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

Modelo I³.

Cautivando el interés de la junta directiva en los temas de ciberseguridad

Diciembre 2018

PUBLICACIÓN ARPEL N° MP03-2018

MEJORES PRACTICAS

Introducción

En un escenario asimétrico de información y con cambios permanentes a nivel político, económico, social, tecnológico y normativo, las organizaciones se encuentran en tensión permanente para enfrentar las discontinuidades provocadas por nuevas propuestas de actores emergentes en diferentes sectores. Bajo este panorama de incertidumbre e inestabilidad, y el aumento de flujos de información entre los diferentes actores de la cadena de suministro y los terceros de confianza que articulan la dinámica de sus negocios, los retos de la ciberseguridad empresarial se hacen evidentes ahora en las relaciones empresariales que se habilitan a través de la convergencia tecnológica y los ecosistemas digitales.

En este contexto, cautivar a los ejecutivos de primer nivel para atender una realidad que desborda los más exigentes y detallados pronósticos, requiere descubrir y conectar con un imaginario de estos directivos, para lo cual es importante comprender las características del nuevo entorno digital (5 Ds – Desintermediación, Desinstalación, Distribución, Desinformación y Deslocalización), la dinámica sistémica de los ciber riesgos y la evolución de las prácticas de protección de las infraestructuras informáticas (pasar del proteger y asegurar, al defender y anticipar).

De esta manera, la ciberseguridad empresarial como capacidad organizacional emergente, establece un referente inédito para las corporaciones, habida cuenta que en la medida que éstas comprenden que hacen parte de un ecosistema digital de negocio, pueden identificar no solamente, cómo puede ser afectadas por los terceros, sino como ella puede, con sus actividades y acciones, impactar a los miembros de dicho ecosistema (Hogg, 2017). En consecuencia, los ejecutivos no sólo tendrán que tener claridad sobre cómo protegen sus intereses y activos de la empresa, sino cómo se advierte la dinámica de los flujos de información con sus pares y terceros de confianza.

Si bien el ejercicio de gobierno corporativo, no es democrático y demanda una dosis de aprendizaje e inteligencia política (Calleja & Rovira, 2015), los retos de las organizaciones modernas, articulados desde un entorno digitalmente modificado, establecen una dinámica distinta que implica repensar lo que es conocido hasta el momento y romper con los esquemas estandarizados que los miembros del directorio tienen sobre los riesgos de la empresa.

Así las cosas, la ciberseguridad, articulada desde la distinción de los ciber riesgos, exige que los miembros de la junta directiva comprendan que las fórmulas para adquirir ventajas competitivas basadas en bajo costo, diferenciación de producto o mercados cautivos, han sido superadas, y es ahora, en el estudio en profundidad del cliente, en la articulación de una cadena logística eficiente y en la capacidad de concretar nuevas capacidades tecnológicas, donde se crean oportunidades de negocio y se abren escenarios digitalmente enriquecidos, que capturan y concretan diferentes experiencias en las personas (Weil & Woerner, 2018).

Luego, este documento introduce el Modelo I^3 (Modelo I^3: Imaginarios, Interrogantes e Inmersión) para desarrollar algunas estrategias que cautiven a los ejecutivos de las organizaciones respecto de los retos de la ciberseguridad y cómo articular sus decisiones para motivar una transformación empresarial frente al desafío de un mundo digitalmente modificado.

Las 5 D's que definen el entorno digital

La acelerada convergencia tecnológica y el aumento sostenido de la densidad digital configuran un incremento de flujos de información sobre los objetos físicos (Zamora, 2017). Smart watch, Smart Tv, Smart Phone, Smart Glass, entre otros objetos, configuran el nuevo escenario de conexiones que habilitan funcionalidades novedosas que generan experiencias distintivas en los clientes.

Esta demanda acelerada para desplegar nuevos productos y servicios, basados en la dinámica de la información de los clientes, exige una capacidad de las organizaciones para lograr una mejor lectura de las expectativas de sus usuarios, lo cual implica un incremento de interfases de datos sobre elementos físicos y por lo tanto, un mayor compromiso de la organización respecto del aseguramiento y el adecuado tratamiento de los mismos.

En este contexto, cinco conceptos (ver figura 1) definen el desarrollo de un entorno digital y tecnológicamente modificado: la Desintermediación, la Desinstalación, la Distribución, la Desinformación y la Deslocalización, los cuales estructuran la base de un nuevo conjunto de relaciones, que tanto las empresas como los individuos, configuran para concretar nuevas apuestas de valor.

La ***desintermediación*** es una tendencia que se confirma en la actualidad en diferentes emprendimientos conocidos como son Uber, Airbnb, Netflix, entre otros, donde el cliente contacta y se relaciona directamente con el proveedor del servicio, sin un tercero que medie en la relación. Esto aumenta la capacidad de negociación de las personas y mejora la experiencia en el uso del producto o servicio.

