TECNOLOGÍA

Ayudar a las empresas a mejorar su resiliencia

Durante la cuarentena, la tecnología ha pasado de ser una palanca de crecimiento a convertirse en un factor de continuidad del negocio. A medida que las empresas se ponen a punto para el futuro, es necesario que la tecnología consiga ambos objetivos.

7 junio, 2021

Mercado

La tecnología ha desempeñado un papel fundamental a la hora de mitigar el impacto del virus. Ya sea ayudando a los empleados a realizar su trabajo u ofreciendo una plataforma para suministrar productos y servicios, la tecnología ha hecho posible nuevas formas de hacer negocios. Sin embargo, de cara al futuro, el desarrollo de la resiliencia mediante la transformación digital implica equilibrar las necesidades a corto plazo con la materialización de oportunidades a largo

sean factores clave para desarrollar la resiliencia operativa de las empresas. De hecho, según la última edición del estudio Global Business Pulse de Grant Thornton, el 44% de las empresas de tecnología encuestadas asegura que han podido operar utilizando sus fondos existentes sin tener que hacer recortes de cara al impacto generado por el COVID-19.

Reevaluar los sistemas de IT

Tras la rápida adopción de la tecnología en las primeras fases de la crisis, conviene examinar ahora qué medidas y sistemas se han adoptado y evaluar si son sostenibles en una nueva escala y con nuevas formas de trabajo que permitan operaciones más seguras y eficientes.

Frente a esta realidad, Eduardo Diego, gerente de sistemas en Grant Thornton Argentina, comenta: "La llegada de la pandemia provocó que las empresas tuvieran que implementar esquemas de trabajo remoto para poder seguir operando. Muchas estaban preparadas para afrontar este desafío y lo pudieron implementar sin demasiados inconvenientes, pero muchas otras han tenido que improvisar soluciones de emergencia, con lo que tenían, asumiendo un alto riesgo tanto en la continuidad de la operación como de ciberseguridad."

Considere la posibilidad de realizar una auditoría remota del *hardware* y *software* de su organización para asegurarse de que sus equipos de trabajo dispongan de las herramientas

Mercado

puedan estar expuestas por las prácticas de teletrabajo adoptadas.

En consonancia, existen algunas medidas básicas que se pueden tener en cuenta al momento de preservar la seguridad informática como pueden ser la utilización de antivirus y protección; tomar precaución cuando se comparten datos personales; utilizar navegadores web actualizados; actualizar las contraseñas; y proteger los datos mediante cifrados, entre otras.

La automatización

Un aspecto fundamental de la crisis es el grado de presión al que se han visto sometidos los empleados para cumplir determinados procesos rutinarios desde el hogar, al tiempo que lidiaban con otros compromisos familiares. En este sentido, más de la mitad de las empresas de tecnología encuestadas (51%) han implementado el trabajo remoto como acción para hacerle frente al coronavirus.

Trabajar de forma remota implica estar conectado con compañeros de trabajo y clientes a través de dispositivos móviles y/o computadoras. Ligado a esto, es importante destacar los avances de la automatización y la robótica, los cuales sirven de sostén frente a los procesos operativos. Por ejemplo, la RPA (automatización robótica de procesos) es una tecnología de software fácil de usar para todo aquel que quiera automatizar tareas digitales. Con la RPA, los usuarios de software pueden crear robots de software o "bots" que pueden aprender, imitar y luego ejecutar

Inversiones adecuadas en tecnología

Antes del COVID-19, puede que fuera necesario convencer a algunas empresas de la necesidad de adoptar ciertas tecnologías y mejoras digitales, pero ahora la transformación digital ha pasado de ser una aspiración deseable a ser un elemento esencial en todos los ámbitos.

Asimismo, 45,6% de los encuestados a nivel mundial afirma que tendrán que hacer un mayor uso de la tecnología y la transformación digital tras la crisis del COVID. Al mismo tiempo, el 78% de las empresas tienen previsto mantener o aumentar sus niveles de inversión en tecnología en los próximos 12 meses. A nivel nacional, el 42% de los encuestados asegura que aumentarán la inversión en tecnología.

