Primeras aproximaciones prácticas. Blog IT-Insecurity. Recuperado de: http://insecurityit.blogspot.com.co/2015/09/ciberseguridad-empresarial-primeras.html

Cano, J. (2016) La seguridad de la información en el imaginario de las Juntas Directivas. Un reto de transformación de creencias, actitudes y valores. *Revista Nova et Vetera.* Universidad del Rosario. ISSN: 2422-2216. 2, 22. Diciembre. Recuperado de: http://www.urosario.edu.co/revista-nova-et-vetera/Inicio/Cultura/La-seguridad-de-la-informacion-en-el-imaginario-de/

Cano, J. (2016b) Protección de la información. Un ejercicio de confianza imperfecta. Blog IT-Insecurity. Recuperado de: http://insecurityit.blogspot.com.co/2016/09/proteccion-de-la-informacion-un.html

Cloutier, R. (2016) *Becoming a Global Chief Security Executive Officer. A how to guide for next generation security leaders.* Kidlington, UK: Butterworth-Heinemann.

Cooper, T., Siu, J. y Wei, K. (2015) Corporate digital responsability. Doing well by doing good. Accenture research. Recuperado: https://www.accenture.com/t20150521T071950__w__/us-en/_acnmedia/Accenture/Conversion-Assets/Outlook/Documents/2/Accenture-Corporate-Digital-Responsibility-Web-PDF-V2.pdf

Deloitte (2016) Assessing cyber risk: Critical questions for the board and the C-suite. Recuperado de: http://www2.deloitte.com/global/en/pages/risk/articles/assessing-cyber-risk.html

Ernst & Young (2013) Technology risk management in a cyber world. A C-suite responsibility. Recuperado de: http://www.ey.com/Publication/vwLUAssets/Technology_risk_management_in_a_cyber_world-a_C-suite_responsibility_-_5_Insights_for_executives/$FILE/Technology_risk_management_in_a_cyber_world-a_C-suite_responsibility-5_Insights_for_executives.pdf

Frappolli, M. (2015) *Managing cyber risk.* Malvern, Pennsylvania. USA: American Institute for Chartered Property Casualty Underwriters.

Johansen, B. (2009) *Leaders Make the Future: Ten New Leadership Skills for an Uncertain World.* San Francisco, USA: Berrett-Koehler Publishers.

Kaplan, J., Bailey, T., O'Halloran, D., Marcus, A. y Rezek, C. (2015) *Beyond cybersecurity. Protecting your digital business.* Hoboken, New Jersey. USA: Wiley.

KPMG (2015) Global CEO Outlook – Energy perspective. Recuperado de: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/03/global-CEO-outlook-energy-perspective.pdf

Mcafee (2016) Mcafee Labs 2016 threats predictions. Recuperado de: http://www.mcafee.com/uk/resources/reports/rp-threats-predictions-2016.pdf

Moraleda, E. (2014) *Los retos del directivo actual. Conductas, competencias y valores imprescindibles del profesional del siglo XXI.* Barcelona, España: Gestión 2000.

Paloalto – NYSE (2015) Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers. Chicago, Illinois. USA: Caxton Business & Legal, Inc. Recuperado de: https://www.securityroundtable.org/wp-content/uploads/2015/09/Cybersecurity-9780996498203-no_marks.pdf

Phadnis, S., Caplice, C. y Sheffi, Y. (2016) How Scenario Planning Influences Strategic Decisions. *Sloan Management Review. Summer.*

Porter, M. y Heppelmann, J. (2014) How Smart, connected products are transforming competition. *Harvard Business Review.* Noviembre.

Porter, M. y Heppelmann, J. (2015) How Smart, connected products are transforming companies. *Harvard Business Review.* Octubre.

Prahalad, C. K. y Hamel, G. (1990) The core competence of corporation. *Harvard Business Review.* May-June.

PwC (2013) Building digital trust. The confidence to take risk. Recuperado de: https://www.pwc.com/sg/en/publications/assets/build_digital_trust_201312.pdf

Rogers, D. (2016) *The digital transformation playbook. Rethink your business for the digital age.* New York, USA: Columbia University Press.

Rowsell-Jones, A. (2013) Su empresa también tiene ventaja digital. *IESE Insight.* Tercer trimestre. No. 18.