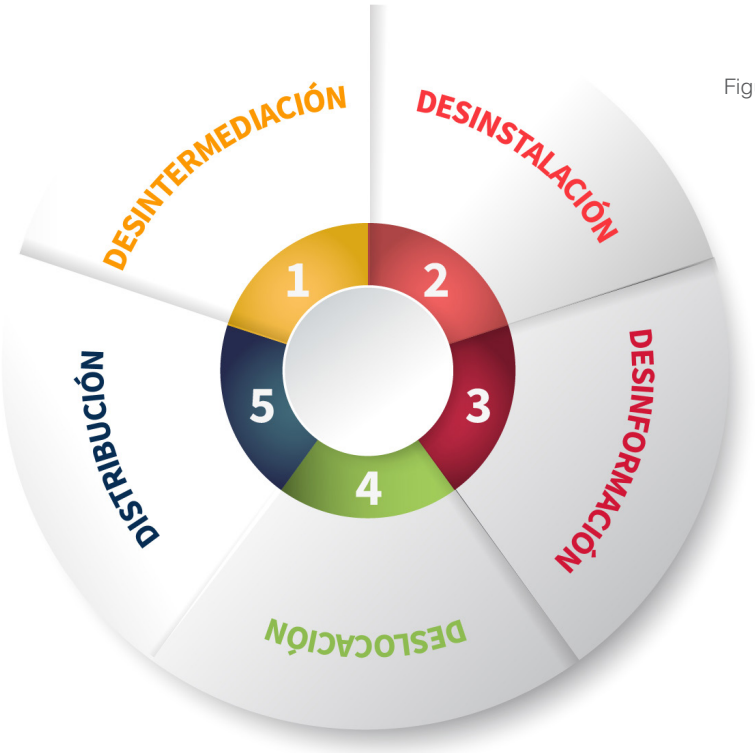


Figura 1. Cinco D's del contexto digital (Elaboración propia)

La ***desinstalación*** implica desconectarse de los medios tradiciones configurados para entrar en contacto con la empresa intermediaria, con el fin de aumentar la capacidad del cliente de crear sus propias formas de conexión y relacionamiento, para lo cual las tecnologías móviles y los objetos inteligentes establecen un referente natural que habilita una experiencia distinta donde el individuo asume el papel principal en la interacción con el proveedor.

La ***distribución*** es un fenómeno que responde a la dispersión de contactos y participantes en los nuevos ecosistemas de negocio. En este sentido, las nuevas capacidades y oportunidades se encuentran conectando distintos participantes de los ecosistemas, para crear condiciones de operación diferentes, que creen escenarios particulares donde explorar nuevas experiencias y nuevos aprendizajes tanto para el proveedor como para el cliente.

La ***desinformación*** es la nueva constante de un mundo hiperconectado y de información instantánea. Verificar o confirmar datos en una dinámica de permanentes flujos de comunicaciones, demanda desarrollar una estrategia permanente de monitorización y seguimiento de la presencia tanto de las personas como de las empresas en las redes sociales, con el fin de asegurar y mantener la integridad de su reputación.

Finalmente, la ***deslocalización*** como una tendencia a considerar en el entorno digital como la zona de localización de los objetos y servicios. Lo anterior implica pasar de una ubicación física caracterizada por un lugar y condiciones de un espacio conocido, a una virtual en la cual el acceso está a un click de distancia, con disponibilidad y servicio permanente, sin restricciones de horario y atención personalizada.

Comprender que el escenario actual responde a estos cinco conceptos, es incomodar los saberes previos sobre la estrategia y la ventaja competitiva, como quiera que lo que era estándar y conocido, ahora se mueve en zonas personalizadas, y muchas veces desconocidas, donde la comprensión de los ciber riesgos, establece una nueva frontera que hasta ahora se empieza a vislumbrar.

El ciber riesgo. Un riesgo sistémico.

La lectura de aquellas situaciones que no es posible controlar, establece el referente natural de la toma de decisiones en las empresas modernas. A mayor nivel de incierto en la decisión, mayores serán las restricciones y las inhibiciones de los ejecutivos para avanzar en este entorno actual lleno de inestabilidades y volatilidades en todos los aspectos.

En este escenario, se hace necesario comprender cuáles son las características que definen los ciber riesgos y su naturaleza sistémica, con el fin de mantener una vista proactiva que permita articular los esfuerzos y estrategias de la junta directiva, y así identificar las nuevas apuestas de valor en un mundo digitalmente modificado.

De acuerdo con Eling & Schnell (2016) un ciber riesgo está compuesto por las siguientes características:

- Una actividad no autorizada: Acciones realizadas de manera intencional o no en el contexto de la organización.
- Un agresor: Todos aquellos actores individuales o colectivos que buscan causar un daño o agresión contra un objetivo particular.
- Una vulnerabilidad: Una situación que expone a una empresa a la materialización de un evento no deseado determinada por las prácticas y estándares que la organización tiene sobre la gestión de la tecnología, sus procesos y las personas.
- Un ataque: Aprovechamiento de las vulnerabilidades conocidas o desconocidas para concretar acciones que interrumpan, deterioren, alteren, revelen o destruyan activos y/o servicios claves de la empresa.
- Una consecuencia: Los efectos que se generan basados en las intencionalidades de los atacantes.

