Nº 70 junio 2021

Claves para la transformación digital y la digitalización con seguridad

Acelerado por la pandemia de la COVID-19, el presente y el futuro inmediato de la transformación digital y las principales iniciativas digitales de las organizaciones públicas y privadas, incluyen el aprovechamiento de la tecnología para mejorar la producción, la seguridad digital proactiva y la automatización inteligente de la gestión operativa y el capital humano.

Manuel Sánchez Gómez-Merelo
Consultor Internacional de Seguridad

Actualmente, para evitar y reducir riesgos y mejorar la seguridad, la concienciación debe impregnar toda una nueva cultura en las organizaciones.

Un reto cultural digital basado en el talento y la tecnología como los nuevos pilares de las organizaciones digitales. Una necesaria transformación digital basada en la digitalización transversal, la tecnología y la conciliación con control de la privacidad y la seguridad.

Nueva normalidad. Liderar la transformación

Liderar la transformación digital, capitalizar la analítica de datos y colaborar más con la organización encabezará la lista de prioridades en las entidades con gran impulso para mejorar las capacidades de análisis de datos.

Como recomienda la consultora estadounidense Gartner debemos *"practicar la influencia, no la coacción",* limitando el número de batallas que los líderes de seguridad decidan librar y buscando formas de aplicar sus limitados recursos allí donde sean más beneficiosos para la reducción y la gestión del riesgo.

Así, la digitalización, la automatización y la seguridad son claves en la *"nueva normalidad".* El mundo ha cambiado por completo con una pandemia, que ha acelerado el proceso de digitalización y ahora, es clave para las organizaciones, disponer de una fuerza de trabajo que esté protegida en su gestión en cualquier lugar y dispositivo.

La pandemia ha obligado a empresas y administraciones a adaptarse aceleradamente a un mundo digital y a distancia donde la transformación de las organizaciones implica una combinación de cuatro prioridades estratégicas: reinventar las aplicaciones, proteger la información, automatizar la infraestructura y su gestión y facilitar el trabajo colaborativo, todo sobre la base de la seguridad.

Las empresas y administraciones deberán reforzar su capacidad de resiliencia y acelerar su transformación digital, y en este año se pondrán en marcha un gran número de iniciativas basadas en la tecnología y la gestión.

Una de las tecnologías estrella será sin duda lo que Gartner ha denominado SASE (Secure Access Service Edge), que es la combinación de la red y la seguridad en la nueva era *"multicloud".*

Transformación digital. Definiciones, retos y claves

Lo primero hemos de tener claro qué es exactamente la transformación digital, cuáles son sus retos y claves para el éxito.

Transformar digitalmente una organización significa saber elegir qué herramientas tecnológicas y de gestión serán la guía para este fundamental cambio.

Inicialmente, hemos de ver en qué punto tecnológico está la organización y cómo esas herramientas las podemos utilizar para mejorar nuestra actividad, incluso para reinventarnos.

Una cuestión por resolver para la adecuada transformación es saber analizar hasta qué punto nuestra organización es capaz de entender la necesidad del cambio y adoptar la tecnología para esta nueva etapa. Transformarse también implica asumir que la organización debe estar preparada para el cambio permanente.

Uno de los retos más importantes es saber entender, no sólo en qué punto estamos, sino cómo vamos a ir evolucionando con la implementación de la tecnología con velocidad e incertidumbre.

Igualmente, hemos de entender la diferencia entre digitalizar documentación y digitalizar una actividad u organización.

Podemos definir la digitalización como el proceso de conversión de flujos analógicos individuales de información en bits digitales. Por el contrario, nos referimos a la digitalización de una actividad u organización como la forma en que ésta se reestructura en torno a la comunicación digital y las infraestructuras de los medios digitales.

Para conseguir estos objetivos de transformación digital y digitalización, hemos de apoyarnos en seis grandes claves: Elevada capacidad de proceso (Cloud Computing); Alta posibilidad de análisis de datos (Big Data); Nuevos procesos de gestión integral y simplificados; Adecuación de la experiencia al cambio; Multicanal y glocalización; Seguridad (prevención + protección).

Digitalización: datos, información, conocimiento

En plena era digital y en la denominada cuarta revolución industrial, los datos están ocupando una posición cada vez más relevante en la toma de decisiones.

Uno de los ámbitos donde están tomando mayor importancia es en el empresarial, donde diferentes herramientas se utilizan para transformar esos datos en información y ésta en conocimiento. Este conocimiento permite mejorar la toma de decisiones y realizar acciones como segmentación de clientes, optimización de la producción o desarrollo de nuevos productos y servicios y su incorporación al mercado.

En este sentido, a medida que las empresas aumentan su digitalización, se encuentran con la necesidad de administrar conjuntos de datos e información cada vez más grandes y que incluyen datos críticos y sensibles sobre personas y sobre la organización y sus actividades, siendo un objetivo especial su protección.