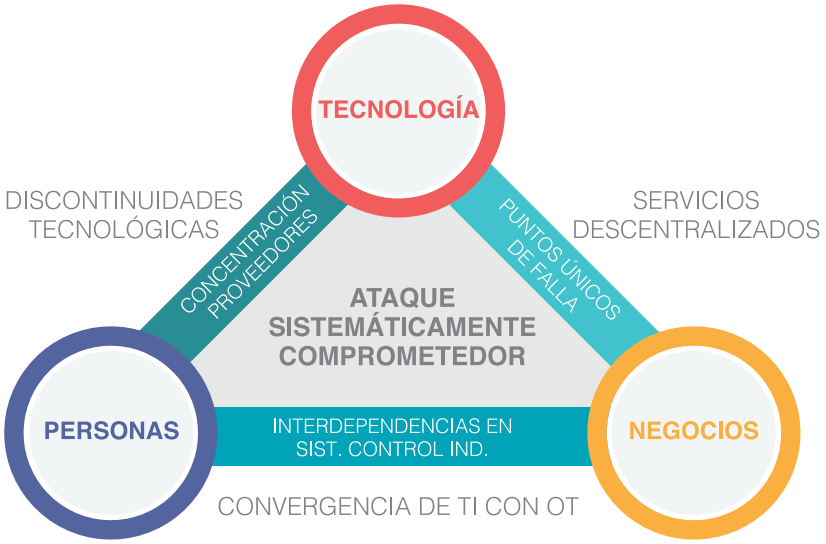
Scholtz, T. (2016) Security and risk leadership visión for 2017. *Gartner Report.*

Scholtz, T. (2016b) Managing risk and security at the speed of digital business. *Gartner Report.*

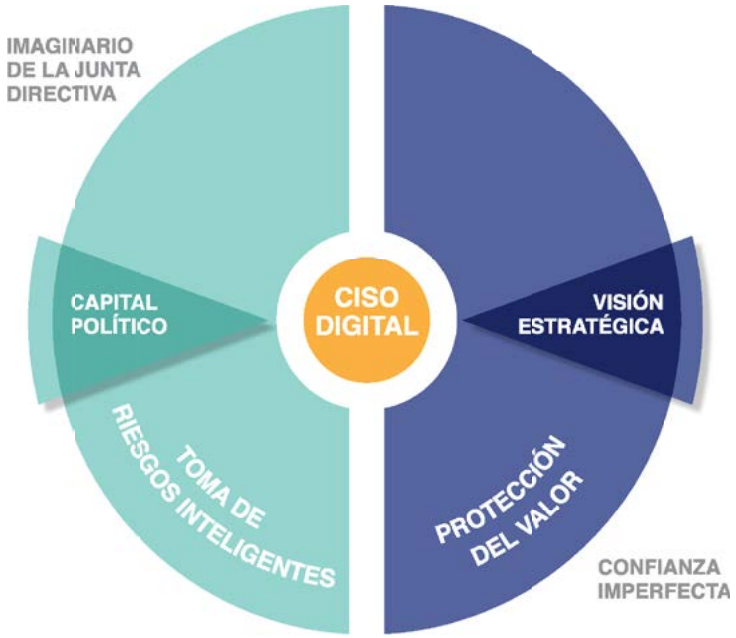
Schwab, K. (2016) The Fourth Industrial Revolution: what it means, how to respond. Recuperado de: https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