Con este panorama conceptual de los ciber riesgos es posible advertir, que las corporaciones enfrentan un escenario asimétrico de interacciones a su interior y exterior, que puede configurarse de formas inesperadas, comprometiendo sus activos digitales estratégicos, los cuales podría llegar a caer en manos equivocadas. En razón con lo anterior, los ciber riesgos revelan su carácter sistémico (ver figura 2), que se traduce en una lectura relacional y de conexiones conocidas y emergentes cuyos impactos pueden, no sólo afectar una empresa particular, sino todo un ecosistema de participantes, donde ella actúa y desarrolla su actividad de negocio (Kaplan, Bailey, O'Halloran, Marcus, & Rezek, 2015).

Figura 2. Ciberriesgo. Riesgo sistémico (Elaboración propia)

Las características sistémicas del ciber riesgo se advierten dado que:

Los IMPACTOS son difícilmente pronosticables o cuantificables.

Las VULNERABILIDADES son inciertas y emergentes.

La CONECTIVIDAD aumenta la superficie de afectación.

El CONTEXTO es sensible a las externalidades e inestabilidades.

El incremento de la DEPENDENCIA de los terceros.

La ASIMETRÍA de la información disponible.

La acelerada CONVERGENCIA tecnológica.

Por tanto, los ciber riesgos representan un quiebre en la manera de comprender la dinámica del entorno, para repensar las expectativas y retos empresariales de cara al diseño y despliegue de nuevas propuestas de experiencias para los clientes, para concretar un ejercicio de confianza imperfecta (Cano, 2017b) donde, tanto empresa como cliente, hacen parte de un mismo ejercicio de prácticas y comportamientos de confiabilidad e integridad en el diseño, implementación y uso de un producto y servicio digitalmente modificado.

Evolución de las prácticas de protección de infraestructuras informáticas

Si bien en el pasado las prácticas que se tenían sobre la protección de la información clave de la empresa, estaban articuladas en el ejercicio de restringir el acceso, en una era de mayor conectividad y flujos de información desde objetos digitalmente modificados, esta estrategia resulta algo contraria con la necesidad de contar con la información para tomar las decisiones más relevantes que cambien el rumbo de las corporaciones.

Es así que las organizaciones han venido evolucionando y aumentando la sensibilidad de la información que manejan, como quiera que ahora es el adecuado tratamiento y uso de ésta lo que se tiene como la base del ejercicio de aseguramiento y control de la misma. En este sentido, la información fluye ahora más que el pasado dado los diferentes medios a través del cuales las personas y organizaciones interactúan, por lo que el acceso no se convierte en el reto más relevante, sino la forma cómo ésta se va a utilizar en un escenario abierto e hiperconectado.

Con este fundamento, las prácticas actuales de seguridad y control de las empresas están orientadas al proteger la información que se genera y fluye entre sus diferentes actores y componentes, para lo cual se apoya en los marcos de referencia disponibles a la fecha como son las normas ISO 27000, ISO 31000, ITIL, buenas prácticas del NIST, COBIT 5 de ISACA, entre otras, las cuales buscan cercar la incertidumbre propia de las operaciones, para tratar de hacer más predecible el ejercicio de protección que demanda la organización sobre los activos claves de información disponibles (Kovacich, 2016).

Al mantener este esfuerzo sistemático, por demás requerido para asegurar los mínimos de seguridad y control, es posible que se pierda de vista los nuevos retos emergentes que trae el aumento de la densidad digital de los objetos físicos, lo que puede generar nuevas brechas de seguridad de la información y ciberseguridad, habida cuenta de la opacidad del concepto de ciberriesgo que las empresas puedan desarrollar.

En consecuencia, considerando que las potenciales amenazas y riesgos en el contexto digital son evolutivos e inciertos, marcados por la conectividad y la necesidad de brindar una mejor experiencia a los clientes (Raban & Hauptman, 2018) , se hace necesario establecer un marco actualizado de seguridad y ciberseguridad que no sólo proteja los activos de información clave, sino que defienda los objetivos de la empresa frente a contexto adversos y anticipe posibles escenarios que puedan afectarla y dar cuenta así de la custodia de su información clave.

Esto es, defender como el entendimiento del territorio donde se mueve la organización y sus negocios, con el fin de conocer y establecer escenarios de riesgos y amenazas que permitan estudiar posibles flujos de información potencialmente valiosa, con la cual se puedan desbalancear posiciones de jugadores claves de los mercados y favorecer las estrategias planteadas por la empresa. La defensa es del valor de la información, que se concreta en funciones de inteligencia activa que reconstruyan los escenarios de actuación de la empresa.

