White Paper

Las cinco tecnologías esenciales que habilitan un marco de ciberresiliencia

Patrocinado por: IBM

Frank Dickson Phil Goodwin
Octubre 2020

LA OPINIÓN DE IDC

El año 2020 fue un punto de quiebre. Por primera vez, las encuestas de IDC sobre el tema de la seguridad revelaron que los datos corporativos que residen en la nube superaron en cantidad a los que se encuentran en el entorno local. Además, la mayor parte del procesamiento ahora se efectúa en la nube, porque el 53 % de las cargas de trabajo se encuentran en IaaS.

Desafortunadamente, los hackers siguen el rastro de los datos hasta la nube: en los últimos dos años, una organización promedio sufrió 2 vulneraciones vinculadas a la nube, y tuvieron que desembolsar "gran cantidad de recursos extra para rectificarlas".[1] Al igual que en los entornos locales, las brechas vinculadas a los entornos IaaS ocurrieron como consecuencia de diversos factores, entre ellos, malware sofisticado (17,7 %), falta de suficientes herramientas de seguridad (17;7 %), robo de credenciales (14,6 %), incorrecta configuración del entorno IaaS (14,3 %), vulnerabilidad sin parches de seguridad (13,9 %), amenazas internas (13,3 %) y vulnerabilidad del día cero (8,5 %). ¿La conclusión? A medida que el mercado se traslada hacia la nube, los hackers también lo hacen, lo que nos obliga a esforzarnos por garantizar la seguridad de los datos.

Esto no significa que las tecnologías vinculadas a la nube y las nuevas maneras de comunicarse sean la *causa-raíz* de las brechas y las fallas del negocio, sino que a medida que las empresas adoptan nuevas tecnologías sus estrategias de protección deben modificarse para adaptarse a las nuevas circunstancias. Estas estrategias deben incluir mecanismos de seguridad más sólidos y variados, pero también maneras de recuperarse rápidamente en caso de que se produzca una vulneración o un incidente.

Las empresas de todo el mundo están avanzando incesantemente hacia la transformación digital, que es el proceso de integrar tecnología en todos los aspectos del negocio con el fin de acelerar las actividades empresariales, sustentar la agilidad y sacar provecho de una visión estratégica y oportunidades dinámicas. Un elemento imprescindible para lograrlo es convertirse en una empresa impulsada por datos y capaz de monetizar la información. Al mismo tiempo, la transformación digital conlleva nuevos riesgos inherentes que quizás se hayan pasado por alto anteriormente o que hayan complicado el perfil de riesgo de los procesos de negocio ya establecidos, por lo cual las empresas buscan niveles más altos de integración entre funciones esenciales de soporte de negocio y una

[1] Encuesta sobre seguridad en la nube de IDC, diciembre 2019

mayor disponibilidad de los datos si desean asegurarse de estar preparadas para hacer frente a cualquier desafío. Esto es lo que se conoce como “ciberresiliencia”.

La ciberresiliencia combina las mejores prácticas vinculadas a la seguridad de TI, la continuidad del negocio y otras disciplinas para crear una estrategia de negocio más alineada con las necesidades y los objetivos de la empresa digital actual. En este documento de IDC se describe de qué manera la transformación digital está quebrantando las protecciones tradicionales entre empresas y participantes dentro de la economía global, mientras las tecnologías esenciales para el negocio se convierten en puertas de entrada para riesgos, ataques y fallas de sistemas. También, se describe cómo las prácticas de ciberresiliencia pueden ayudar a las empresas a defenderse contra esos riesgos y a recuperarse tras una brecha o falla de una manera controlada y cuantificable. Por último, se presenta un marco que puede ayudar a las organizaciones a emprender su camino hacia la ciberresiliencia, además de estrategias para modificar las prácticas de protección y restauración de datos con el objetivo de luchar mejor contra los ataques más dañinos y deliberados que ocurren en la actualidad.

EN ESTE WHITE PAPER

¿Es este el momento de la verdad, el día en que sus operaciones de negocio frenan bruscamente? ¿Acaso ha llegado el día en que su empresa deba cerrar sus puertas? Esta es una visión muy pesimista de la realidad empresarial.
En cualquier momento podría ocurrir algún acontecimiento que altere el tejido operativo de la empresa y, en la vorágine actual del mundo de los negocios, cada segundo cuenta.

No es necesario que esos eventos sean catastróficos para que tengan un impacto duradero. Las empresas más maduras ya tienen instaurado un sistema de gestión del riesgo y alguna que otra medida de continuidad o resiliencia empresarial. Seguramente esas organizaciones comprenden que los eventos de gran magnitud con efectos devastadores son menos probables que los eventos pequeños y discretos que pueden hacer tambalear las operaciones. Pensemos, por ejemplo, lo que sucedió con la gripe aviar a mediados de la década de 2000, cuando las empresas estaban demasiado pendientes del posible impacto que podría ocasionar un virus que se propaga rápidamente por el aire sobre los empleados y las operaciones de negocio. Si bien es cierto que el concepto en sí es motivo de preocupación, la probabilidad de que se materialice la gripe aviar o cualquier otra amenaza similar fue y sigue siendo muy baja. Esta baja probabilidad no impidió que las organizaciones trataran de crear planes de contingencia operativos basados en la naturaleza del impacto potencial. Lo mismo ocurre en el caso de otros desastres naturales o amenazas físicas. El potencial de que tengan consecuencias de gran impacto es motivo de preocupación, y a veces enfocarse en la posible magnitud de un evento único puede impedir que las organizaciones se focalicen en las amenazas bien reales, tangibles y discretas que pueden causar estragos en el negocio.