Adicionalmente, Diego afirma: "las empresas deben invertir en la digitalización de sus procesos para hacerlos más accesibles, más ágiles y seguros, de manera de estar mejor preparados para adecuar sus operaciones a los cambios de mercado que se vayan produciendo."

Una vez transformados en información utilizable, los datos constituyen un valioso activo sobre el que desarrollar la resiliencia y volver a poner a punto su negocio. Asegúrese de que cuenta con los análisis, cuadros de mando, informes y estructuras de datos adecuados para ayudarle en la toma de decisiones.

Mercado

atravesando dificultades económicas y que pueda estar dispuesto a vender la empresa. Utilice fuentes de información como los datos de clientes, las encuestas a empleados, la información

de organismos comerciales o de analistas de mercado para ayudarle a mejorar su entendimiento.

Los datos son fundamentales para el éxito de los negocios y para mantenerse al día en un entorno tan cambiante como el actual. Independientemente del escenario al que se enfrente, obtener informes precisos de lo que está sucediendo en su negocio es clave y seguirá siéndolo cuando haya pasado la pandemia.

Riesgos de ciberseguridad

Con el objetivo de facilitar el teletrabajo, se han tenido que generar puntos de acceso remotos a los empleados, algo que los hackers aprovechan para realizar ataques y poder acceder a la información interna de las empresas. Estos ataques suelen representar un golpe duro para cualquier compañía o negocio, principalmente en términos económicos y de credibilidad, ya que una filtración de datos supone una pérdida en la confianza de los clientes hacia la compañía.

El gran número de empleados que probablemente trabajen a distancia en el futuro aumentará la "superficie de ataque" de los ciberdelincuentes, incrementándose las oportunidades de hackear

En Argentina, desde la Defensoría del Pueblo bonaerense advierten que se han incrementado los casos de estafas virtuales a través de emails y WhatsApp por parte de los ciberdelincuentes que intentan robar dinero. Los casos denunciados durante el 2020 presentan las características propias del "phishing" o suplantación de identidad, en donde se intenta imitar una comunicación oficial y así poder engañar al usuario. Según Fortinet, las amenazas de correos electrónicos de phishing se extendieron por América Latina con archivos HTML adjuntos, tratando de redirigir el navegador web a sitios web maliciosos.

Las empresas también deben adoptar políticas de privacidad por diseño y de segmentación de datos, de modo que tengan conocimientos y control sobre quién tiene acceso a los datos tanto en entornos propios como en entornos externos. También deben asegurarse de que los proveedores de servicios tecnológicos cumplan los estándares básicos de seguridad y comprendan los riesgos que existen en la cadena de suministro.

"Considerando las encuestas que se vienen realizando, tanto empleados como empleadores coinciden en que el esquema de trabajo remoto se va a seguir aplicando, en mayor o menor medida, aún después de superada la pandemia. Esto implica que las empresas deben invertir

para mejorar las soluciones que implementaron pensándolas ya no como algo transitorio sino como el escenario futuro, contemplando esquemas de continuidad de negocio y aplicando

Las oportunidades futuras asociadas con la tecnología implican formación, mejora de habilidades y adquisición del talento adecuado, pero también conllevan un cierto nivel de comprensión y conocimiento a nivel del consejo.

Los ganadores emergentes serán las empresas que hayan adaptado su capacidad tecnológica y su visión más rápidamente durante este período. Aquellas entidades que tengan un claro entendimiento de las oportunidades futuras, así como de los riesgos que la tecnología puede mitigar, estarán bien posicionadas para operar y prosperar en el nuevo entorno operativo.

"Finalmente, en un entorno de trabajo más descentralizado, se deben incrementar las acciones de concientización del personal mostrando los riesgos de ciberseguridad a los que nos exponemos cotidianamente si no estamos atentos y realizamos acciones sin evaluar los riesgos. Esta actividad de concientización no solo ayuda a proteger los datos de las empresas sino que también ayuda a las personas a proteger sus datos personales, bancarios, etc.", concluye Diego.