La digitalización de los datos supone un avance y un cambio en los sistemas de gestión del riesgo y las seguridades. Y es que permite tomar decisiones y definir acciones preventivas alejadas de los métodos tradicionales, basados en técnicas reactivas donde las medidas correctivas se toman después de incidencias o fallos en la prevención.

Hay que definir un nuevo marco ante la contingencia e intervención, sobre la base de la implementación de medidas proactivas que se anticipen a posibles contingencias a través del análisis de tendencias y detección de áreas de mejora.

Llegados a este punto, es obvio preguntarse qué valor pueden aportar las técnicas de análisis de datos al mundo de la prevención. Partiendo de la base de que estas estrategias sirven para recopilar, analizar y visualizar información, los principales beneficios de su implantación son: Combinar el análisis de datos internos con información de fuentes externas; Permitir un análisis multidimensional mejorando el análisis de causas; Realizar control y seguimiento de los datos e indicadores establecidos; Transformar y tratar la información de forma que permita un análisis predictivo; Visualizar toda esta información de una manera gráfica e interactiva.

Para ello, una vez seleccionados los datos hay que tener en cuenta, que por sí solos no aportan valor, se deben transformar en información clasificada y analizada para que se conviertan en conocimiento.

Como estamos hablando de la seguridad de los datos personales y empresariales y no debemos de dejar de pensar en qué consecuencias extremas pueden traer esas *"carencias o insuficiencias de las soluciones adoptadas",* no podemos adoptar una posición de *"ignorante legis non excusat",* es decir, que la ignorancia de la ley no excusa de su cumplimiento, los principios de concienciación y responsabilidad nos exige unas garantías de seguridad.

Digitalización para la gestión

Son varias las líneas de actuación sobre las que hemos de trabajar enmarcadas en las claves de liderazgo, análisis, supervisión y capacitación, y las tecnologías de la información nos ayudarán a gestionar y analizar la información para la mejora continua.

La digitalización no puede plantearse como una mera eliminación del papel o un repositorio documental que evidencie el cumplimiento de esta irreversible e importante obligación ante la sociedad y la *"nueva normalidad",* sino que es una herramienta para facilitar y mejorar la gestión de la información con seguridad.

Debemos trabajar sobre las premisas de que, desde los departamentos de seguridad no sólo evidenciamos, documentamos y controlamos, sino que investigamos, analizamos y prevenimos. La tecnología debe optimizar nuestro tiempo, permitir simplificar las tareas de análisis y facilitar la toma de decisiones con seguridad.

Así, en la era de las tecnologías 4.0, abordamos una nueva transformación digital aplicada a la seguridad que nos permitirá optimizar nuestra gestión del riesgo, profundizar en el análisis de datos e integrar la información de todas nuestras operaciones permitiendo visualizar, controlar y analizar mejor lo que acontece para adoptar soluciones rápidas que minimicen la exposición al riesgo de los trabajadores y activos de la organización.

Digitalización de las organizaciones

Digitalizar forma parte del proceso de transformación, como se ha comentado. Una organización que se digitalice no necesariamente se acaba transformando.

Pero, una empresa que empieza a digitalizar y optimizar sus procesos primero reducirá costes, pero además al digitalizar obtendrá información que antes no veía ni tenía acceso. Y ahí está una de las claves de la transformación digital.

Si la organización está preparada para saber usar esta tecnología y sabe qué hacer con esa información tendrá muchas más posibilidades para saber qué puede o debe cambiar o qué nuevas oportunidades tiene a su alcance.

En definitiva, habrá nueva información que permitirá tomar decisiones en función de los objetivos de la entidad. Por lo tanto, la digitalización es un paso previo a la transformación. Y digitalizar no implica transformar una organización, situación que se inicia por las personas y la tecnología y será nuestro medio para llegar a los objetivos. Si nuestra organización no está preparada para el cambio organizativo y cómo adecuarse a las nuevas tecnologías que formarán parte de este proceso, no habrá transformación.

En este sentido, y en la mayoría de los casos, para cumplir con las nuevas expectativas del cliente, las entidades deben acelerar la digitalización tanto de su información como de sus procesos de gestión. Deben reinventar todo el proceso como la: Reducción de la cantidad de pasos requeridos; Reducción de los documentos necesarios; Desarrollo de una toma de decisiones automatizada; Tratamiento de problemas regulatorios y de fraude; Garantía de la seguridad de la información.

Para ello será necesario rediseñar los modelos operativos, las habilidades, las estructuras organizativas y los roles de forma que coincidan con los procesos reinventados. Los modelos de análisis de datos también deben ajustarse y reconstruirse para permitir una mejor toma de decisiones, seguimiento del rendimiento y perspectivas del cliente.

La transformación digital se presentó como uno de los puntos prioritarios en la agenda de los directores de sistemas y seguridad ya en 2017, según el Wall Street Journal.

Claves para la Gestión del Riesgo y las Seguridades

Es imprescindible actualizar la seguridad informática y de los datos para aumentar la protección y resiliencia de las organizaciones.

Para comenzar un programa de digitalización de una organización ha de tenerse muy en cuenta la seguridad corporativa, independientemente de la actividad a la que se dedique.