La transformación digital está poniendo en tela de juicio los conceptos tradicionales de resiliencia empresarial. Es el proceso mediante el cual la tecnología se interrelaciona con todos los ámbitos de la experiencia humana. En la empresa, la transformación digital se traduce en el mayor nivel de conectividad entre aplicaciones y procesos empresariales con el fin de aumentar la agilidad del negocio y conectarse más fácilmente con clientes y socios para brindar a los usuarios una experiencia sin interrupciones las 24 horas del día, los 7 días de la semana. La transformación digital se puede manifestar de muchas maneras. Es posible que una empresa esté buscando integrar mejor

infraestructura existente y sistemas heredados o quizá se esté encaminando lentamente hacia la nube o tenga en mente una estrategia del tipo «la nube primero». Cualquiera sea el caso, el concepto de una empresa conectada resulta esencial a la hora de evaluar la resiliencia empresarial. Ya sea que se trate de agrupar procesos de negocio o desarrollar entornos multinube o de nube híbrida, cuanto más hiperconectados estén los sistemas y procesos de negocio, mayor será la probabilidad de que un evento discreto pueda desbaratar todo el negocio. Lo que alguna vez fuera un pequeño tambaleo, ahora podría tener fuertes repercusiones en toda la organización.

Es por eso que la ciberresiliencia ha cobrado muchísima importancia tanto para los profesionales de la seguridad como para los responsables de la continuidad del negocio y la planificación de la gestión del riesgo. La ciberresiliencia es la fusión de ciberseguridad, gestión del riesgo y prácticas de resiliencia y continuidad del negocio con el fin de crear una disciplina que sirva para mejorar las capacidades de ciberrespuesta, desde la gestión de eventos y la recuperación hasta la mejora incesante de los procesos. Los clientes ahora reconocen que las estrategias tradicionales en torno a la continuidad del negocio, centradas en las fallas e interrupciones de sistemas, tienen que evolucionar y enfocarse en las ciberamenazas dirigidas a sus datos. Los procedimientos tradicionales de recuperación tras una interrupción en los sistemas seguramente no lo protegerán de una ciberamenaza que pueda dañar los datos.

El crecimiento y las falencias de la transformación digital

El gasto en la transformación digital de prácticas empresariales, productos y organizaciones se va a acelerar a pesar (o como consecuencia) de los desafíos que trae aparejados COVID-19. En el año 2021, el gasto global en tecnologías y servicios vinculados a la transformación digital se incrementará un 16,6 % hasta alcanzar 1,54 billones de dólares. Este aumento es sin duda muy superior al 10,4 % calculado para 2020, ya que en 2021 las empresas buscarán implementar la transformación digital para contrarrestar los impactos económicos negativos de la pandemia de COVID-19, un fenómeno al que IDC se refiere como «aplanar la curva» de la recesión económica (Figura 1). Incluso los sectores que más están sufriendo el impacto de la situación económica seguirán aumentando su gasto en transformación digital. El sector de servicios personales y de consumo, que incluye hoteles, parques temáticos, casinos, cines y teatros, aumentará un 16 % el gasto en transformación digital en 2021, pero los sectores que más gasto tendrán en 2021 son el de la construcción (27,9 %) y el comercio minorista (20,3 %).

FIGURA 1

Aplanando la curva: el rol de la tecnología para crear resiliencia empresarial y sustentar la agilidad

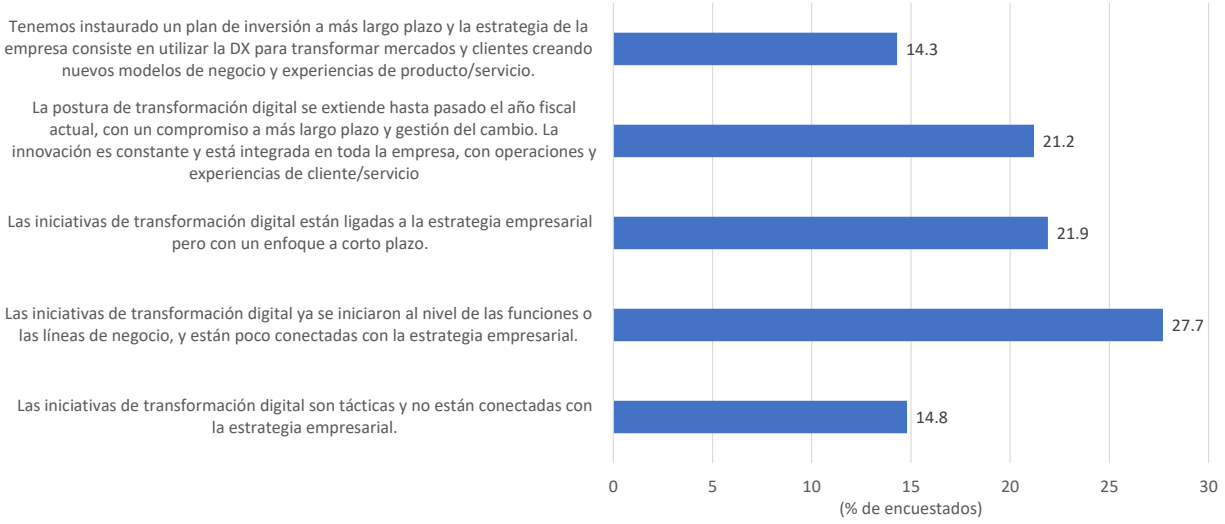
Fuente: IDC, 2020

Cada organización adopta una postura diferente con respecto a la transformación digital. Muchas han adoptado una actitud proactiva, lo que indica que tienen instaurado «un plan de inversión a más largo plazo y la estrategia de la empresa consiste en utilizar la transformación digital para transformar mercados y clientes con nuevos modelos de negocio y experiencias de productos y servicios». Otras procuran ser más proactivas. Es evidente que la transformación digital ocupa el primer puesto en la lista de prioridades de las empresas, independientemente de su postura (Figura 2).

FIGURA 2

Postura respecto de la transformación digital

P. ¿Cómo evaluaría la postura de su empresa con respecto a su transformación digital antes de la pandemia de Covid-19?



n= 880

Fuente: Encuesta de IDC "*COVID-19 Impact on IT Spending Survey",* realizada del 4 al 15 de junio 2020

¿A qué se debe semejante gasto? Simplemente a que las empresas creen que la transformación digital es el camino que seguir en un mundo hiperconectado. Deben buscar innovación y agilidad si desean sobrevivir y estar preparadas para salir al mercado rápidamente, a escala, con nuevos productos y servicios, al tiempo que desarrollan los conocimientos esenciales que se necesitan para llegar a los destinatarios clave y abrir nuevos mercados. En este sentido, IDC considera que el apogeo de la transformación para la mayoría de las organizaciones ocurrirá cuando empleen una infraestructura con un núcleo inteligente que convierta los conocimientos sobre la actividad del negocio en inteligencia utilizable, en un proceso continuo y optimizado. Esto es lo que IDC describe como la plataforma de transformación digital (Figura 3). En el centro, esta plataforma utiliza datos diversos, distribuidos y dinámicos para generar oportunidades.