Y de otra parte, anticipar, como la forma de concretar visiones y realidades emergentes que pronostiquen cambios inesperados y realidades imprevistas, frente a las cuales la organización pueda actuar sin mayores contratiempos, limitando impactos en su operación, reputación y valor; con la menor afectación de sus grupos de interés y la mayor claridad para la junta directiva frente a los cursos de acción definidos ante la inevitabilidad de la falla.

Modelo I^3. Cautivando el interés de la junta directiva en los temas de ciberseguridad

Todos estos cambios que se han comentado previamente revelan una realidad diferente, una manera distinta de hacer las cosas, un entendimiento del escenario actual que demanda un actuar distinto, que debe llevar a las empresas a declarar que aquello que conocían ha dejado de existir y que la dinámica corporativa, ahora exige una vista más holística y centrada en la confianza digital que los clientes requieren para potenciar las oportunidades en un contexto digitalmente modificado.

En este sentido, los cuerpos colegiados ejecutivos, como las juntas directivas, requieren comprender cómo el aumento de la densidad digital en la cotidianidad de las operaciones de la empresa y la interacción de los clientes, establecen importantes oportunidades para acelerar la apuesta de generación de valor de la empresa y así mismo, un nuevo universo de riesgos (conocidos, latentes, focales y emergentes) (Cano, 2017) que debe ser entendido al tenor de las nuevas relaciones digitales que se plantean con los consumidores, para crear experiencias totalmente distintas y retadoras que consoliden una posición estratégica para la empresa.

En consecuencia con lo anterior, se detalla a continuación el Modelo I^3 (Imaginarios, Interrogantes e Inmersión), que busca cautivar el interés de los diferentes miembros del directorio, con el fin de alinear los esfuerzos requeridos y necesarios para avanzar en el reto de la ciberseguridad empresarial, creando un entorno más allá de su comprensión técnica, para situarlo en su dimensión de negocios, que es donde realmente hace la diferencia y crea el marco de actuación ejecutiva requerido para dar cuenta del nuevo contexto digital y tecnológicamente modificado.

En primer lugar se encuentran los **imaginarios sociales**, que siguiendo la definición de Juan Luis Pintos (1999) son “aquellos esquemas, construidos socialmente, que nos permiten percibir algo como real, explicarlo e intervenir operativamente en lo que en cada sistema social se considere como realidad”. Es ese entendimiento que el ejecutivo tienen de la ciberseguridad, el cual trata de explicar desde su lectura local para hacer evidente una postura particular en este sentido. De acuerdo con ejercicios prácticos realizados en diferentes empresas y cuerpos ejecutivos, los imaginarios más frecuentes sobre la ciberseguridad identificados son:

- “Seguridad y ciberseguridad son temas de tecnología”
- “Nos podemos recuperar ante cualquier falla”
- “Tenemos capacidades y competencias para lo inesperado”
- “Incorporar tecnología avanzadas nos hace resistentes”
- “Podemos atender incidentes como otros lo hacen”

En segundo lugar, se tienen los **interrogantes**, que representan las preguntas que los directivos tienen sobre la ciberseguridad, los cuales generalmente responden a los imaginarios que se tiene sobre la temática. Cada interrogante lo que busca encontrar puntos de certezas que le permitan al ejecutivo tratar de advertir si ha tenido el debido cuidado para darle la importancia y no tener opacidades en las decisiones que tomen a este respecto. Las preguntas frecuentes son:

- ¿Estamos seguros?
- ¿Cómo sabemos que hemos tenido una brecha de seguridad?
- ¿Cómo se compara nuestro programa de seguridad con los de la industria?
- ¿Tenemos suficientes recursos para apoyar el programa de ciberseguridad?
- ¿Qué tan efectivo es nuestro programa de seguridad, y está nuestra inversión alineada adecuadamente? (Hellickson, 2018)

En tercer lugar, se tiene la **inmersión**, es decir, el conocimiento detallado de la estrategia de ciberseguridad, ese marco de trabajo que demanda la organización para avanzar en el reto de comprender el nuevo escenario de ciberriesgos y las asimetría del entorno, con el fin de generar una postura organizacional que le permite defender y anticipar amenazas y riesgos emergentes. Para ello, es necesario que los directivos conozcan con algunos detalles de cómo se adelanta la gestión del riesgo, los temas de gobierno, políticas y procedimientos, cómo se involucra la participación interna y colaboración externa frente a estos eventos y finalmente la cultura de ciberseguridad, alineada con el reto de los ciberriesgos.