6. Anexos

1. Ataques sistémicamente comprometedores



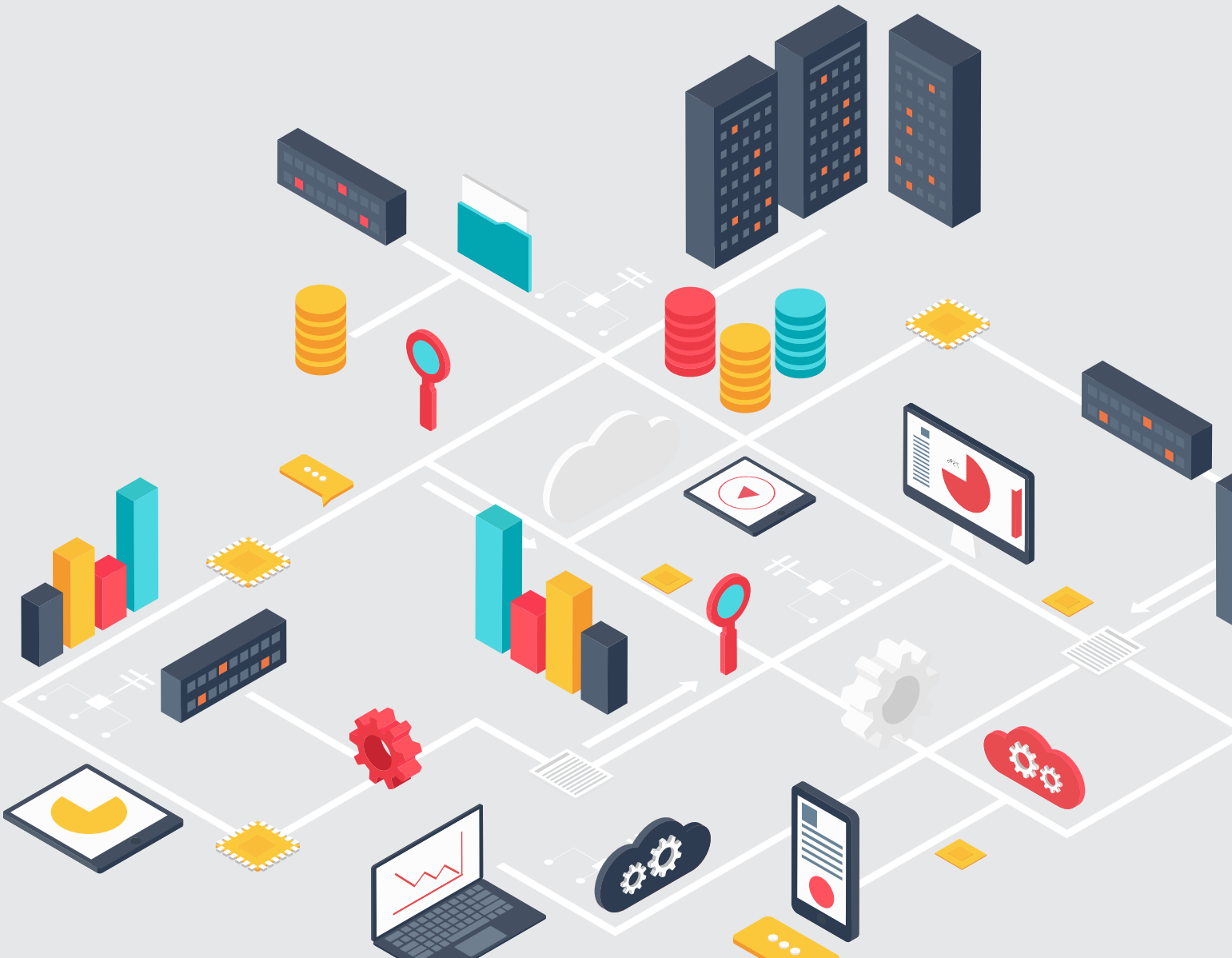
2. Consideraciones claves de un CISO en la era digital



Autor: **Jeimy J. Cano**

Profesor Distinguido, Facultad de Derecho. Universidad de los Andes, Colombia.

Miembro investigador del Grupo de Estudios en Comercio Electrónico, Telecomunicaciones e Informática (GECTI) de la Facultad de Derecho y profesor distinguido de la misma Facultad, Universidad de los Andes, Colombia. Ingeniero y Magíster en Ingeniería de Sistemas y Computación de ese mismo claustro educativo. Especialista en Derecho Disciplinario de la Universidad Externado de Colombia. Ph.D in Business Administration de Newport University, CA. USA. y Ed.D.(c) – Candidato a Doctor en Educación por la Universidad Santo Tomás, Colombia. Executive Certificate in Leadership and Management del MIT Sloan School of Management, Boston. USA. Egresado del programa de formación ejecutiva Leadership in 21st Century. Global Change Agent, de Harvard Kennedy School of Government, Boston. USA. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y COBIT5 Certificate. Director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas – ACIS.
Entre sus publicaciones se encuentran: “Computación Forense. Descubriendo los rastros informáticos” e “Inseguridad de la información. Una visión estratégica” ambos publicados por la editorial Alfaomega.
Recientemente ha recibido el reconocimiento como “Cybersecurity Educator of the Year 2016” por el Cybersecuriy Excellence Awards. Su blog: http://insecurityit.blogspot.com y twitter: @itinsecure.



WHITE PAPER

Ruta estratégica de ciberseguridad empresarial

Un marco de orientación directiva

ASOCIACIÓN REGIONAL DE EMPRESAS DEL SECTOR
PETRÓLEO, GAS Y BIOCOMBUSTIBLES
EN LATINOAMÉRICA Y EL CARIBE.

ARPEL es una asociación sin fines de lucro que nuclea empresas e instituciones del sector petróleo, gas y biocompustibles en Latinoamérica y el Caribe. Fue fundada en 1965 como vehículo de cooperación y asistencia recíproca entre empresas del sector, con el propósito principal de contribuir actívamente a la integración y crecimiento competitivo de la industria y al desarrollo energético sostenible en la región.
Actualmente sus socios representan más del 90% de las actividades del upstream y downstream en la región e incluyen a empresas operadoras nacionales, internacionales e independientes, a proveedoras de tecnología, bienes y servicios para la cadena de valor, y a instituciones nacionales e internacionales del sector.

Sede Regional:
Javier de Viana 1018. CP 11200, Montevideo, Uruguay
Tel.: +(598) 2410 6993 | info@arpel.org.uy

www.arpel.org