LA TRANSFORMACIÓN DIGITAL DE LOS MERCADOS, UNA MIRADA A TRAVÉS DE LA SEGURIDAD DE LA INFORMACIÓN Y LA RELACIÓN DEL NEGOCIO CON TECNOLOGÍA.

Rojas Alarcón, Miguel Andrés
'rmiguel1016@gmail.com'
Universidad Piloto de Colombia

***Abstract* —** In this article, different aspects that have been changing industries by generating high competition will be mentioned. One of these components is the digital transformation, which has increased markets to expand digital ability in processes, products, and assets to improve operating efficiency and customer value, manage risk and discover new income generation opportunities. Another factor involved in this process is the information security component, which allows to protect different assets that are part of the operation and the delivery of both internal and external service, in the same way, not being one of the least important factors, there is the relationship between the business and the technology area, which facilitates and optimizes the operation of different transversal components of the business.

***Index Terms* —** Digital Transformation, Business, Cyber-Security and IT Area**.**

***Resumen* —** En el presente documento, se mencionarán diferentes aspectos que han venido transformando las industrias y los mercados que generan alta competencia. Uno de estos componentes que es la transformación digital, que ha impulsado a los mercados a la ampliación de las capacidades digitales en los procesos, productos, y activos para mejorar la eficiencia de operación, mejorar el valor al cliente, gestionar el riesgo y descubrir nuevas oportunidades de generación de ingresos. Otro de los factores involucrados en este proceso, es el componente de seguridad de la información, que permite asegurar diferentes activos que hacen parte de la operación y de la entrega de servicio tanto interna como externa, asimismo, no siendo uno de los factores menos importantes, está la relación del negocio y del área de tecnología, la cual permite facilitar y optimizar la operación de diferentes componentes transversales del negocio.

***Índice de términos* –** transformación digital, negocio, ciber-seguridad y el área de TI.

I. INTRODUCCIÓN

Durante el crecimiento industrial se han venido involucrando diversos factores que han sido apoyo transversal para las operaciones de negocio, en donde se ven involucradas diversas áreas que permiten gestionar la operación continua de cada negocio. El mercado se ha venido fortaleciendo a través de diversas tecnologías emergentes, que han apoyado a la gestión de diferentes mercados, optimizando la operación de los negocios con infraestructura de alto rendimiento, administración en la nube, internet de las cosas, Ciber-Security, Robotic Process Automatization (RPA), entre otros. Las cuales se han involucrado en el mercado de manera progresiva; sin embargo, la adopción o la inclusión de éstas en la operación ha generado nuevas tendencias que inician un proceso de gestión y permiten la toma de decisión a nivel organizacional.

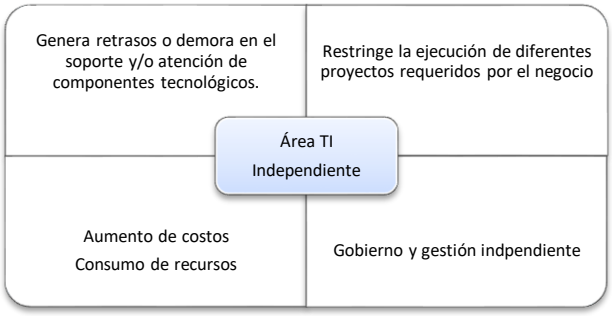
Ahora bien, ¿de dónde nace el termino de transformación digital?, a partir de las diferentes tecnologías que han posicionado en el mercado, las empresas tienden a perfeccionar su operación, no sólo desde el punto de vista de gestión, sino de apoyarse transversalmente en dicha tecnología. Sin embargo, la transformación digital tiene un horizonte más profundo, debido que baja hasta el modelo de negocio, en donde se involucran diferentes áreas como, por ejemplo, el negocio y sus áreas de apoyo. Como lo cita la revista Dinero, en uno de sus artículos "El cuento de la transformación digital", del 08 de junio de 2018, "…*La transformación digital es el resultado del cambio organizacional donde las personas, los procesos y el modelo de negocio, entienden a la tecnología como una herramienta para generar valor entre sus consumidores y colaboradores*" [1].