Mercado

Notas Relacionadas

La sector de retail pierde millones por inactividad
23 septiembre, 2015

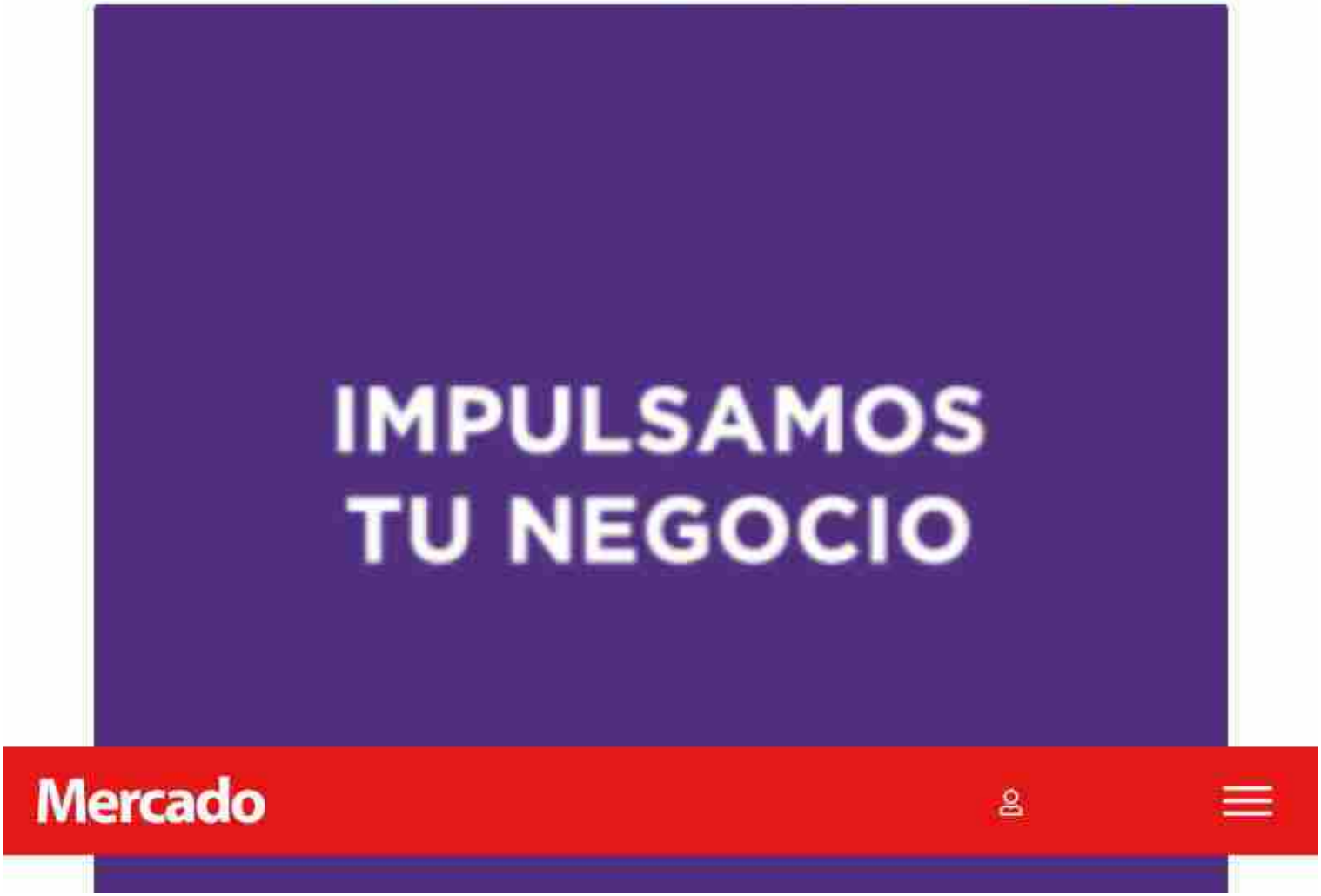
Banca móvil cada vez con más usuarios
14 septiembre, 2015