FIGURA 3

Plataforma de transformación digital: un marco para el núcleo inteligente

Fuente: IDC, 2020

Sin datos, el modelo no funciona. Los datos ya no se pueden convertir en productos ni ser monetizados. Tampoco se pueden utilizar para agilizar el negocio. Por eso, se vuelven imprescindibles para la supervivencia de la empresa, lo que hace que su integridad y accesibilidad sean sagradas. Sin embargo, los atributos y la ubicación de los datos relevantes para una plataforma de transformación digital siguen cambiando. Los datos son cada vez más diversos y abarcan no solo sistemas estructurados, sino también datos no estructurados, como los de series temporales, los generados por máquinas y los generados en *stream*. Los datos también son cada vez más dinámicos, no solo en procesamiento por lote sino también inherentemente en tiempo real, mientras se generan datos de telemetría a través de una cantidad cada vez mayor de sensores y dispositivos. Además, los datos cada vez se distribuyen más y se encuentran no solo en centros de datos con ubicaciones centrales sino también en la periferia, en dispositivos y en servicios en la nube. Al ser tan diversos, dinámicos y distribuidos, los datos exacerban la necesidad de implementar un programa eficaz de ciberresiliencia.

Esto no significa que los datos sean el único factor a tener en cuenta. Para la mayor parte de las organizaciones, el camino hacia la transformación digital comienza con una serie de sistemas poco conectados que esperan poder establecer como un sistema interconectado. Pensemos en la transformación digital como si fuera una máquina Rube Goldberg. Para los que lo desconocen, Rube Goldberg fue un ingeniero, inventor y caricaturista ganador del premio Pulitzer que se hizo famoso por sus ilustraciones de aparatos muy complejos construidos con utensilios domésticos para realizar tareas mundanas. ¿Le resulta familiar? Las empresas están conectando sistemas de gestión de recursos humanos, gestión de contratos, sistemas ERP, aplicaciones dirigidas al cliente, etc., con la esperanza de que todos funcionen en una misma dirección y orientados al negocio. Es aquí donde la transformación digital comienza a presentar un desafío para quienes están a cargo de reducir el riesgo empresarial.

¿Qué sucede cuando colocamos un palo de escoba entre los rayos de una rueda de bicicleta? Si los rayos no están conectados con nada, probablemente no suceda nada. Pero los rayos de una rueda están conectados. Si uno o dos rayos quedan bloqueados por un objeto extraño, la rueda completa deja de girar. Ese es el riesgo de los sistemas de negocio interconectados. Un solo sistema que falle puede interrumpir las actividades de toda la empresa.

Si lo relacionamos con la ciberresiliencia, esto significa que cualquier proceso empresarial podría representar una puerta de entrada a otros procesos de negocio. Es decir, que la superficie de ataque de un proceso tiene el potencial de permitir el acceso lateral a prácticamente cualquier otro proceso.

Los obstáculos en el camino de transformación digital

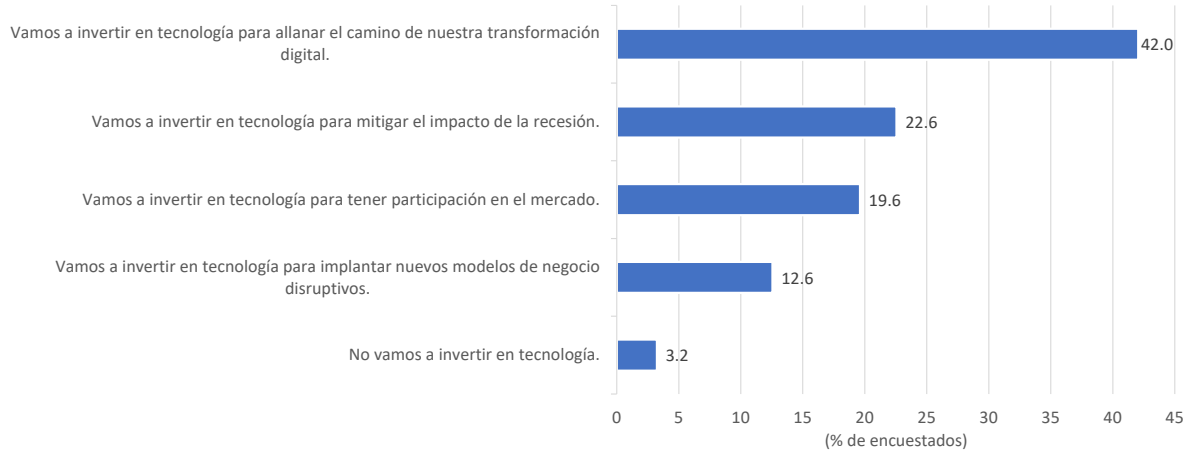
Si bien el gasto en transformación digital es impresionante, IDC ya vislumbra que habrá cada vez más presiones externas que comenzarán a tener un impacto sustancial en la estrategia de ciberseguridad de las empresas. Como ya mencionamos, la interconexión entre sistemas y el empleo constante de servicios externos tales como la nube y la IoT entrañarán riesgos para los cuales muchas organizaciones aún no están preparadas.

Lo que es peor: la transformación digital no se detiene en épocas de crisis, sino que se acelera. Una encuesta reciente de IDC reveló que todos los encuestados excepto el 3 % prevén invertir en tecnología para enfrentar la recesión económica (Figura 4).

