PowerData

¿Qué es la Ciber Resiliencia y cómo lograrla?

Garantizando la privacidad de datos y la continuidad del negocio

Índice

Introducción

Se llame pandemia, ransomware, terremoto o una crisis financiera global, las organizaciones deben estar preparadas para sobrellevar cualquier situación extraordinaria y salir indemnes. Eso, en esencia, es la resiliencia. Esa capacidad de caer de pie en los negocios, necesita su correlato en la tecnología.

Durante la emergencia sanitaria que aún ronda por el mundo, la consultora IDC realizó diversas investigaciones. Uno de los resultados más llamativos es que la violación de datos encabeza el ránking de preocupación de las empresas medianas y grandes, seguida por el malware y los ataques dirigidos. La cuestión del resguardo de información es crítica por diversos factores; en caso de falla:

1. Se podrían ver afectadas las estrategias de negocios.
2. Algunas negociaciones podrían quedar comprometidas.
3. Se expondrían debilidades de la organización.
4. Otros problemas de seguridad podrían derivar de fugas de información.
5. Podrían generarse costosos procesos judiciales o multas por incumplimiento de políticas.

La globalización de las cadenas de valor hace que aún las compañías más pequeñas puedan quedar alcanzadas por normativas referidas a protección de datos, lo que pone en evidencia que los flujos de información deben circular por tuberías sin costuras ni filtraciones.

El tiempo de la Ciber Resiliencia

Esto tiene que ver con que los riesgos pueden tener múltiples orígenes, internos y externos, y adoptar las formas más diversas. A diferencia de la ciberseguridad, la idea de la ciber resiliencia apunta a superar ataques deliberados, fallas o errores accidentales, o imponderables que están más allá de todo control humano, como pueden ser los desastres naturales o los vaivenes de la economía a nivel mundial.

Por otra parte, no se trata sólo de respuestas ante incidentes, sino también de posibilitar el tránsito por las diversas tendencias de la transformación digital, incluyendo los avances previsibles con el multi-cloud, el 5G y la Internet de las Cosas (IoT), de manera segura, aprovechando las ventajas comparativas que pueden ofrecer.

Según cuál sea el tamaño de una organización, la ciber resiliencia puede ocupar a un equipo específico de la compañía, o bien constituir una práctica asimilada por personas de diversas áreas. Es necesario que quienes asuman estos roles, entiendan cómo son las múltiples interacciones del negocio, y cuáles son las interdependencias (internas y externas), mientras se preparan para la acción.

El Instituto de Ingeniería de Software publicó el Modelo de Gestión de Resiliencia CERT, que es un marco de resiliencia cibernética con todas las funciones fundamentales.

La resiliencia cibernética es la fusión de la ciberseguridad, la gestión de riesgos, la continuidad del negocio y la resiliencia, es decir, un conjunto de prácticas que aumentan la capacidad de la organización para resistir y recuperarse de cualquier intento accidental o deliberado de impedir que la organización realice sus funciones básicas.