No obstante, el desenvolvimiento que trae la transformación digital habilita diferentes entornos o medidas que las compañías deben fortalecer, como por ejemplo sus sistemas de gestión y

control, procesos como seguridad de la información y/o un poco más abajo, seguridad informática, que son temas transversales que apoyarán al aseguramiento de la transformación de cada empresa. A continuación, se detallará sobre el gobierno y la gestión de estos componentes según prácticas estándar del mercado y asimismo, algunos puntos de vista que se tienen desde el negocio y el área de apoyo de TI.

II. Interacción entre el negocio y el área de TI

Durante el crecimiento de las compañías y de la competencia entre mercados, se han identificado diferentes variaciones que han hecho que el negocio vea al área de TI como:



Sin embargo, con el impacto tecnológico que han enfrentado las empresas ha generado una nueva visión sobre el área de TI, en donde los nuevos componentes tecnológicos están fortaleciendo la toma de decisiones, la operación, la efectividad de procesamiento de la información, la optimización de procesos, entre otros. Con el paso del tiempo, la inclusión de componentes tecnológicos en cada área de operación y de apoyo, ha llevado a que el área de TI es parte estructural de las empresas, debido que se ha convertido en la base para administrar la contabilidad, activos, finanzas, clientes, proveedores, recursos humanos, entre otros, a través de los componentes tecnológicos (infraestructura, aplicaciones, dispositivos móviles entre otros) que soportan la operación de cada proceso mencionado.

Con base en lo anterior, Francisco Gonzalez, Socio de KPMG, en el artículo "El área de TI como generador de valor en el negocio", menciona que "*...Para que esta arquitectura funcione de manera adecuada es necesario que los Directores de Tecnología (también conocidos como CIO, por las siglas de Chief Information Officer) ocupen un lugar estratégico en el organigrama de la empresa...*" [2]. Esto hace referencia a que el entorno cambiante que han tomado las industrias ha llevado a que el área de tecnología se convierta en un aliado estratégico de las compañías debido que a través de las tecnologías emergentes que han surgido, se ha logrado fortalecer los siguientes aspectos:

- Optimización de recursos.
- Eficacia operativa.
- Toma de decisiones.
- Crecimiento empresarial.
- Alta competencia en cada industria.

Sin embargo, un estudio realizado por EY Colombia revela que el 55% de Compañías no hacen de la protección cibernética de la organización un elemento integral de su estrategia de negocios y sus planes de ejecución. No obstante, de acuerdo con lo descrito en el artículo, *"...la mayoría de las organizaciones (77%) ahora buscan ir más allá de las técnicas básicas de seguridad cibernética para perfeccionar sus capacidades, haciendo uso de tecnologías avanzadas como inteligencia artificial, automatización robótica de procesos y analítica de datos, entre otras. Estas organizaciones continúan trabajando en sus aspectos esenciales de ciberseguridad, pero también están reconsiderando su marco de trabajo y arquitectura frente a este tema para soportar la estrategia de negocio de manera más efectiva y eficiente. Sin embargo, la encuesta encontró que sólo el 8% de los encuestados considera que su función de seguridad de la información satisface las necesidades del negocio en la actualidad..."*. [3]

Con base en el estudio realizado por EY Colombia, identificamos que no sólo las tecnologías apoyan el crecimiento de la operación de negocio, sino que a su vez apoyan los mecanismos de protección que pueden contemplar las compañías, para así optimizar los procesos de monitoreo y levantar las acciones necesarias y oportunas frente alguna debilidad de seguridad explotada en la compañía.