Desde ahora, todas las empresas son tecnológicas
15 febrero, 2019

Responsabilidad de la empresa
14 abril, 2020

Grupo Núcleo presenta soluciones de seguridad
1 julio, 2015


Aprendé
a organizar
tu economía en
educacionfinancieragalicia.com.ar
Mercado
Galicia


IMPULSAMOS
TU NEGOCIO
Mercado

Notas Relacionadas

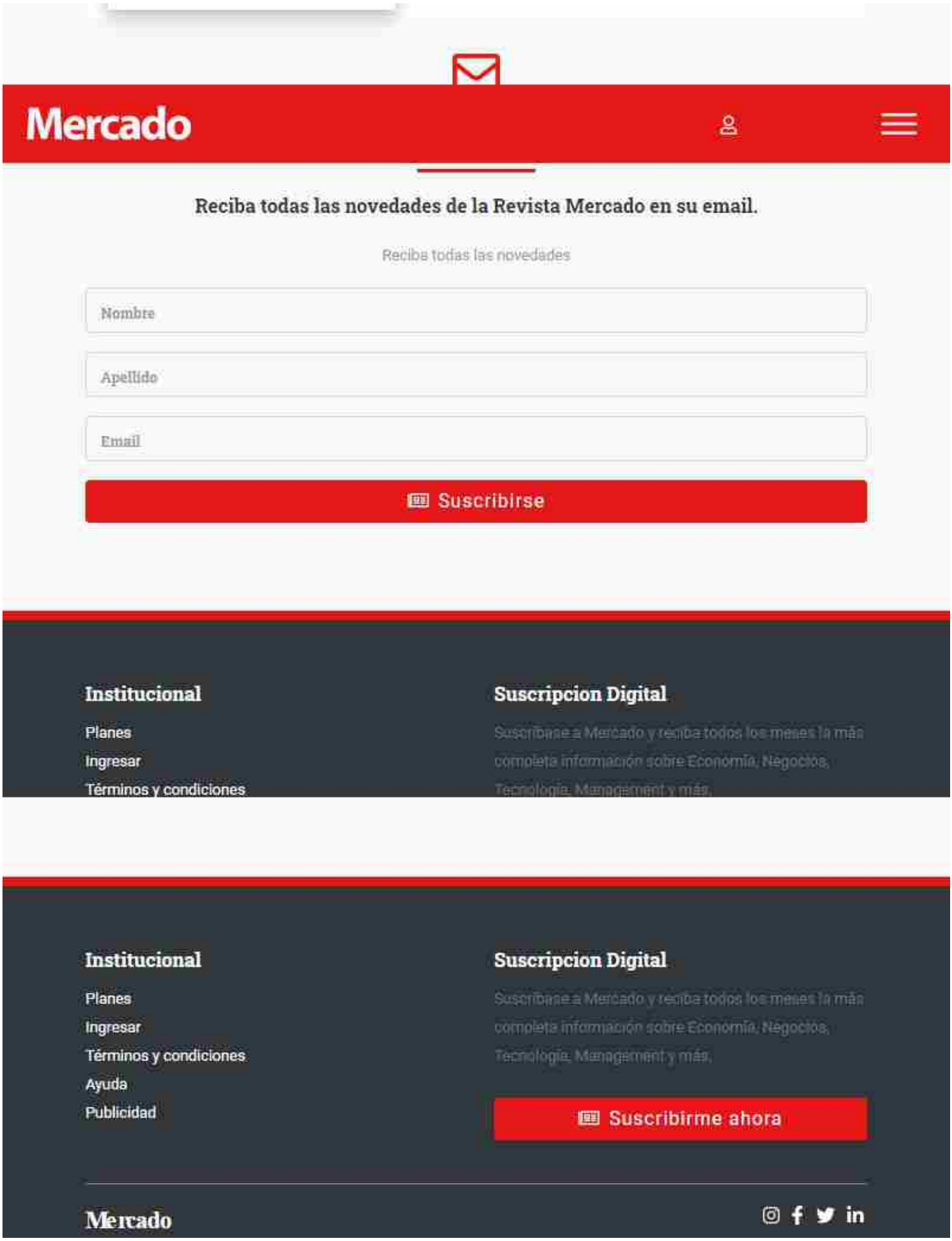
Japón también quiere asegurarse semiconductores