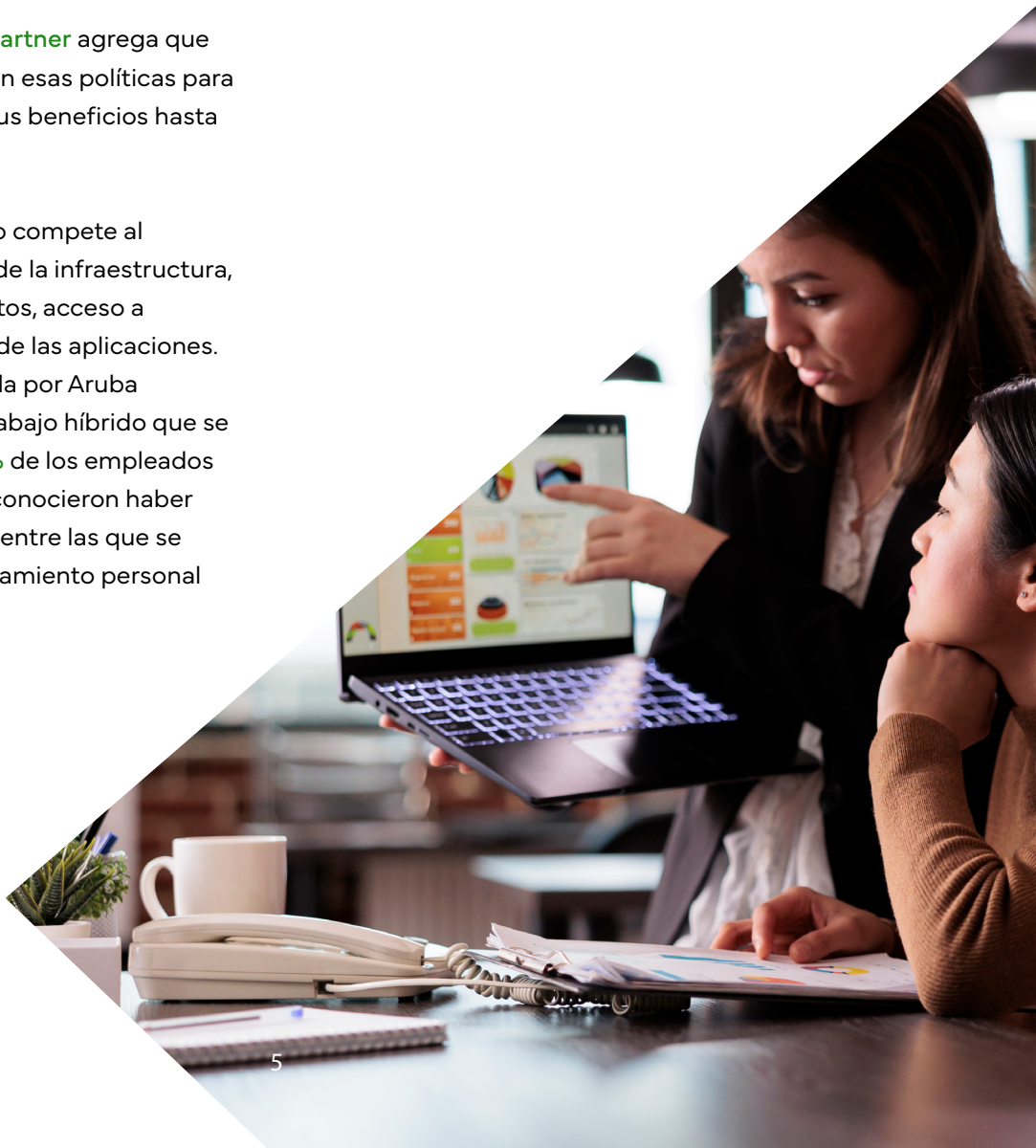
Fuente: IDC

La privacidad de los datos

En el marco de este resguardo de la ciber resiliencia, una cuestión central es la protección de los datos, algo cada día más sensible. Según una investigación de Cisco, el 84% de los consumidores afirma que se preocupa por la privacidad de sus datos y quiere tener más control sobre ellos, y más del 50% rechaza utilizar productos o servicios de compañías que no cuenten con políticas confiables de resguardo de la información personal de sus clientes.

Por su parte, el informe de Gartner agrega que las compañías que sí adoptan esas políticas para retener clientes aumentan sus beneficios hasta en un 30%.

Eso no es un asunto que sólo compete al personal de TI en la gestión de la infraestructura, por ejemplo, de bases de datos, acceso a sistemas o al código fuente de las aplicaciones. Según una encuesta realizada por Aruba Networks en contexto del trabajo híbrido que se impuso en pandemia, el 70% de los empleados de diferentes compañías reconocieron haber tenido conductas de riesgo, entre las que se destacan el compartir equipamiento personal utilizado para el trabajo.