Seguido de la inclusión de la transformación digital Posada, Gerente de EY Colombia, afirma que *"las organizaciones están invirtiendo cada vez más en tecnologías emergentes como parte de sus programas de transformación digital, y si bien han creado nuevas posibilidades de negocio, también se generan nuevas vulnerabilidades y amenazas..."* [3]. Lo que conlleva a que la transformación digital es un apoyo indispensable para el crecimiento organizacional, sin embargo, las compañías no deben perder su visión frente el aseguramiento y protección de sus recursos, debido que el impacto que genera la transformación trae consigo nuevas brechas que la operación continua del negocio no contempla desde su inicio.

III. Estrategia, Ambiente de Control y Seguridad de la Información

Diferentes compañías han fortalecido los esquemas de aseguramiento para proteger su operación y negocio, a través de mecanismos que han sobre salido en la industria, tales como las prácticas de referencia que han movilizado y fortalecido los esquemas de control y seguridad. Ahora bien, con la transformación digital, la inclusión de nuevos componentes de tecnología y los recurrentes ataques de seguridad, las compañías empiezan a establecer los mecanismos suficientes para fortalecer el aseguramiento de sus áreas de operación a través los siguientes componentes:

- Áreas estratégicas de toma de decisión.
- Ambiente de control interno.
- Seguridad de la información / Seguridad Informática.

Para el fortalecimiento de estas áreas, el mercado ha venido estableciendo diferentes estándares, frameworks, líneas base, entre otros, tales como:

- Lineamientos de gobierno.
- Lineamientos de gestión / operación.
- Estructura de servicios.
- Gestión de riesgos.
- Diseño e implementación de controles.
- Estructura de procesos.
- Métricas de desempeño.

A continuación, se relaciona para cada área mencionada, algunos de los componentes clave para movilizar la gestión de la transformación digital de las Compañías.

A. Áreas estratégicas de toma de decisión.

Como bien lo define el marco de referencia COBIT 5, en su proceso "APO02 – Gestionar la Estrategia", el cual estable que "*Optimizar la contribución al valor del negocio desde los procesos de negocio, de los servicios TI y activos de TI resultado de la inversión hecha por TI a unos costes aceptables.*" [4], identificamos que las Compañías deberían definir transversalmente a través del negocio, servicios y activos, los componentes que deben tener el enfoque de soporte necesario y asimismo, el aseguramiento sobre cada uno de ellos.

Por ejemplo, la inclusión de nuevas tecnologías las cuales nos incluye la transformación digital, habilitan a que las compañías re-modelen sus procesos de negocio, modelo de negocio, tiempos de atención y respuesta, entre otros, sobre toda su operación actual. Esto hace referencia que las empresas pueden incluir:

- Personal profesional.
- Tecnología
- Procesos.
- Capacitaciones
- Clientes - Proveedores

Entre otros, sobre los cuales es necesario aplicar todo tipo de esquema de seguridad, el cual les permita dar confianza sobre su operación a los nuevos clientes y proveedores que les permitirán crecer en el mercado e inclusive cambiar el paradigma de su empresa.

Áreas de seguridad de la información hacen que las Compañías establezcan menos focos de atención debido que es un área pasiva que según el comportamiento del negocio, no genera rentabilidad sobre sus productos o servicios finales, sin embargo, el hecho de no operar en conjunto, si hace que las compañías pierdan valor, nombre, productos, información, entre otros. Lamentablemente, las Compañías no deciden invertir en este tipo de áreas de apoyo que son transversales a su operación, debido que hasta que no les sucede un incidente de seguridad crítico, ellos ven el área común a las demás.

Ahora bien, analizando el panorama general de los ataques realizados, en el reporte de ESET "Security Report, Latinoamérica 2018", la Compañía identifica que durante el 2017 aumentaron los ataques relacionados con randsomware, debido que ha venido evolucionando gracias a la rentabilidad que les ofrece a los atacantes.

