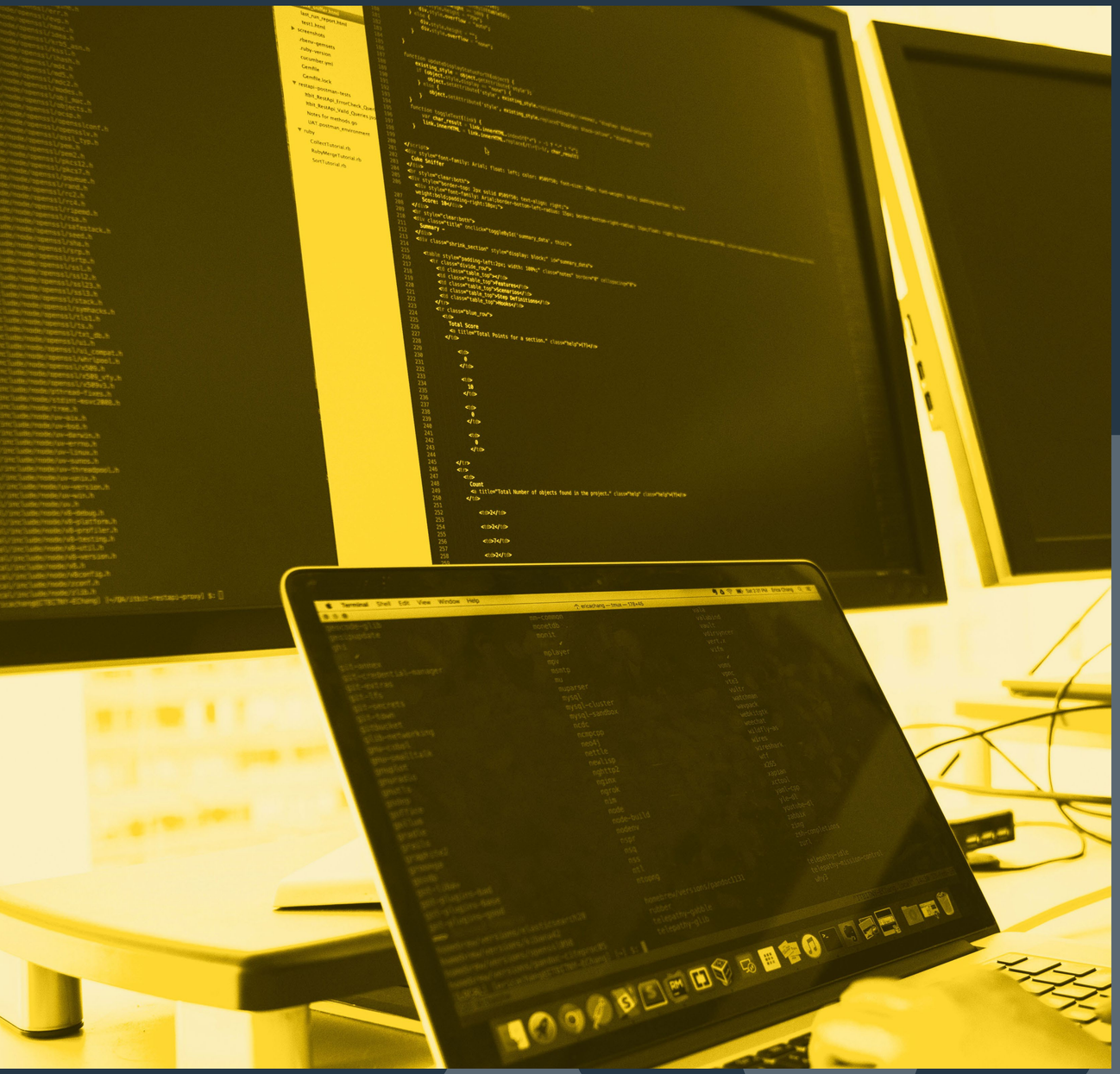


Schneider Electric

SCHNEIDER ELECTRIC – MÉXICO

La nueva realidad de ciberseguridad en México

oxfordbusinessgroup.com

Julio 2021

CONTEXTO GLOBAL

El Covid-19 se extendió rápidamente desde China al resto del mundo durante los primeros meses del 2020. Por tal razón, gobernantes y líderes empresariales se han visto forzados a adaptarse constantemente a la situación socioeconómica y a formular planes efectivos para responder a los retos. Sus metas han tenido dos vertientes; fortalecer la economía y proteger la salud de la población.