A continuación un cuadro (figura 3) con el detalle de cada uno de los temas mencionados:

GESTIÓN DE RIESGOS	¿Cuáles son nuestros datos más importantes y quién puede acceder a ellos? ¿Cuáles son nuestros activos más importantes?
	¿Cuánto riesgo cibernético, físico y de marca podemos permitirnos?
	¿Cómo abordamos el riesgo de los proveedores, socios y ecosistemas? ¿Cómo nos fanamos la confianza del consumidor?
GOBIERNO, POLÍTICAS Y PROCEDIMIENTOS	¿A quién pertenece la ciberseguridad y el ciberriesgo en nuestra organización, y cómo se les presta apoyo?
	¿Cómo se han implementado los procesos y políticas de ciberseguridad y gestión de riesgos cibernéticos?
	¿Cuándo probamos por última vez nuestra red y nuestro proceso de respuesta a incidentes preguntándonos “¿y si...?”
PARTICIPACIÓN EXTERNA Y COLABORACIÓN INTERNA	¿Estamos compitiendo con otras empresas en ciberseguridad o colaborando con ellas?
	¿Están trabajando juntas nuestras funciones de ciberseguridad, seguridad y gestión de calidad?
CULTURA DE CIBERSEGURIDAD	¿Hemos establecido una cultura apropiada de ciberriesgo en nuestra organización?
	¿Cómo utilizamos nuestra cultura de ciberseguridad para hacer posible nuestras estrategias empresariales y digitales?

Figura 3. Estrategia de ciberseguridad. Traducido de: Deutscher, S., Bohmayr, W. y Asen, A. (2017) Develop a Cybersecurity Strategy as if Your Organization's Existence Depends on It. BCG Research. October. Recuperado de: https://www.bcg.com/publications/2017/technology-digital-develop-cybersecurity-strategy-your-organization-existence-depends-it.aspx

Finalmente, se tiene una vista integral de los tres componentes que permite comprender y cautivar la junta directiva, a través de los cruces de estos elementos, es decir cómo la ciberseguridad hace la diferencia en la práctica general de los negocios. En la figura 4, se advierten las tres palabras claves (verificación, brechas y gestión) que permiten tener la información necesaria y enviar los mensajes claros a los ejecutivos de primer nivel sobre la ciberseguridad y cómo ellos suman en el ejercicio de cuidar la promesa de valor de la empresa en el contexto digital.

Figura 4. Modelo I³ (Elaboración propia)

La verificación, que es el ejercicio de confrontación de los imaginarios sociales de los ejecutivos frente a lo que la estrategia de ciberseguridad les dice, les propone y se despliega en la organización. Es una vista práctica de cómo se construye una distinción de ciberseguridad compartida, basada en hechos y datos que hacen parte de la realidad de la organización.

Las brechas representan las respuestas que aún no se responden desde su imaginario y que se materializan en las preguntas propias de sus cargos, toda vez que es necesario tener un marco de debida diligencia frente a la temática y sus diferentes interrogantes buscan encontrar las respuestas más concretas posibles para poder responder frente a un futuro juicio de responsabilidades (Boney, Hayslip, & Stamper, 2018) en el caso de un evento inesperado que comprometa la promesa de valor de la empresa.

La gestión representa cómo la organización actúa de forma regular frente a la estrategia de ciberseguridad, guiada por los interrogantes de los ejecutivos de primer nivel, con el fin de mantener una postura proactiva y de aseguramiento que permita movilizar a toda la organización frente a los retos de la ciberseguridad. No es un ejercicio más de gestión basado en un estándar, sino una declaración de defensa del valor de los activos digitales de la empresa, los cuales representan las nuevas experiencias de los clientes en un contexto digitalmente modificado.

Consolidar la práctica de cautivar a la junta directiva en los temas de ciberseguridad, implica dar respuesta a las tres palabras clave previamente desarrolladas, teniendo en cuenta que si bien, no existe cero riesgos, ni seguridad ciento por ciento, es posible establecer umbrales de riesgo concretos donde la organización conoce y aprende todo el tiempo sobre cómo anticipar sus riesgos, y a mantener una práctica de gestión de incidentes activa, que permite atender cualquier eventualidad de forma coordinada y confiable para sus diferentes grupos de interés.

Estrategias prácticas para cautivar a la junta directiva sobre la ciberseguridad

Aplicar el Modelo I³ demanda una comprensión concreta de la realidad de la organización en los temas de ciberseguridad. De igual forma, es necesaria una mirada en perspectiva global que permita contrastar el ejercicio interno y establecer la brecha permanente que los diferente agentes nocivos crean, para mantener la natural tensión creativa entre aquellos que tratan de defender la promesa de valor de las empresas y aquellos que retan constantemente sus supuestos de protección, más allá de las conocidas vulnerabilidades técnicas.

En este sentido, se presenta la siguiente propuesta de acciones prácticas que permiten conectar los diferentes intereses de las juntas directivas sobre el tema de ciberseguridad y avanzar en su sensibilización y concientización, piezas clave para sintonizar los retos que el contexto digital presenta a todas las empresas.