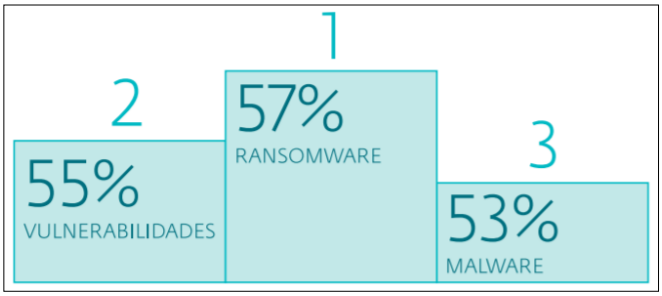


Imagen No. 1 (Referencia del reporte de seguridad de ESET, Latinoamérica 2018, página 04) [5]

Seguido de esto, se encuentran las vulnerabilidades por falta de aseguramiento de componentes de infraestructura y aplicaciones, por último, los malware o código malicioso que se aprovecha de algunos huecos de los sistemas de información e inclusive del recurso humano que de las empresas. Sin embargo, existe un alto porcentaje (64%) al 2017 de las compañías que saben que el presupuesto asignado para gestionar los procedimientos de seguridad de la información es muy bajo frente al comportamiento de la industria.

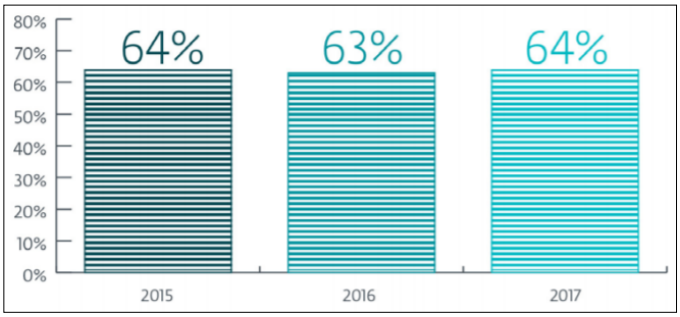


Imagen No. 2 (Referencia del reporte de seguridad de ESET, Latinoamérica 2018, página 013) [5]

Ahora bien, el proceso de transformación digital que viene cubriendo los diferentes mercados e industrias, viene cargado de procesos tecnológicos que soportarán las nuevas visiones y emprendimientos de las compañías. Teniendo en cuenta esto como insumo, las áreas de aseguramiento permitirán a las Compañías tomar decisiones de manera oportuna en su

operación, es decir, procesos como los de seguridad deberán obtener un mayor presupuesto para fortalecer y cubrir los procesos de negocio que generarán el crecimiento gradual de la Compañía.

B. Ambiente de control interno

En este ámbito, adquiere gran importancia el ambiente de control interno, siendo éste el responsable de supervisar la gestión de cada proceso realizado en las organizaciones, identificando posibles hallazgos y estableciendo inmediatamente planes de mejora que permitan el desarrollo continuo de cada una de las gestiones. Se hace necesario que el ambiente de control interno esté a la vanguardia de los avances tecnológicos controlando así los riesgos intrínsecos de la transformación digital.

La transformación digital está redefiniendo la sociedad y los modelos de negocio. En este punto, es necesario reconocer que las nuevas tecnologías presentan un crecimiento exponencial, mientras que las organizaciones y la sociedad en general mantiene el comportamiento lineal frente a esta realidad (Sánchez, S.F) [6]. Es por ello que a nivel estratégico la transformación digital de los modelos de negocio debe ser lo suficientemente efectiva y eficiente para soportar los requerimientos de la sociedad actual y la operación de negocio.

Esto genera oportunidades para crear ventajas competitivas que respondan a las necesidades de la economía actual. Esto implica rediseñar la visión de la organización, garantizar procesos de actualización y capacitación constante con el fin de obtener una verdadera transformación e innovación digital con un personal capaz de asumir esta nueva realidad institucional y tomando todas las medidas de seguimiento y control que permitan garantizar excelentes procesos de seguridad de la información. Pues una desatención en el control interno representa un incremento en el riesgo de fraude, robo de información, entre otros.