FIGURA 4

Estrategias de inversión en tecnología para enfrentar la recesión económica

P. ¿Cuál de las siguientes afirmaciones describe mejor la manera en que su empresa piensa como primera opción para invertir en tecnología en relación a sus esfuerzos de transformación digital?



n= 880

Fuente: Encuesta de IDC "*COVID-19 Impact on IT Spending Survey",* realizada del 4 al 15 de junio 2020

Si bien la inversión agresiva es impactante, aún no sabemos a ciencia cierta cuántas de esas organizaciones reconocen que la disponibilidad de esos datos y aplicaciones (información) es imprescindible para el éxito de la transformación digital. Si los datos no están disponibles, no pueden monetizarse. Las empresas que tengan una mayor disponibilidad de la información gozarán de una ventaja competitiva relativa frente a las empresas que no la tengan. Aunque IDC ha observado un gasto cada vez mayor en torno a los productos y servicios anti DDoS, a muchos clientes les cuesta instaurar una estrategia coherente para la defensa de los datos y disponibilidad de la información que sea rápida e integral y que abarque todo el proceso de acceso a los datos.

Otro desafío externo para las organizaciones son las crecientes exigencias impuestas por el marco regulatorio. Para el año 2025, más del 70 % de los datos corporativos estarán sujetos al cumplimiento normativo. Estos datos no solo requieren un manejo especial sino que también generan riesgos adicionales para la organización, que podría tener que pagar multas elevadas por no proteger correctamente los datos.

El creciente uso de la nube y la IoT

Ofrecer disponibilidad óptima de los datos a los usuarios y garantizar el acceso a ellos con privilegios mínimos suelen ser fuerzas opuestas que afectan sustancialmente el negocio, pero que, al mismo tiempo, solo podrían verse afectadas de manera indirecta por el negocio. Cuantas más empresas utilicen la nube y los dispositivos de Internet de las Cosas (IoT) en funciones esenciales para el negocio, la capacidad de proporcionar un acceso sin fricciones *y* en cumplimiento de las normativas para datos sensibles se hace cada vez más complicado.

Hoy las empresas están utilizando la nube híbrida, y la mayoría de las aplicaciones en el futuro estarán basadas en la nube. En una encuesta reciente de IDC, las organizaciones indicaron que el 53 % de sus cargas de trabajo están desplegadas en un modelo de nube IaaS. La seguridad es tanto un impulsor como un inhibidor para la adopción de la nube híbrida, ya que los datos críticos ahora se extienden por numerosas regiones geográficas, centros de datos y la nube, y deben estar protegidos de acuerdo con los requisitos corporativos, independientemente de dónde residan. Las empresas encuestadas calculan que la mitad de todos los datos corporativos están almacenados en la nube, y el 48 % de estos datos son de carácter sensible. Las principales prioridades son la copia de seguridad y la restauración, además de la evaluación del costo y el valor de los datos.

Cada vez más, las empresas están recabando datos sensibles no solo provenientes de la nube sino también de dispositivos de IoT. Si bien estos dispositivos suelen tener un poder de procesamiento inferior al de los sistemas completos, los atacantes han demostrado la capacidad de emplearlos como parte de su estrategia de ataque. Esta capacidad, combinada con una carencia general de seguridad en torno a los dispositivos de IoT, implica que las organizaciones deben determinar cómo defender mejor los dispositivos de IoT que pueden ser fáciles de acceder, supervisar y resguardar, además de los dispositivos tradicionales de computación.

Fallas cada vez más complejas

Si bien IDC observa que las empresas muestran más confianza en su capacidad de brindar seguridad a la nube, y la tasa de adopción de la nube y de soluciones de seguridad basadas en la nube no ha dejado de aumentar, un desafío para el cual las empresas parecen estar menos preparadas que nunca es el acecho de las vulneraciones.

En una encuesta reciente de IDC a sus clientes, el 73 % de los consultados indicaron que habían sufrido vulneraciones graves de seguridad de sus entornos IaaS en los últimos dos años por las que tuvieron que gastar gran cantidad de recursos extra para rectificarlas. Efectivamente, las empresas que fueron afectadas los últimos dos años sufrieron un promedio de 2 vulneraciones.

La copia de seguridad y la recuperación ante desastres son protecciones tradicionales insuficientes a la hora de luchar contra las amenazas modernas. La mejor práctica de IDC recomienda un RTO (tiempo de recuperación objetivo) de una hora para aplicaciones de misión crítica y de cuatro horas para aplicaciones no críticas. Es posible que ciertas copias de momentos determinados (instantáneas) sean incompletas o ineficientes, lo que las hace vulnerables a los ataques cuando no están diseñadas correctamente. El marco en general está diseñado para una recuperación al nivel del sistema y no para una restauración del entorno, por ejemplo, daños en la plataforma o configuración. Un mantenimiento inadecuado y la falta de higiene en las pruebas también pueden sabotear sólidos esquemas de protección de las instantáneas.

Las investigaciones de IDC revelan que el costo «promedio» del tiempo de inactividad supera los 200.000 dólares por hora, aunque varía según el sector de la economía y el tamaño de la empresa. En algunas organizaciones, los directores de TI indicaron que el tiempo de inactividad de aplicaciones clave de ERP, como Oracle E-Business Suite o SAP Business One instaladas solas puede superar los 200.000 dólares por hora. Por lo general, estos costos se pueden utilizar para ayudar a alentar a las organizaciones a la hora de tomar decisiones vinculadas a construir planes de recuperación y de infraestructura. Las estimaciones de costos incluyen la pérdida de ingresos real y los costos de recuperación, entre ellos, los gastos propios del cumplimiento regulatorio, que suelen ser elevados. Estas estimaciones no contemplan el costo vinculado a la reputación y al daño a largo plazo que sufre la marca y que pueden ocurrir como resultado de una brecha vergonzosa, pero sí se pueden utilizar para ayudar a determinar el gasto organizativo adecuado en una estrategia de infraestructura para remediar una brecha. El siguiente es un ejemplo reciente e ilustrativo: en abril de 2020, una empresa multinacional de servicios informáticos reconoció públicamente que su red había sufrido un ataque del ransomware Maze, que había encriptado servidores e inhabilitado las capacidades de teletrabajo además de neutralizar las herramientas que se utilizan para automatizar y aprovisionar laptops. Maze es una forma especialmente maliciosa de ransomware ya que no solo se basa en la encriptación sino también en la exfiltración de datos del sistema infectado, lo que permite a los ciberdelincuentes pedir un rescate con la amenaza de exponer públicamente los datos de la empresa. Se estima que el impacto que sufrió esta empresa fue entre 50 millones y 70 millones de dólares en el primer semestre de 2020, más los gastos legales y honorarios profesionales vinculados a la recuperación y reparación.