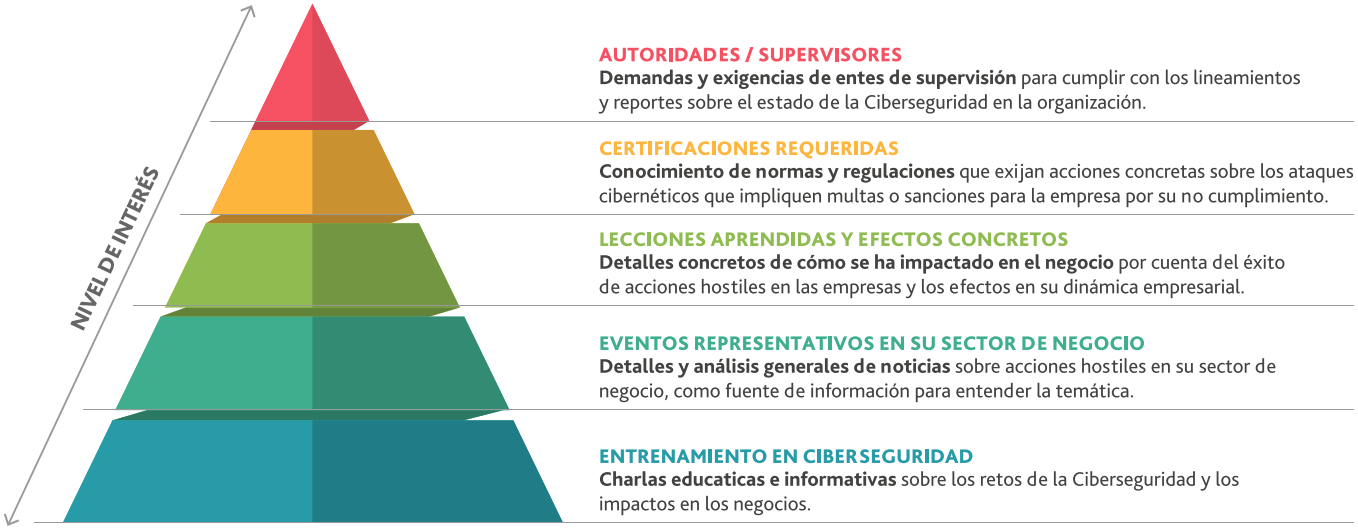


Figura 5. Estrategias prácticas para cautivar a la Junta Directiva sobre ciberseguridad (Elaboración propia)

El entrenamiento en ciberseguridad, son las tradicionales charlas educativas e informativas que los encargados de seguridad o ciberseguridad presentan a los ejecutivos con el fin de mantenerlos informados de los cambios de estrategias de los atacantes en escenarios cada vez más interconectados y de mayores flujos de información. Si bien estas presentaciones deben ser ilustrativas y motivadoras, su uso permanente, no causa toda la impresión requerida si se hace repetitiva y sin mayores novedades, y si no viene acompañada de otros elementos o testimonios que sorprendan a la audiencia.

Los eventos representativos en su sector de industria, permiten establecer un análisis de noticias sobre las acciones hostiles en su sector de operaciones, que habilita un mejor entendimiento de la problemática en contexto y ayuda a situar a la organización en los retos que este tipo de actividades adversas genera, no solamente para los temas técnicos, sino sus implicaciones para los negocios. Hablar desde la perspectiva de procesos e impactos en la industria, permite conectar con la audiencia y sus intereses, rompiendo el paradigma de lo técnico y acercándolo a la realidad de los clientes de la empresa.

Las lecciones aprendidas y efectos concretos, hablan de los hechos y datos que han ocurrido en empresas particulares. Identificar y conseguir información propia de organizaciones de la industria con casos específicos, suele ser una tarea complicada y restrictiva. Sin embargo, es clave adquirirla bien por canales oficiales o ejercicios de benchmarking propios o con terceros de confianza, para establecer una base conceptual sólida desde la cual acompañar las reflexiones de los ejecutivos de la empresa. Las lecciones aprendidas son precisamente los aprendizajes que las empresas han logrado y la manera como se preparan en adelante para anticipar los nuevos retos.

Las certificaciones requeridas hablan de aspectos regulatorios que las empresas deben cumplir en los temas de ciberseguridad. Es una ilustración pedagógica y formal de las implicaciones de las normas vigentes sobre el tema y la manera en que la organización está asumiendo el reto de su cumplimiento. Esta temática supone un esfuerzo de nivel corporativo, que bien puede ser liderado por el encargado de los temas de ciberseguridad, deberá contar con el respaldo de los ejecutivos de primer nivel, habida cuenta que las posibles sanciones que se derivan de su no cumplimiento afectan el capital político de los miembros de los directorios.

Finalmente las demandas y exigencias de entes de supervisión, son las que mayor interés causan entre los ejecutivos, habida cuenta que en el cumplimiento de las reglas de regulador no caben puntos medios o negociaciones alternas, sino hacer evidente el nivel de avance de la organización sobre la temática. En este escenario, la organización debe demostrar su debido cuidado y diligencia, y las estrategias concretas que tiene para dar cuenta con los detalles que la norma establece. De no hacerlo, sabe que se expone a pérdida de reputación y confianza en su sector, el cual permanece a la vista de sus diferentes grupos de interés.