La pandemia generó una disrupción en las cadenas de suministro globales, cerró fronteras y restringió severamente la movilidad de las personas, generando cambios quizás permanentes en el comportamiento de los consumidores, los procesos de las empresas, los viajes internacionales y las cadenas de valor. Además de esta forma tangible de disrupción física, el ambiente de negocios en general también se ha visto afectado, con compañías, gobiernos e individuos operando y consumiendo en formas completamente distintas, en ocasiones con la ayuda de una rápida aceleración de la digitalización.

CONTEXTO EN MÉXICO

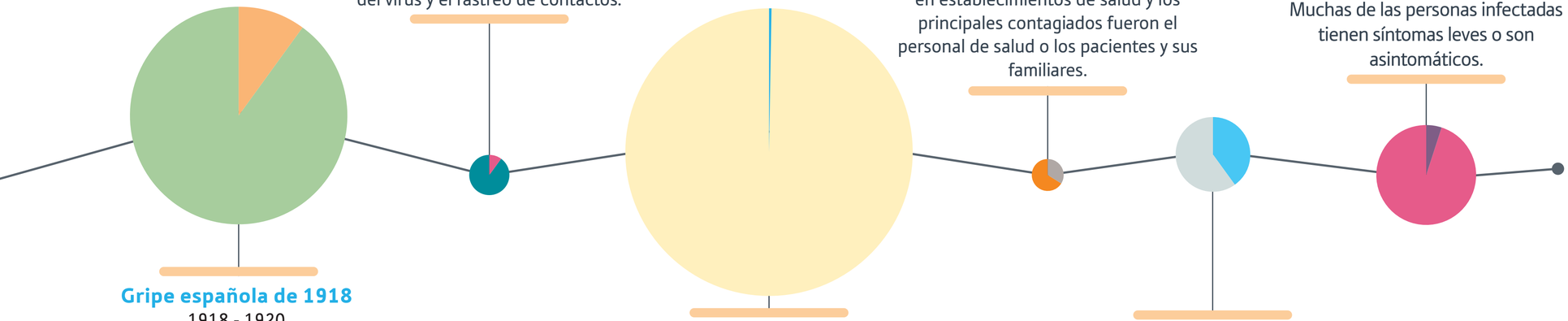
El primer caso confirmado de Covid-19 en México ocurrió el 27 de febrero de 2020, 15 días antes que la Organización Mundial de la Salud (OMS) hiciera la declaratoria oficial de pandemia el 11 de marzo. Se trató de un ciudadano mexicano quien viajó a Italia y regresó con síntomas leves. La Ciudad de México registró su primer caso un día después. El 28 de febrero un ciudadano italiano residente en la capital regresó de Italia y dio positivo en una prueba. De esta manera continuó la tendencia de primeros casos mayoritariamente importados de Europa.

¿Cómo se compara el Covid-19 con pandemias pasadas?

SARS
Noviembre 2002 a Julio 2003
Número de casos: 8096
Letalidad de casos: 10%
Causado por un coronavirus, propagación por gotas respiratorias y superficies contaminadas. Los síntomas severos facilitaron el monitoreo del virus y el rastreo de contactos.

MERS
Septiembre 2012 a Noviembre 2019
Número de casos: 2494
Letalidad de casos: 34%
Causada por un coronavirus propagado por contacto cercano con una persona infectada. Los portadores pueden ser asintomáticos. La mayoría de los casos confirmados sucedieron en establecimientos de salud y los principales contagiados fueron el personal de salud o los pacientes y sus familiares.