El modelo de control interno, COSO, a partir de lo citado por Galaz (2015) [7], cuya misión es "Proporcionar liderazgo intelectual a través del desarrollo de marcos generales y orientaciones sobre la Gestión del Riesgo, Control Interno y Disuasión del Fraude, diseñado para mejorar el desempeño organizacional y reducir el alcance del fraude en las organizaciones", responde de manera oportuna y asertiva a la necesidad actual de las organizaciones a través del desarrollo de lineamientos para monitorear y revisar los procesos de apoyo y core. De igual manera, realiza análisis sobre componentes SOX (si aplican para una compañía). Generando puntos de enfoque con controles relevantes para cada principio y componente de acuerdo con las necesidades de la organización. Gracias al dinamismo e integralidad de este modelo, es posible responder de manera asertiva a la realidad de cada negocio.

C. Seguridad de la Información / Seguridad Informática.

A lo largo del crecimiento de la tecnología, se han identificado estas dos áreas que han movilizado transversalmente diferentes componentes para mitigar el impacto de los riesgos sobre los diferentes modelos de operación de la tecnología en las Compañías. Éstas dos áreas que cuentan con un propósito en común y están segmentadas en:

- La Seguridad de la Información cuenta con un canal directo de comunicación con la alta gerencia y dirección de la organización, estableciendo los lineamientos mínimos que permiten asegurar los procesos, tecnología, personas, entre otros recursos habilitadores que fortalecen el aseguramiento de los activos críticos de la Compañía.

- Por otro lado, el área de seguridad informática realiza una función más operativa o de gestión basada en los lineamientos establecidos por el área de seguridad de la información. Sus esquemas de operación están orientados al monitoreo de eventos de seguridad, canales de aseguramiento de infraestructura, fortalecimiento de las aplicaciones críticas de operación, atención de incidentes de seguridad, entre otros.

Sin embargo, estas áreas cuentan con diferentes lineamientos que han fortalecidos sus esquemas de operación debido que con el incremento de tecnologías que vienen inmersas en la transformación digital, se han identificado y cubierto diferentes brechas que hacen que las Compañías se vuelvan robustas en sus esquemas de aseguramiento. Entre estas prácticas identificamos marcos de referencia como Cobit v5, ITIL v3, ISO27001-2 y con el apoyo del gobierno se han establecido leyes que han hecho que las Compañías fortalezcan el tratamiento de los datos, teniendo en cuenta que la información utilizada para sus mecanismos de operación debido que el procesamiento de esta incluye información de terceros (personas, empresas, proveedores y demás).

Con base en lo anterior, revisando las generalidades del marco de referencia COBIT v5, identificamos que su orientación está en la segmentación del gobierno y la gestión (operación), lo cual permite establecer canales de comunicación transparentes entre las partes interesadas. En el marco de referencia establecen los procesos de "APO13 – Gestionar la Seguridad" que en el dominio "APO – Alienar, Planificar y Orientar" está orientado a "…*provee orientaciones para la planificación de la adquisición, incluyendo planes de inversión, gestión del riesgo, planificación de programas y proyectos y planificación de la calidad...*" [4], asimismo, el proceso "DSS05 – Gestionar los Servicios de Seguridad", en el dominio de "DSS – Entrega, Servicio y Soporte" el cual está orientado al soporte, operación y atención de los servicios prestados interna y externamente a la Compañía.

La segregación de estos dos controles definidos por el marco de referencia es:

- [APO13]: *Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.* [4]
- [DSS05]: *Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.* [4]

Esto permite a las Compañías a organizar sus áreas de gobierno y operación, con el fin de cubrir los riesgos transversales que nacen a partir de la transformación digital. Por otro lado, los demás marcos de referencia establecen los comportamientos generales que tienen los procesos para así, iniciar con el fortalecimiento de las actividades generales que soportan la operación de cada Compañía, incluyendo los procesos de negocio y de apoyo.