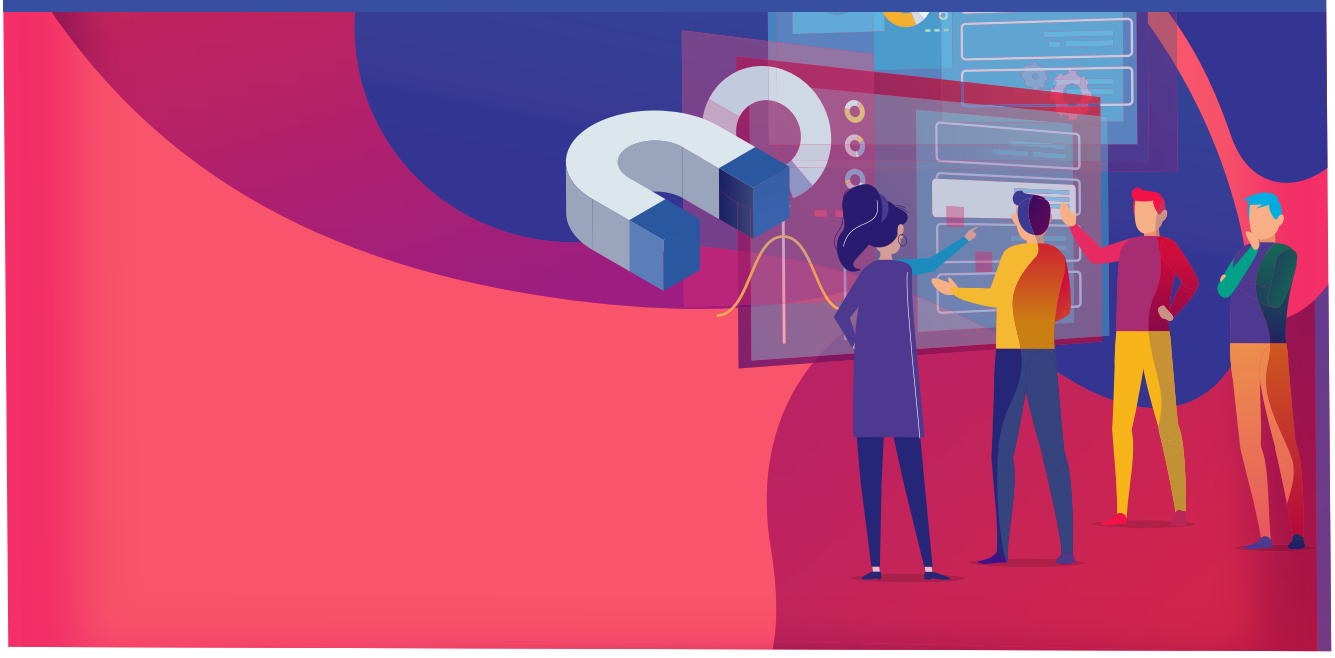
Conclusiones

Cautivar a la junta directiva no es un ejercicio de cifras o números concretos, es una declaración de acciones decididas que revelan y detallan los inciertos y vacíos alrededor de la ciberseguridad, para tener un fundamento claro y preciso sobre los retos y avances de la organización sobre el contexto cibernético.

En este escenario, la sensibilización, la concientización y el detalle normativo, juegan un papel fundamental a la hora de comprender los “porqués” y la importancia de tomar en cuenta los impactos de los ciberataques, elementos claves requeridos, cuando de mirar y explorar nuevas oportunidades en el contexto digital se trata (Bissell, LsSalle, & Richards, 2017).

Los ejecutivos de primer nivel inmersos en una sociedad digital y tecnológicamente modificada que piensan que “conocen los riesgos” estarán creando una zona de opacidad de vulnerabilidades y amenazas latentes, que aumentará la exposición de sus negocios frente a las exigencias de las nuevas experiencias de sus clientes. En consecuencia, se hace necesario desarrollar una postura de falla segura y acciones de respuesta resilientes de tal forma que la ciberseguridad sea una distinción natural de la forma como se hacen negocios en el escenario actual (Portilla, Vázquez, Harreis, Pancaldi, Rowshankish, & Samandari, 2017).

Cautivar al directorio con el tema de la ciberseguridad, debe crear una zona de confianza, una ventana de aprendizaje y una construcción colectiva, donde los intereses de la empresa y las exigencias de los clientes, le den forma a las decisiones y acciones concretas que la organización debe tomar para defender y anticipar las amenazas emergentes y así, establecer un marco general de responsabilidad demostrada que de cuenta de los requerimientos de los reguladores, las expectativas de los ejecutivos, los retos de los atacantes y los impactos en los grupos de interés.



Referencias

Bissell, K., LsSalle, R. & Richards, K. (2017) *The Cyber-committed CEO and Board. Accenture.* Recoved from: https://www.accenture.com/us-en/insight-cyber-committed-ceo

Boney, B., Hayslip, G. & Stamper, M. (2018) *CISO Desk Reference Guide. A practical guide for CISOs.* Volumen 2. San Diego, CA. USA: CISO DTG Joint Venture Publishing.