Covid-19
Diciembre 2019 –
Número de casos a Junio 2021: 180 millones
Letalidad de casos: ~2.2%
Causado por una cepa novedosa de coronavirus. Altamente contagioso, propagado por gotas respiratorias, aerosoles y otros fluidos corporales. Muchas de las personas infectadas tienen síntomas leves o son asintomáticos.



Gripe española de 1918
1918 - 1920
Número de casos: 500 millones
Letalidad de casos: 10%
Altamente contagiosa, propagación por gotas respiratorias. Transmisión acelerada debido a viviendas aglomeradas; instalaciones sanitarias inadecuadas y falta de entendimiento científico acerca del virus.

H1N1 2009
2009
700 millones a 1.4 mil millones
Letalidad de casos: 0.02 – 0.04%
Se trata de una cepa de la gripe. El tratamiento con antivirales permitió a la mayoría de las personas recuperarse sin complicaciones severas.

Ebola
2014-2016
Número de casos: 28,652
Letalidad de casos: 40%
La letalidad de casos es muy alta: se transmite con menor facilidad a través de un contacto cercano y mediante fluidos corporales. Es más contagioso al final de la enfermedad. No existía tratamiento o vacuna en su momento.

Contexto global

La tasa elevada de contagios y la falta de predictibilidad del Covid-19, aunado a una economía sumamente globalizada, presentó un reto jamás visto respecto a epidemias anteriores. La interconectividad de la economía global y del transporte aéreo en la época actual implicó que fuera difícil contener el virus dentro de las comunidades y fronteras. Esto ocasionó medidas de confinamiento y restricciones sin precedentes en muchos países.

La disminución de la actividad económica resultante obligó a los responsables de gobierno alrededor del mundo a tratar de movilizar una respuesta de salud efectiva y aliviar la carga financiera en los hogares y negocios vulnerables.

Guía de Contenido

Resiliencia

¿Cuál era la situación económica de México antes de la pandemia?

¿Cómo ha evolucionado la preparación digital de México en años recientes?

¿Cuáles aspectos de la preparación digital de México fueron los más robustos al encararse a la pandemia?

Respuesta

¿Cuál fue la respuesta en general del gobierno ante la pandemia?

¿Cómo evolucionó el comportamiento empresarial como resultado de los cambios en el ambiente operativo de los negocios?

¿De qué forma cambiaron las iniciativas digitales debido a la pandemia?

Recuperación

¿Qué papel jugará la digitalización en la recuperación económica de México?

¿De qué forma evolucionará la preponderancia de la ciberseguridad en los siguientes años?

¿Qué aspectos deben mejorar en temas de infraestructura en México para facilitar una recuperación económica impulsada digitalmente?

Reinvención

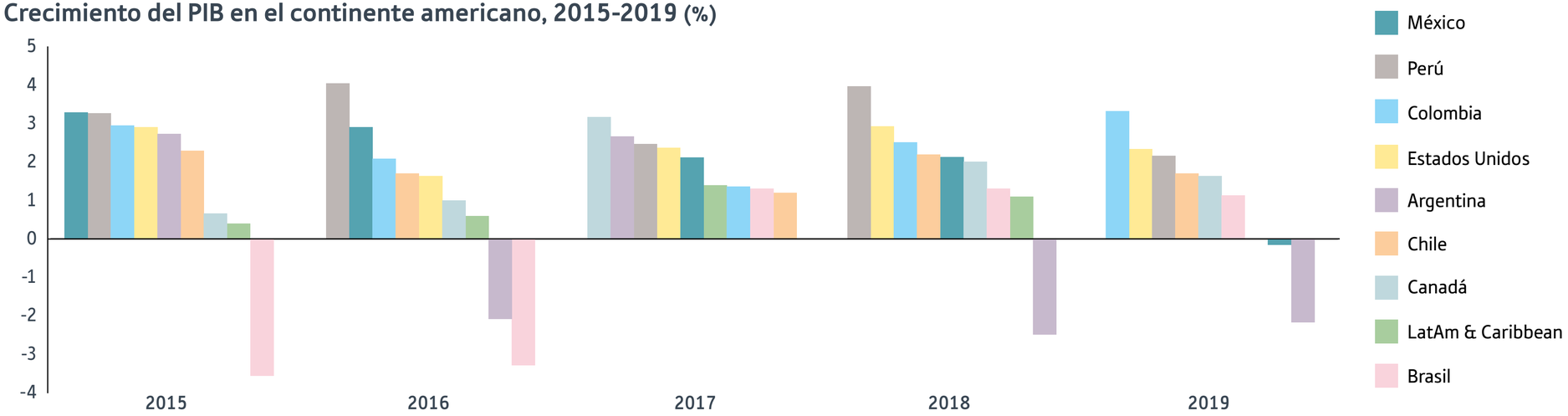
¿A qué grado la sofisticación de la manufactura requiere un replanteamiento de las estrategias de digitalización corporativas?