El auge de los ataques sofisticados

IDC también sigue notando un aumento en la cantidad de ataques sofisticados. Las estadísticas del sector muestran que muchos ataques pasan inadvertidos durante más de 200 días. Con tanto tiempo para esconderse en una red, los atacantes pueden instalar malware que se abra paso a través de los sistemas de copia de seguridad, lo que ocasiona que los datos de recuperación también se infecten. Los ataques pueden permanecer latentes durante semanas o meses, y esto permite que el malware se propague a todo el sistema. Incluso después de que se detecta un ataque, puede resultar extremadamente difícil eliminar el malware que está tan diseminado por toda la empresa.

DESCRIPCIÓN DE LA SITUACIÓN

El concepto de ciberresiliencia

Cada vez existen más recursos de infraestructura disponibles en la nube y en dispositivos de IoT. Sin embargo, las defensas tradicionales para contrarrestar efectivamente las amenazas que van surgiendo no son eficaces, por lo cual las empresas deben adoptar una nueva postura con respecto a la seguridad. El panorama actual de las amenazas requiere una solución integrada que abarque todo el ciclo de vida de los datos. Las empresas deben centrarse en acortar las etapas del ciclo de vida entre defensa y detección y entre respuesta y recuperación, para lograr una capacidad de ciber-resiliencia. En una encuesta reciente de IDC, los consultados indicaron que «crear planes sólidos de resiliencia» es una práctica tecnológica de importancia para brindar seguridad a la nube.

El marco de ciberresiliencia

La ciberresiliencia es un marco diseñado para ayudar a las empresas a hacer frente a un ataque. No se trata de una única capa de protección o de un único producto, sino de la forma en que las empresas pueden estructurar sus defensas de manera que ningún evento resulte catastrófico. La ciberresiliencia es un proceso iterativo que le permite recuperarse de un ataque. En comparación con las defensas tradicionales que ya no sirven una vez ocurrido el incidente, la ciberresiliencia ofrece una vigilancia constante en toda la organización.

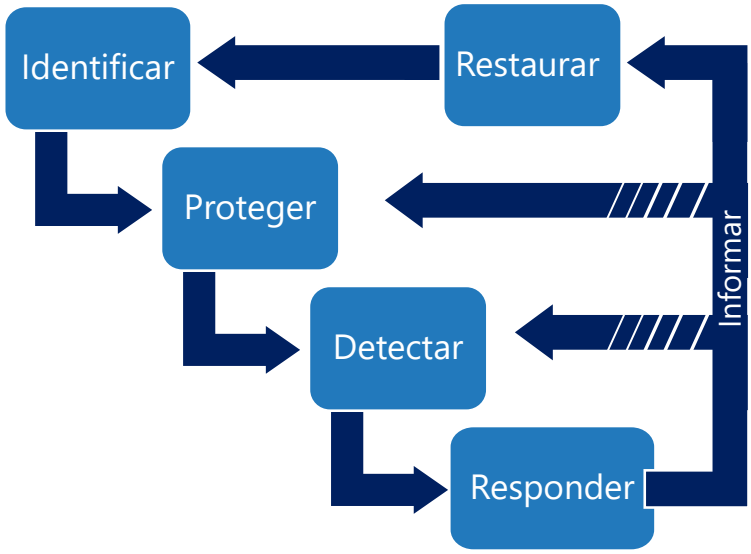
El marco de ciberresiliencia está compuesto por cinco acciones (Figura 5):

- **Identificar:** correlación de activos y procesos críticos, evaluación del riesgo y la preparación para afrontarlo, etc.
- **Proteger:** primera línea tradicional de los mecanismos de seguridad defensivos
- **Detectar:** análisis de la seguridad, verificación de la integridad de los datos de configuración en tiempo real
- **Responder:** respuesta ante una vulneración de la seguridad o falla de sistemas
- **Restaurar:** mecanismos coordinados de restauración

La principal ventaja del marco de ciberresiliencia es que está dirigido al negocio. Tradicionalmente, la seguridad funcionaba como un componente adicional del negocio. La ciberresiliencia integra la seguridad dentro de la empresa en sí, lo que permite que los cinco componentes estén presentes en todas las áreas del negocio.

FIGURA 5

El marco de ciberresiliencia



Fuente: IDC, 2020

¿El evento o sus consecuencias?

Una y otra vez el sector ha demostrado que los ataques tendrán éxito. La seguridad es compleja, y sencillamente no hay manera de probar que un entorno sea totalmente seguro. Los atacantes siguen utilizando métodos innovadores para irrumpir en las organizaciones, recurriendo a cualquier táctica que sea necesaria para lanzar un ataque exitoso. Lo mejor que puede esperar una organización es contar con una infraestructura reforzada, funciones y procesos auditables, usuarios capacitados, personal de seguridad idóneo y procesos de monitoreo continuo. Estar en esa posición sería fantástico, pero lo primordial para casi todas las organizaciones es crear un enfoque renovado sobre lo que sucede después de un ataque. Si con una lista variada de controles y verificaciones ya sabemos que un ataque será exitoso en algún punto, ¿no es razonable estar preparados para las consecuencias? Cuando un ataque tiene éxito, las empresas deben hallar una manera de acortar el ciclo entre detección y respuesta, y el ciclo entre respuesta y restauración. Cuanto más cerca se pueda estar de lograr una continuidad de las operaciones, mejor preparados estaremos, incluso después de sufrir un ciberataque.

El negocio como entidad es implacable. No le importa cuán avanzado sea un ataque, ni cómo el atacante pudo infiltrarse en la organización. El negocio debe seguir funcionando, pero la persistencia no es suficiente. Los clientes de hoy son exigentes, especialmente en medio de una crisis. En este mundo digital, desean que los servicios estén siempre disponibles, y las empresas simplemente no pueden darse el lujo de negarse. Antes de la pandemia de COVID-19, las operaciones de negocio resilientes y los programas de experiencia del cliente estaban bien abajo en la lista de prioridades. Tras el inicio de la pandemia, ahora se ubican en los dos primeros puestos de la lista. En épocas de crisis, la continuidad de las operaciones y el cuidado del cliente son las prioridades principales (Figura 6).