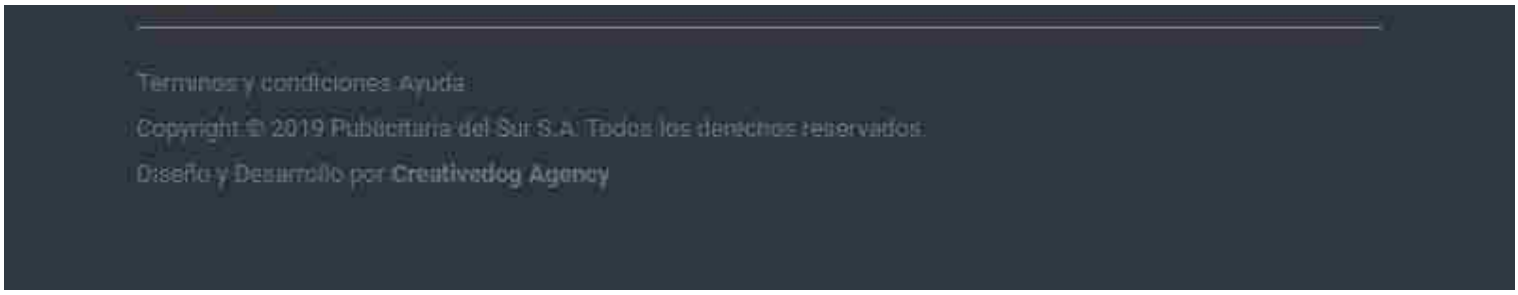
Recurre a incentivos fiscales para atraer a jugadores extranjeros.

Leer más

La tecnología del futuro: entre la realidad y la utopia

En 1982 se estrenó la película *Blade Runner* bajo la dirección de Ridley Scott. La película relata cómo, en el año 2019, la bioingeniería se había desarrollado de tal manera


Mercado
Reciba todas las novedades de la Revista Mercado en su email.
Reciba todas las novedades
Nombre
Apellido
Email
Suscribirse
Institucional
Planes
Ingresar
Términos y condiciones
Suscripcion Digital
Suscribirse a Mercado y reciba todos los meses la más completa información sobre Economía, Negocios, Tecnología, Management y más.
Institucional
Planes
Ingresar
Términos y condiciones
Ayuda
Publicidad
Suscripcion Digital
Suscribirse a Mercado y reciba todos los meses la más completa información sobre Economía, Negocios, Tecnología, Management y más.
Suscribirme ahora
Mercado


Terminos y condiciones Ayuda
Copyright © 2019 Publicitaria del Sur S.A. Todos los derechos reservados
Diseño y Desarrollo por Creativedog Agency

Durante la cuarentena, la tecnología ha pasado de ser una palanca de crecimiento a convertirse en un factor de continuidad del negocio. A medida que las empresas se ponen a punto para el futuro, es necesario que la tecnología consiga ambos objetivos. La tecnología ha desempeñado un papel fundamental a la hora de mitigar el impacto del virus. Ya sea ayudando a los empleados a realizar su trabajo u ofreciendo una plataforma para suministrar productos y servicios, la tecnología ha hecho posible nuevas formas de hacer negocios. Sin embargo, de cara al futuro, el desarrollo de la resiliencia mediante la transformación digital implica equilibrar las necesidades a corto plazo con la materialización de oportunidades a largo plazo.