¿Qué segmentos de la economía mexicana deben ser priorizados ante un incremento de las amenazas cibernéticas?

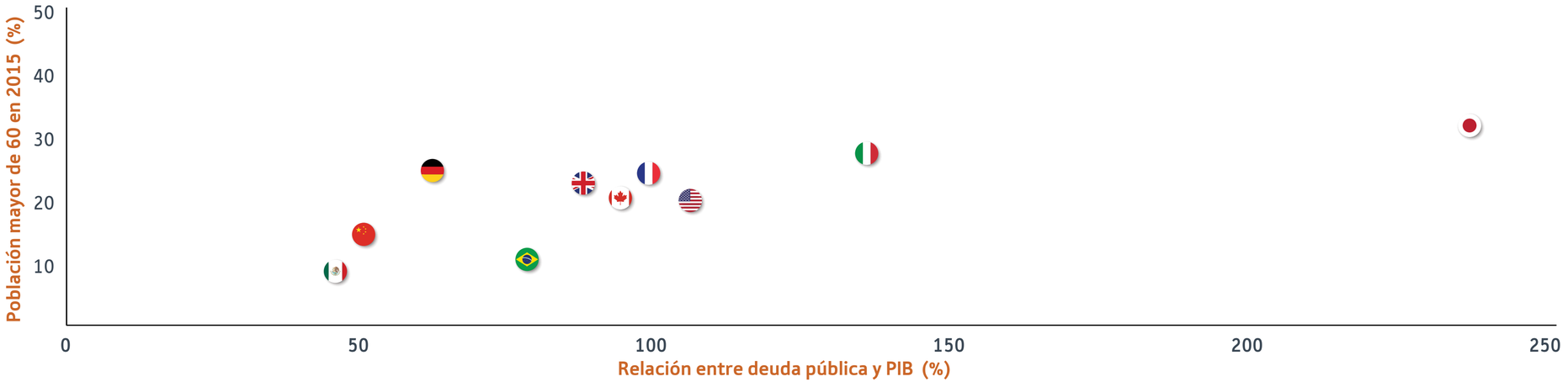
¿Cómo pueden las organizaciones desarrollar estrategias de ciberseguridad más amplias?

A pesar del estancamiento económico previo a la pandemia, México gozaba de una relación favorable entre deuda pública y PIB

Crecimiento del PIB en el continente americano, 2015-2019 (%)