FIGURA 6

Prioridades de la alta gerencia: antes y después del COVID-19

Prioridades antes de la COVID-19 (enero de 2020)

Ranking de prioridades	Temas en la agenda para la empresa del futuro
1	Programas de lealtad digital
1	Resiliencia de la infraestructura digital
3	Programas de datos (para obtener insights sobre nuestras operaciones de negocio, productos y/o ecosistemas)
4	Transformación del lugar de trabajo
4	Capacidades de desarrollo de software para impulsar la innovación de productos/experiencia
4	Nuevos ecosistemas en el sector
7	Operaciones empresariales resilientes
8	Programas centrados en la experiencia del cliente
9	Programas de conectividad

Prioridades después de la COVID-19 (mayo de 2020)

Ranking de prioridades	Temas en la agenda para la empresa del futuro
1	Operaciones empresariales resilientes
2	Programas centrados en la experiencia del cliente
3	Programas de datos (para obtener insights sobre nuestras operaciones de negocio, productos y/o ecosistemas)
4	Programas de conectividad
5	Capacidades de desarrollo de software para impulsar la innovación de productos/experiencia
6	Programas de lealtad digital
7	Nuevos ecosistemas en el sector
8	Resiliencia de la infraestructura digital
9	Transformación del lugar de trabajo

n = 483 (prioridades antes de la COVID-19); n = 908 (prioridades después del COVID-19)

Nota: Los encuestados son quienes toman decisiones de tecnología a nivel global.

Fuente: Encuestas de IDC "*The CxO View of the Future Enterprise in the Digital Economy",* enero-febrero de 2020 y "*COVID-19 Impact on IT Spending Survey",* del 7 al 14 de mayo 2020

Al emplear estrategias para minimizar los tiempos operativos de detección, respuesta y restauración, las organizaciones no solo pueden reducir el costo de un incidente sino también, con el tiempo, crear una ventaja competitiva. Según IDC, las empresas que puedan minimizar las interrupciones tendrán una enorme ventaja con respecto a las que no están bien preparadas para generar confianza entre sus consumidores y socios de negocio.

PERSPECTIVAS FUTURAS

Las cinco tecnologías clave de la ciberresiliencia

Aunque el marco de ciberresiliencia pueda parecer intuitivo, debe implementarse a través de una cuidadosa selección de tecnologías. No existe un único producto que pueda crear un entorno ciberresiliente, sino que existen tecnologías clave que una organización puede implementar para afrontar una posible interrupción en las actividades como consecuencia de un ciberataque. Las cinco tecnologías que se describen en las siguientes secciones son fundamentales para que las organizaciones puedan crear un entorno resiliente.

Automatización y orquestación para la recuperación de plataformas y datos de aplicaciones

El término "automatización" siempre fue aterrador para los profesionales de la seguridad y ha generado preocupación en torno a la respuesta automática en todo el sector desde que existen las soluciones automatizadas. Pero en el entorno altamente automatizado de los ataques actuales, la automatización de la inteligencia es fundamental, porque la escasez de habilidades de TI sigue siendo un problema apremiante: se necesitan 10,5 millones de FTE (equivalentes a tiempo completo) adicionales en los próximos cinco años (Figura 7). En lugar de emplear métodos tradicionales como la

solución, los profesionales de la seguridad deben incorporar la orquestación y la automatización como parte de la respuesta.

FIGURA 7

Escasez de habilidades de TI

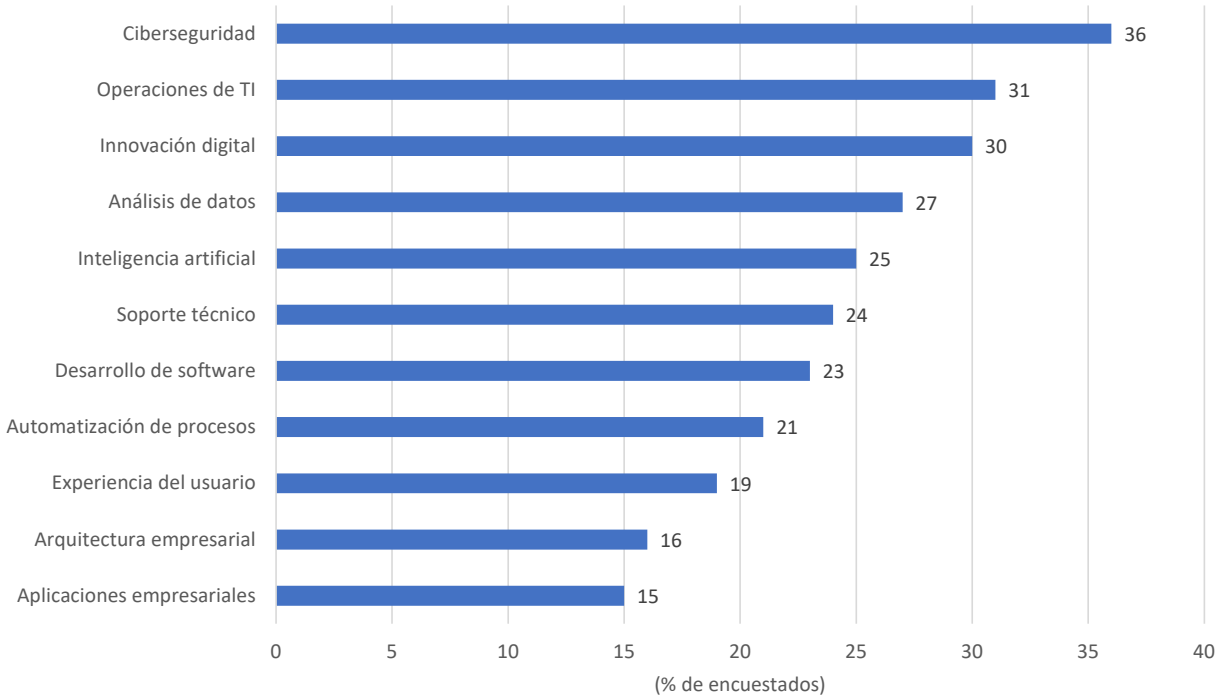
Fuente: IDC, 2020

Durante una crisis aumenta la demanda de las habilidades que no abundan. Las organizaciones identificaron la ciberseguridad y las operaciones de TI como las habilidades principales de TI que necesitarán para recuperarse de la pandemia de COVID-19 (Figura 8).