La pandemia de la COVID-19, con la consiguiente implementación precipitada del teletrabajo, ha potenciado esta tendencia: la digitalización y sus riesgos. El mundo se ha trasladado al entorno digital y los ataques se han incrementado. Las oficinas eran entornos más o menos seguros y controlados, pero nos hemos instalado en nuestros hogares y, en general, este tipo de entornos presenta más vulnerabilidades.

El rápido traslado del trabajo presencial en las oficinas al trabajo a distancia, combinado con una ola de hackers oportunistas, creó un aumento del 200% en los incidentes de phishing en el año 2020 y un nuevo enfoque urgente en la protección de las redes y los sistemas, según el Centro de Denuncias de Delitos en Internet del FBI.

Pero, la digitalización de los datos supone un avance y un cambio en los sistemas de Gestión del Riesgo y las Seguridades. Entre otros aspectos, permite definir un nuevo marco de intervención sustentado en la implementación de medidas proactivas que se anticipen a posibles incidencias a través del análisis de tendencias y detección de áreas mejoradas.

La sobrecarga de información y la incapacidad para su análisis, especialmente en el ámbito de las seguridades, genera cierto inmovilismo en las organizaciones y una pérdida del enfoque real preventivo, así como una falsa sensación de *“seguridad”.*

Así, tan importante como el análisis de los datos es medir la consecución de los objetivos marcados, para lo que es preciso definir los indicadores necesarios para el adecuado control.

Será de gran ayuda diseñar un Cuadro de Mandos que contenga, además de los indicadores de siniestralidad, indicadores del conjunto de la organización aportados por diferentes departamentos. O lo que es lo mismo, establecer un *"Cuadro de Mandos de Gestión Integral del Riesgo y las Seguridades".*

Cada organización definirá qué indicadores y relación entre ellos serán importantes a la hora de medir el desempeño en las áreas de prevención, protección e intervención, así como el éxito del análisis de datos.

Ciberseguridad protagonista

Con todo lo anteriormente expuesto, es fácil deducir el irreversible protagonismo de la ciberseguridad en este proceso de digitalización y transformación digital.

Los directores de seguridad y gestión del riesgo se enfrentan a dos grandes retos en 2021, según la consultora Gartner. La aceleración del negocio digital está incrementando las inversiones en ciberseguridad previstas, y la demanda de habilidades de ciberseguridad ya supera la disponibilidad. Las nuevas iniciativas digitales implican que las organizaciones dispongan de más recursos en ciberseguridad con nuevos y diferentes conjuntos de habilidades.

Los efectos globales de la COVID-19, sus incertidumbre e inseguridades, ha llevado la ciberseguridad a los comités de dirección. Frente a este auge de las amenazas, y significación de los riesgos y vulnerabilidades, la mejor respuesta es instaurar una cultura de ciberseguridad en toda la organización, y para ello, la concienciación debe empezar por la alta dirección.

En este sentido, lo primero que hay que tener en cuenta es que la ciberseguridad no proviene de un componente de un dispositivo individual o red de comunicación, sino que es el resultado de un proceso que comienza con las fases de diseño (seguridad por diseño) y continúa durante toda la vida operativa de ese dispositivo por parte del fabricante y el ecosistema existente que afecta al usuario final.

Todo ello, sin olvidar que la ciberseguridad requiere un enfoque integral e integrado, con la implicación y responsabilidad de todos los actores de la cadena operativa, desde los fabricantes de los dispositivos hasta el usuario final, pasando por todos los demás implicados en el ecosistema operativo.

Nadie está exento de responsabilidad, especialmente los comprometidos en la gestión del riesgo y las seguridades ya sea en una organización pública o privada.

Finalmente, hay que tener en cuenta el programa de cumplimiento pues, prácticamente todo está especialmente regulado por las normas internacionales y las leyes nacionales en vigor durante años, ahora actualizadas no sólo en aspectos cualitativos de los sistemas y procedimientos, sino que también identifican a quienes tienen la responsabilidad de implementarlos estableciendo sanciones que afectan, no tanto a la mera violación de requisitos sino, más bien, a la posible insuficiencia de las soluciones adoptadas para la seguridad de los datos e información.

Integración de la prevención

Desde la perspectiva que se acaba de describir, la prevención en la gestión del riesgo y las seguridades se convierte, en la transformación digital, en una disciplina transversal presente en la mayoría de las áreas y actividades de las organizaciones, demandando respuesta a la integración preventiva a través de una colaboración bidireccional entre la dirección de seguridad y el resto de los departamentos.

Desde esta perspectiva proactiva, la prevención contribuye no solo a la disminución del riesgo y de la siniestralidad, sino que también se presenta como un área productiva dado que permite, entre otros aspectos: Colaborar en el incremento de la productividad mejorando procesos operativos; Aumentar el bienestar laboral y la mejora de la reputación permitiendo la retención y atracción del talento; Reducir costes derivados de sanciones, aseguradoras, etc.; y mejorar la satisfacción de clientes al aumentar la calidad de los productos y servicios ofrecidos.