Calleja, L. & Rovira, M. (2015) *Gobierno institucional. La dirección colegiada.* Navarra, España: Ediciones Universidad de Navarra (EUNSA).

Cano, J. (2017) *The AREM Window: A Strategy to Anticipate Risk and Threats to Enterprise Cyber Security.* ISACA Journal. 5.

Cano, J. (2017b) *Riesgo y seguridad. Un continuo de confianza imperfecta.* En Dams, A., Pagola, H., Sánchez, L. y Ramio, J. (eds) (2017) Actas IX Congreso Iberoamericano de Seguridad de la Información. Universidad de Buenos Aires - Universidad Politécnica de Madrid.

Deutscher, S., Bohmayr, W. y Asen, A. (2017) *Develop a Cybersecurity Strategy as if Your Organization's Existence Depends on It.* BCG Research. October. Recuperado de: https://www.bcg.com/publications/2017/technology-digital-develop-cybersecurity-strategy-your-organization-existence-depends-it.aspx

Eling, M. & Schnell, W. (2016) *What do we know about cyber risk and cyber risk insurance?* The Journal of Risk Finance. 17(5). 474-491. Doi: https://doi.org/10.1108/JRF-09-2016-0122

Hellickson, J. (2018) CISOs: H*ow to Answer the 5 Questions Boards Will Ask You.* Darkreading. Recuperado de: https://www.darkreading.com/vulnerabilities---threats/cisos-how-to-answer-the-5-questions-boards-will-ask-you/a/d-id/1332914

Hogg, J. (2017) *Why the Entire C-Suite Needs to Use the Same Metrics for Cyber Risk.* Harvard Business Review. Noviembre. Recuperado de: https://bit.ly/2mz3Nc2

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

Kovacich, G. (2016) *The information systems security officer's guide. Establishing and Managing a cyber security program.* Third Edition. Kidlington, Oxford. UK.: Butterworth-Heinemann

Pintos, J. (1999) *Los imaginarios sociales del delito: La construcción social del delito a través de las películas* (1930-1999). Recuperado de: http://idd00qmm.eresmas.net/articulos/delitocine.htm

Portilla, A., Vázquez, J., Harreis, H., Pancaldi, L., Rowshankish, K. & Samandari, H. (2017) *The future of risk management in the digital era. R*esearch Report. Institute of International Finance – Mckinsey & Company. October. Recuperado de: https://www.mckinsey.com/business-functions/risk/our-insights/the-future-of-risk-management-in-the-digital-era

Raban, Y. & Hauptman, A. (2018) *Foresight of cyber security threat drivers and affecting technologies*, Foresight, https://doi.org/10.1108/FS-02-2018-0020

Weil, P. & Woerner, S. (2018) *What's your digital business model? Six questions to help you build the next-generation enterprise.* Boston, Massachusetts. USA: Harvard Business Review Press.

Zamora, J. (2017) *¿Es posible programar modelos de negocio?* IESE Insight. II Trimestre.

Autor: **Jeimy J. Cano**

Ph.D, CFE, CICA

Ingeniero y Magíster en Ingeniería de Sistemas y Computación por la Universidad de los Andes. Especialista en Derecho Disciplinario por la Universidad Externado de Colombia. Ph.D en Business Administration por Newport University, CA. USA. y Ph.D en Educación por la Universidad Santo Tomás, Colombia. Cuenta con más de 20 años de experiencia como académico, ejecutivo y profesional en seguridad de la información, privacidad, ciberseguridad, sistemas de información, gobierno y auditoría de TI. En 2016 recibió el reconocimiento como "Cybersecurity Educator of the year 2016" para América Latina por el Cybersecurity Excellence Awards. Es Examinador Certificado de Fraude (CFE), Auditor Certificado de Control Interno (CICA) y Certificado Ejecutivo en Liderazgo y Gestión de MIT Sloan School of Management. Cuenta con más de 160 publicaciones en revistas y eventos internacionales. Así mismo, ha sido conferencista invitado en foros y congresos nacionales e internacionales sobre temas de seguridad y control en América Latina. A la fecha es miembro del Grupo de Estudios en Comercio Electrónico Telecomunicaciones e Informática – GECTI y profesor distinguido de la Facultad de Derecho de la Universidad de los Andes.

MEJORES PRACTICAS

Modelo I³. Cautivando el interés de la junta directiva en los temas de ciberseguridad

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 a empresas e instituciones del sector petróleo, gas y biocombustibles en Latinoamérica y el Caribe. Fue fundada en 1965 como un vehículo de cooperación y asistencia recíproca entre empresas del sector, con el propósito principal de contribuir activamente 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:
Av. Luis A. de Herrera 1248. WTC. Torre 2. Piso 7. Of. 717.
CP 11300. Montevideo, Uruguay
Tel: (+598) 2623-6993 • info@arpel.org.uy

www.arpel.org