FIGURA 8

Habilidades importantes de TI que se deben construir, reconstruir o contratar en la primera ola de recuperación económica

P. *¿Cuáles serán las habilidades de TI más importantes que su empresa necesitará construir, reconstruir o contratar en la primera ola de recuperación económica (después de la pandemia de COVID-19)?*



n= 888

Fuente: Encuesta "*COVID-19 Impact on IT Spending",* IDC, del 4 al 15 de junio 2020

La orquestación no consiste en sacar a los humanos de la ecuación ni habilitar cambios de políticas a ciegas, sino que se trata de aumentar la cantidad de analistas y brindarles rápido acceso a la información y la capacidad de responder con mayor rapidez que si lo hicieran manualmente. Además, para que la recuperación de las aplicaciones sea eficaz, es imprescindible un restablecimiento gradual y progresivo de los sistemas y datos interconectados. El restablecimiento manual de esos sistemas es propenso al error humano, mientras que la codificación de los procesos de restauración mediante plantillas de software que son validadas y evaluadas puede mitigar el riesgo en esos procesos.

Protección air gap en forma de copia a prueba de fallas contra la propagación del malware

La protección del tipo *air gap* consiste en separar sistemas o redes de otros sistemas o redes, por medios físicos o virtuales. Las empresas, por ejemplo, pueden optar por aislar completamente las redes o sistemas que contienen datos altamente sensibles de la red operativa que se utiliza todos los días.

Si bien el perímetro ha desaparecido y las empresas esperan que los datos fluyan por toda la organización, la capacidad de crear segmentos aislados de la red es más importante que nunca. Como hemos visto en recientes infecciones con ransomware, un malware automatizado puede estar diseñado para introducirse en la red y causar estragos rápidamente. De este modo, la organización queda expuesta, tanto internamente como quizás también externamente, según el sistema o los sistemas afectados. En la actualidad, la mejor práctica consiste en crear una copia aislada de los datos críticos a fin de mitigar la exposición externa, proteger a la organización de sufrir interrupciones en sus operaciones y evitar costos innecesarios.

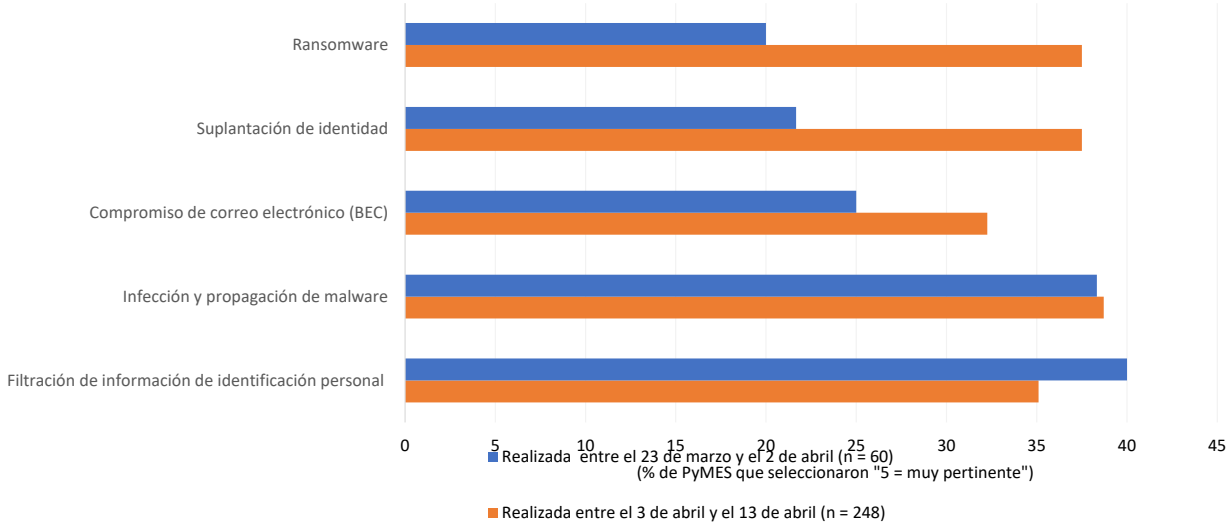
Tecnología de almacenamiento inmutable o WORM para evitar la corrupción o el borrado de datos

El éxito reciente de los ataques con ransomware pone de manifiesto la necesidad de reforzar la protección contra la corrupción o el borrado de datos. Los ciberdelincuentes son oportunistas, que esperan al acecho un momento de debilidad para dar el golpe. Un ejemplo ilustrativo es el reciente auge del malware vinculado a COVID-19 (Figura 9).

FIGURA 9

Opiniones sobre el riesgo que aumenta al mismo ritmo que la pandemia

P. Califique el nivel de pertinencia de los productos de seguridad para mitigar los siguientes riesgos (donde 1 es nada pertinente y 5 es muy pertinente).



Fuente: Encuesta "*North America SMB Security*", IDC, 2020

Todos sabemos que los atacantes procuran borrar los logs para cubrir sus rastros, pero el borrado o la corrupción de los datos puede destruir el negocio. Después de sufrir los efectos de RobbinHood, Maze y REvil, y otros ataques con ransomware, muchas organizaciones se dieron cuenta de que, aunque pagaran el rescate, los atacantes no les devolvían la clave de encriptado. Y, en muchos casos, la clave que les proporcionaban no funcionaba.

Las organizaciones deben contar con tecnologías que les garanticen datos inalterables. Las tecnologías de almacenamiento inmutables o de «escribir una vez, leer muchas» (WORM: *write-once, read-many*) pueden responder a esta necesidad, al permitir que las empresas conserven la integridad de sus datos y mantengan una resiliencia empresarial contra lo que han sido algunos de los ataques más paralizantes de los últimos tiempos. Existen muchas formas de tecnología WORM en la capa de software y en la capa de hardware, y ambas sirven para garantizar que los datos no sean manipulados y para proporcionar una cadena de custodia electrónica.