La privacidad de los datos

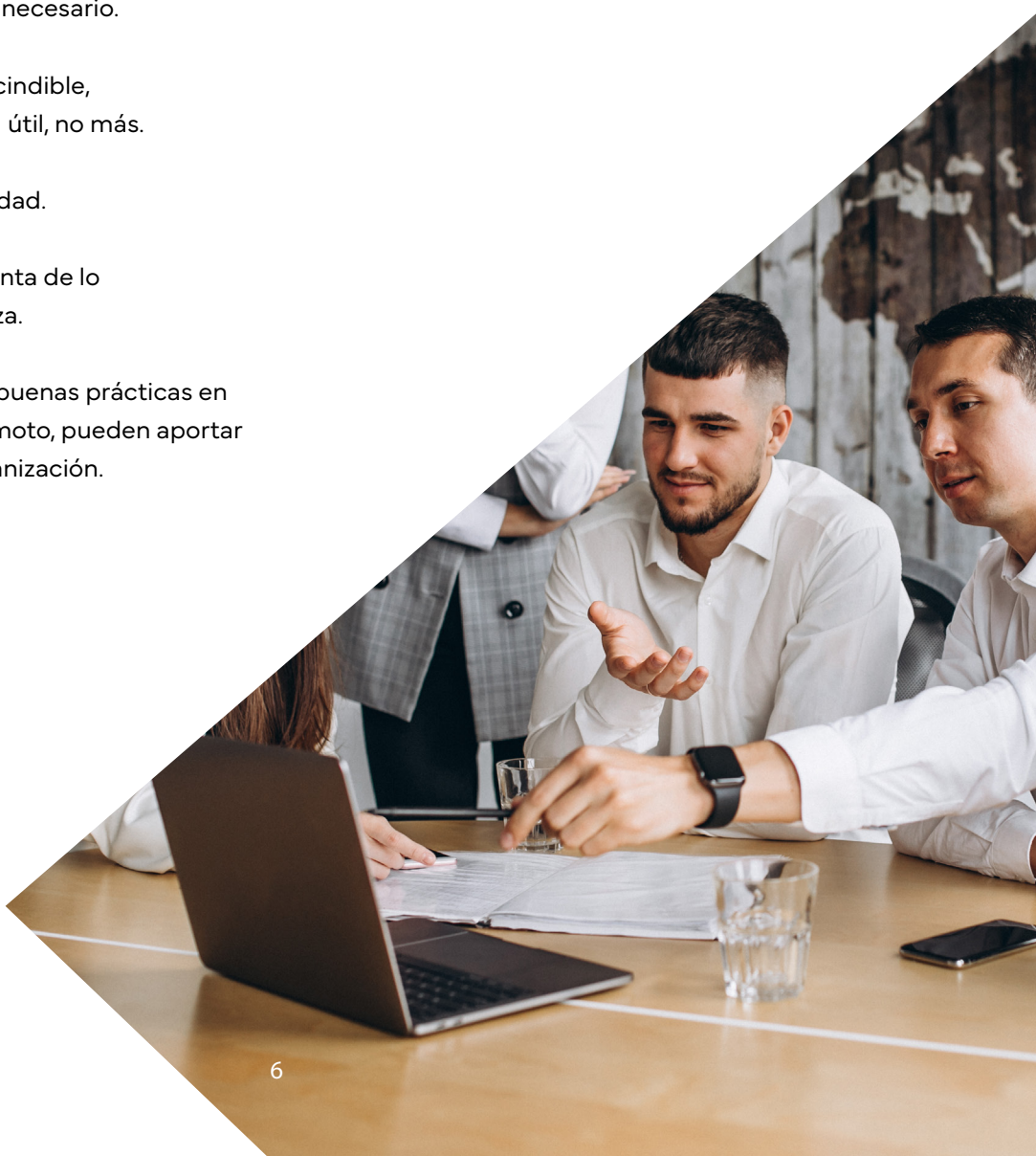
Los principios que debe considerar una política de resguardo de la privacidad, incluyen:

- Legalidad y transparencia.
- Acotar el para qué del registro de datos personales.
- Minimizar los datos requeridos.
- Registrar con precisión lo necesario.
- Almacenar sólo lo imprescindible, durante el tiempo que sea útil, no más.
- Integridad y confidencialidad.
- Mecanismos para dar cuenta de lo registrado y cómo se utiliza.

Todo esto, combinado con buenas prácticas en el trabajo colaborativo y remoto, pueden aportar un gran diferencial a la organización.

Para 2023, el 65 % de la población mundial tendrá sus datos personales cubiertos por alguna normativa de privacidad moderna.

Fuente: Gartner



¿Cómo ser resiliente?

Si el ser ciber resiliente pasará a ser algo constitutivo de la organización, es necesario que haya un alineamiento entre la dirección estratégica y el equipo que gobierne esa resiliencia.

El segundo paso es contar con un plan o marco de trabajo que contenga todos los aspectos involucrados. Luego, es necesario reconocer cuáles son los riesgos y potenciales adversarios que podrían ser un factor de riesgo. Finalmente, hay un cuarto paso que es el estímulo de una cultura colectiva orientada a la ciber resiliencia, lo que convierte a los responsables de sistemas en líderes, entrenadores, agentes de cambio y evangelistas de este paradigma.

Transitar este camino requiere de claridad en los objetivos. Se apunta a la ciber resiliencia para:

- Anticipar interrupciones o eventos disruptivos. Soportar eventos disruptivos o ataques en sistemas críticos.
- Responder a ataques o eventos disruptivos que se produzcan (guías de acción y roles predeterminados).
- Adaptar a la organización para enfrentar escenarios potenciales que impliquen riesgo o problemas.

En resumen, la resiliencia cibernética es la capacidad de una organización para permitir la aceleración del negocio (resiliencia empresarial) preparándose para, responder y recuperarse de amenazas cibernéticas. Una organización con esta gimnasia puede adaptarse a situaciones conocidas y desconocidas, crisis, amenazas, adversidades y desafíos. El objetivo final de la resiliencia cibernética es ayudar a una organización a prosperar ante condiciones adversas, sean crisis, pandemias, volatilidades financieras u otras que el futuro próximo pondrá, seguramente, en el camino.

PowerData

PowerData, es una compañía multinacional de origen español con gran presencia regional, está enfocada en todo lo relacionado con la Gestión y Gobierno de Datos, tiene una trayectoria de más de 20 años impulsado una cultura Data-Driven en las empresas de la mano de sus aliados tecnológicos.

Te invitamos a explorar los proyectos donde aportamos valor con la gestión de datos. powerdata.es