IV. Conclusiones

Durante el proceso de crecimiento de las compañías y tomando como línea base, el horizonte del mercado "Transformación digital", se ha identificado que:

- Las áreas que permiten la toma de decisiones de las Compañías deberán incluir en sus esquemas de planeación de manera incremental, el presupuesto necesario para ir cubriendo cada etapa del proceso de transformación digital, sin dejar de lado, la operación actual sobre la cual se sitúa su negocio.
- Existen diferentes prácticas que han sido referentes y se han fortalecido con el análisis general del comportamiento de las industrias, con el objetivo de mejorar la operación de negocio, e inclusive para fortalecer, optimizar y administrar sus recursos. La adopción de este tipo de prácticas permite que las Compañías no empiecen de cero, sino que, a través de estos comportamientos generales, empiecen a adoptar sus esquemas de aseguramiento y en un corto plazo, puedan tomar decisiones de manera efectiva para mejorar el rendimiento de la Compañía e inclusive establecer un punto de referencia del mercado.
- La transformación digital es un proceso que incorpora diferentes mecanismos que fortalecen la operación y la visión de las Compañías, sin embargo, hay que tener en cuenta que la inclusión de esta requiere un esquema de aseguramiento ya que implica un incremento en los riesgos asociados con la información.
- La inclusión de áreas de aseguramiento como Control Interno, Seguridad de la Información, IT Compliance, entre otras, es necesaria para fortalecer la toma de decisión en las compañías, teniendo en cuenta que, a través de sus procesos de monitoreo y verificación, pueden identificar falencias oportunamente y así, establecer las acciones correctivas correspondientes.
- Se debe acelerar el crecimiento lineal de los negocios para alcanzar el crecimiento exponencial de la inclusión de tecnologías emergentes en cada mercado.
- Es fundamental garantizar puntos de control eficientes que permitan un correcto desempeño de las gestiones, así como buenas relaciones en el equipo de trabajo que favorezcan la los planes de mejora continua a implementar.

References

[1] A. Molano, «Revista Dinero,» Revista Dinero, 08 Junio 2018. [En línea]. Available: https://www.dinero.com/opinion/columnistas/articulo/el-cuento-de-la-transformacion-digital-por-adriana-molano/259207. [Último acceso: 08 Junio 2018].

[2] F. Gonzalez, «KPMG,» KPMG, 2015. [En línea]. Available: https://assets.kpmg/content/dam/kpmg/pa/pdf/delineandoestrategias/DE-area-TI-como-generador-de-valor-negocio.pdf. [Último acceso: 2015].

[3] S. d. E. C. -. J. P. G. d. E. C. Conchita Jaimes, «EY Colombia,» EY Colombia , 20 Noviembre 2018. [En línea]. Available: https://eycolombia.ey.com/2018/11/20/mas-del-80-de-las-juntas-directivas-no-hacen-de-la-ciberseguridad-un-tema-estrategico-para-sus-companias/. [Último acceso: 20 Noviembre 2018].

[4] ISACA, «Un marco de negocio para el Gobierno y la Gestión de las TI de la Empresa,» de *Un marco de negocio para el Gobierno y la Gestión de las TI de la Empresa* , Rolling Meadows, Estados Unidos., ISACA, 2012, p. 94.

[5] ESET, «ESET Security Report, Latinamérica 2018,» ESET, Bratislava, Eslovaquia., 2018.

[6] Íncipy, «TRANSFORMACIÓN E INNOVACIÓN DIGITAL,» Íncipy, Barcelona, Madrid, Valencia, España., SF.

[7] Deloitte, «Marco de referencia para la implementación, gestión y control de un adecuado Sistema de Control Interno.,» Deloitte, New York, 2015.