Pocas empresas pueden dudar de que la tecnología, la transformación digital y la innovación sean factores clave para desarrollar la resiliencia operativa de las empresas. De hecho, según la última edición del estudio Global Business Pulse de Grant Thornton, el 44% de las empresas de tecnología encuestadas asegura que han podido operar utilizando sus fondos existentes sin tener que hacer recortes de cara al impacto generado por el COVID-19.

Reevaluar los sistemas de IT

Tras la rápida adopción de la tecnología en las primeras fases de la crisis, conviene examinar ahora qué medidas y sistemas se han adoptado y evaluar si son sostenibles en una nueva escala y con nuevas formas de trabajo que permitan operaciones más seguras y eficientes.

Frente a esta realidad, Eduardo Diego, gerente de sistemas en Grant Thornton Argentina, comenta: "La llegada de la pandemia provocó que las empresas tuvieran que implementar esquemas de trabajo remoto para poder seguir operando. Muchas estaban preparadas para afrontar este desafío y lo pudieron implementar sin demasiados inconvenientes, pero muchas otras han tenido que improvisar soluciones de emergencia, con lo que tenían, asumiendo un alto riesgo tanto en la continuidad de la operación como de ciberseguridad."

Considere la posibilidad de realizar una auditoría remota del hardware y software de su organización para asegurarse de que sus equipos de trabajo dispongan de las herramientas necesarias para desempeñar sus cometidos. También es vital mantenerse al tanto de la seguridad de las IT y evaluar de forma continua cualquier vulnerabilidad a la que la empresa pueda estar expuesta por las prácticas de teletrabajo adoptadas.

En consonancia, existen algunas medidas básicas que se pueden tener en cuenta al momento de preservar la seguridad informática como pueden ser la utilización de antivirus y protección; tomar precaución cuando se comparten datos personales; utilizar navegadores web actualizados; actualizar las contraseñas; y proteger los datos mediante cifrados, entre otras.

La automatización

Un aspecto fundamental de la crisis es el grado de presión al que se han visto sometidos los empleados para cumplir determinados procesos rutinarios desde el hogar, al tiempo que lidiaban con otros compromisos familiares. En este sentido, más de la mitad de las empresas de tecnología encuestadas (51%) han implementado el trabajo remoto como acción para hacerle frente al coronavirus.

Trabajar de forma remota implica estar conectado con compañeros de trabajo y clientes a través de dispositivos móviles y/o computadoras. Ligado a esto, es importante destacar los avances de la automatización y la robótica, los cuales sirven de sostén frente a los procesos operativos. Por ejemplo, la RPA (automatización robótica de procesos) es una tecnología de software fácil de usar para todo aquel que quiera automatizar tareas digitales. Con la RPA, los usuarios de software pueden crear robots de software o "bots" que pueden aprender, imitar y luego ejecutar procesos empresariales basados en reglas, descargando a los usuarios de aquellas tareas más repetitivas y reduciendo de forma importante los fallos y errores humanos.

Inversiones adecuadas en tecnología

Antes del COVID-19, puede que fuera necesario convencer a algunas empresas de la necesidad de adoptar ciertas tecnologías y mejoras digitales, pero ahora la transformación digital ha pasado de ser una aspiración deseable a ser un elemento esencial en todos los ámbitos.

Asimismo, 45,6% de los encuestados a nivel mundial afirma que tendrán que hacer un mayor uso de la tecnología y la transformación digital tras la crisis del COVID. Al mismo tiempo, el 78% de las empresas tienen previsto mantener o aumentar sus niveles de inversión en tecnología en los próximos 12 meses. A nivel nacional, el 42% de los encuestados asegura que aumentarán la inversión en tecnología.

Adicionalmente, Diego afirma: "las empresas deben invertir en la digitalización de sus procesos para hacerlos más accesibles, más ágiles y seguros, de manera de estar mejor preparados para adecuar sus operaciones a los cambios de mercado que se vayan produciendo."

Una vez transformados en información utilizable, los datos constituyen un valioso activo sobre el que desarrollar la resiliencia y volver a poner a punto su negocio. Asegúrese de que cuenta con los análisis, cuadros de mando, informes y estructuras de datos adecuados para ayudarle en la toma de decisiones.