Copias de momentos determinados y verificación de datos eficientes para identificar rápidamente los datos recuperables

Una vez ocurrido el ataque, las organizaciones necesitan una manera de validar y restaurar rápidamente las copias más recientes y válidas de los datos. Como ya mencionamos, muchos atacantes viven dentro de las redes durante casi un año, lo que significa que con frecuencia las copias de seguridad también están infectadas. Por ese motivo, se necesita una tecnología de momentos determinados muy eficiente para conservar múltiples copias de los datos. Es necesario realizar una verificación constante de los datos en esas copias para identificar de manera proactiva posibles

infecciones y tomar medidas correctivas. También, puede ser de utilidad identificar rápidamente una copia de datos válida para el proceso de restauración. Existen distintos enfoques para respaldar la verificación de datos, con características incorporadas tanto en hardware como en software para garantizar que los datos no fueron infectados.

La verificación de datos es fundamental para los procesos de evaluación de desastres y restablecimiento de las operaciones. En primer lugar, todos deseamos garantizar que los datos replicados o de copia de seguridad tengan integridad, y que la replicación o copia de seguridad se lleve a cabo según lo convenido. En segundo lugar, deseamos inspeccionar los datos replicados o de copia de seguridad para garantizar que la misma infección que afectó los datos de producción no se haya propagado también a los datos replicados o de copia de seguridad. Según el sistema sobre el que se está realizando la copia de seguridad, los usuarios pueden emplear muchas técnicas de verificación de datos. Por ejemplo, un sistema de base de datos puede contar con herramientas nativas de selección e inspección que sirven para aportar capacidades dentro de una solución más amplia de protección de datos.

Unificación y orquestación del panel y la creación de reportes para lograr visibilidad y control

Si bien es cierto que el cumplimiento regulatorio suele tener una mala reputación como un elemento de la lista de verificación que no sirve para mejorar la seguridad global de una organización, la verdad es que validar que haya controles adecuados de los datos, ya instaurados y funcionando correctamente, puede resultar extremadamente eficaz. Además, al incrementarse el monto de las multas por incumplimiento, contar con un sistema eficaz de reportes puede ayudar a las empresas a demostrar que están cumpliendo con las normativas y ahorrarse el tiempo y dinero asociados a costosas auditorías y posibles sanciones. Elaborar reportes de auditoría no tiene que ser una tarea ardua o engorrosa; por suerte se pueden realizar a través de paneles de control eficaces y reportes preconfigurados y automatizados, lo que mejora considerablemente el ánimo de las personas responsables de su ejecución.

DESAFÍOS Y OPORTUNIDADES

La ciberseguridad es el principal desafío en el clima actual de los negocios. La velocidad y el volumen de las amenazas a la seguridad son obstáculos que las organizaciones de todos los tamaños deben sortear, por lo cual la planificación y el despliegue de estrategias de ciberresiliencia ahora cobran más importancia que nunca. Una estrategia eficaz de ciberresiliencia incluye diferentes componentes, tiene amplio alcance y reúne a muchos grupos de interés, que no son solo los profesionales de seguridad, operaciones, ingeniería, asuntos legales y gestión del riesgo, sino también los propietarios de los datos y ejecutivos de líneas de negocio. Para esto se requiere colaboración y planificación en todas las empresas, con diferentes prioridades y profundidad de conocimientos. Esta dinámica al nivel de la organización constituye un desafío que se suele presentar en las empresas más grandes, pero que se puede afrontar si la alta gerencia planifica estratégicamente y establece las prioridades.

CONCLUSIÓN

La ciberresiliencia es esencial para la disponibilidad de los datos y aplicaciones. También es un componente fundamental del camino hacia la transformación digital. Sin medidas adecuadas de ciberresiliencia, las organizaciones serán cada vez más susceptibles a ataques que pueden poner en

jaque a una empresa. Además de los ataques maliciosos, al incrementarse los requisitos en materia de cumplimiento normativo que se extienden a muchas regiones geográficas y sectores, las empresas corren el riesgo de tener que pagar cuantiosas multas si no cuentan con una validación continua de los controles.

La práctica es más que la simple detección de malware, copia de seguridad o recuperación ante desastres: se trata de un enfoque integrado del ciclo de vida en el que participan actores clave de todos los departamentos de la empresa, entre ellos, el CIO, el CISO, el CRO y Operaciones de TI, trabajando juntos para garantizar la disponibilidad de los datos contra todas las amenazas, incluida la plataforma. La ciberresiliencia debe abarcar tanto repositorios locales como en la nube. Los departamentos de TI deben adoptar una postura integral hacia la ciberresiliencia y buscar productos que contemplen toda la extensión de ciberamenazas y que les permitan recuperarse rápidamente de los ataques.

Por último, la ciberresiliencia es un marco que sirve para recuperarse de los ataques. Sin embargo, se necesita una sólida colección de tecnologías clave para abordar cada componente necesario para concretar cada etapa del marco. Ya no se puede describir la seguridad en términos de distintos niveles de confidencialidad, integridad y accesibilidad, sino que debe abarcar estos tres pilares todo el tiempo. Las organizaciones que implementen la ciberresiliencia tendrán una ventaja competitiva en el futuro, cuando los clientes se topen con interrupciones en la disponibilidad de los negocios. Una organización resiliente será aquella que pueda adaptarse y recuperarse rápidamente de los ataques.

Acerca de IDC

International Data Corporation (IDC) es el principal proveedor global de inteligencia de mercado, servicios de consultoría y eventos para los mercados de tecnología de la información, telecomunicaciones y tecnología del consumidor. IDC ayuda a profesionales de TI, ejecutivos de negocio y a la comunidad de inversores a tomar decisiones de compra de tecnología y estrategia de negocio basadas en hechos. Con más de 1100 analistas, IDC ofrece experiencia y conocimientos globales, regionales y locales sobre oportunidades y tendencias de tecnología y del sector en más de 110 países en todo el mundo. Hace 50 años que IDC proporciona conocimientos estratégicos para ayudar a sus clientes a alcanzar sus objetivos clave de negocio. IDC es una subsidiaria de IDG, la empresa líder de medios tecnológicos, investigación y eventos del mundo.

Sede Central

5 Speen Street
Framingham, MA 01701
EE. UU.
508-872-8200
Twitter: @IDC
idc-community.com
www.idc.com