Los directivos necesitan acceder a una serie de indicadores externos a su negocio que les ayuden a encontrar y materializar nuevas oportunidades, como pueda ser un rival que esté atravesando dificultades económicas y que pueda estar dispuesto a vender la empresa. Utilice fuentes de información como los datos de clientes, las encuestas a empleados, la información de organismos comerciales o de analistas de mercado para ayudarle a mejorar su entendimiento.

Los datos son fundamentales para el éxito de los negocios y para mantenerse al día en un entorno tan cambiante como el actual. Independientemente del escenario al que se enfrente, obtener informes precisos de lo que está sucediendo en su negocio es clave y seguirá siéndolo cuando haya pasado la pandemia.

Riesgos de ciberseguridad

Con el objetivo de facilitar el teletrabajo, se han tenido que generar puntos de acceso remotos a los empleados, algo que los hackers aprovechan para realizar ataques y poder acceder a la información interna de las empresas. Estos ataques suelen representar un golpe duro para cualquier compañía o negocio, principalmente en términos económicos y de credibilidad, ya que una filtración de datos supone una pérdida en la confianza de los clientes hacia la compañía.

El gran número de empleados que probablemente trabajen a distancia en el futuro aumentará la "superficie de ataque" de los ciberdelincuentes, incrementándose las oportunidades de hackear los sistemas informáticos de las empresas y poner en jaque a empleados específicos. Las empresas deben asegurarse de que sus sistemas cloud y sus infraestructuras sean seguros y de que haya claridad en cuanto a quién es responsable de protegerlos y supervisarlos.

En Argentina, desde la Defensoría del Pueblo bonaerense advierten que se han incrementado los casos de estafas virtuales a través de emails y WhatsApp por parte de los ciberdelincuentes que intentan robar dinero. Los casos denunciados durante el 2020 presentan las características propias del "phishing" o suplantación de identidad, en donde se intenta imitar una comunicación oficial y así poder engañar al usuario. Según Fortinet, las amenazas de correos electrónicos de phishing se extendieron por América Latina con archivos HTML adjuntos, tratando de redirigir el navegador web a sitios web maliciosos.

Las empresas también deben adoptar políticas de privacidad por diseño y de segmentación de datos, de modo que tengan conocimientos y control sobre quién tiene acceso a los datos tanto en entornos propios como en entornos externos. También deben asegurarse de que

los proveedores de servicios tecnológicos cumplan los estándares básicos de seguridad y comprendan los riesgos que existen en la cadena de suministro.

"Considerando las encuestas que se vienen realizando, tanto empleados como empleadores coinciden en que el esquema de trabajo remoto se va a seguir aplicando, en mayor o menor medida, aún después de superada la pandemia. Esto implica que las empresas deben invertir para mejorar las soluciones que implementaron pensándolas ya no como algo transitorio sino como el escenario futuro, contemplando esquemas de continuidad de negocio y aplicando medidas de Ciberseguridad que protejan adecuadamente sus datos.", agrega Diego.

Las oportunidades futuras asociadas con la tecnología implican formación, mejora de habilidades y adquisición del talento adecuado, pero también conllevan un cierto nivel de comprensión y conocimiento a nivel del consejo.

Los ganadores emergentes serán las empresas que hayan adaptado su capacidad tecnológica y su visión más rápidamente durante este período. Aquellas entidades que tengan un claro entendimiento de las oportunidades futuras, así como de los riesgos que la tecnología puede mitigar, estarán bien posicionadas para operar y prosperar en el nuevo entorno operativo.

"Finalmente, en un entorno de trabajo más descentralizado, se deben incrementar las acciones de concientización del personal mostrando los riesgos de ciberseguridad a los que nos exponemos cotidianamente si no estamos atentos y realizamos acciones sin evaluar los riesgos. Esta actividad de concientización no solo ayuda a proteger los datos de las empresas sino que también ayuda a las personas a proteger sus datos personales, bancarios, etc.", concluye Diego.