Relación entre deuda-PIB y población de edad avanzada



Desaceleración pre-pandemia

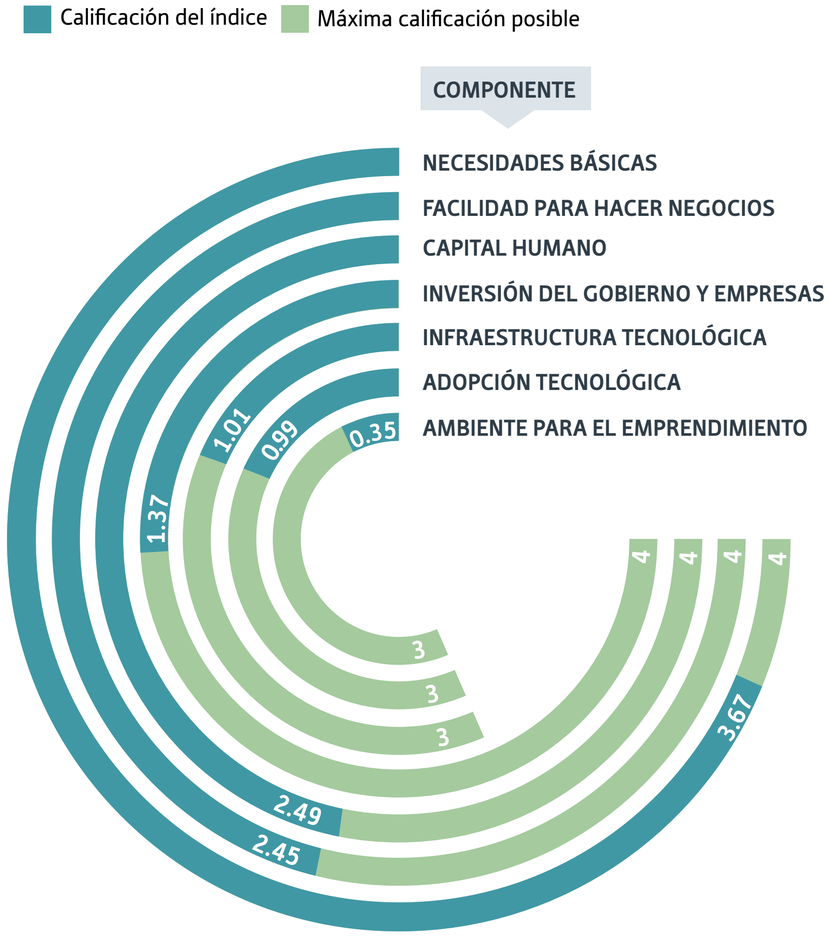
En 2019 la economía mexicana se encontraba estancada, después de experimentar un crecimiento estable en la década anterior. A pesar de que tener que hacerle frente a una pandemia con un crecimiento pequeño o nulo es un reto, el país tenía niveles bajos tanto de desempleo como de deuda pública, incluso si se compara con otras naciones del G20. Esto fue posible gracias al historial del gobierno en materia de prudencia fiscal y de crecimiento orientado al empleo.

El manejo fiscal prudente de la economía de manera sostenida y una baja proporción de población mayor a 60 años, impulsaron la resiliencia del país en términos fiscales y de salud pública.

Fuente: IMF; *UN/Trading Economics*

La preparación digital estaba al alza, impulsada por la penetración del internet, la inversión corporativa y por los consumidores digitales

La preparación digital de México pre-pandemia, 2019

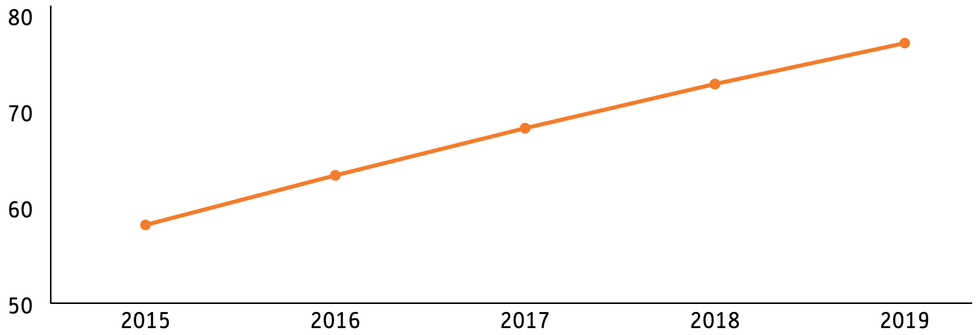


Calificación del índice de preparación digital pre-pandemia en Latinoamérica y el Caribe, 2019

PAÍS	CALIFICACIÓN DEL ÍNDICE (0-25)
Chile	14.86
Uruguay	13.88
Costa Rica	13.58
Argentina	13.06
Panamá	12.74
Trinidad y Tobago	12.59
Colombia	12.44
México	12.34
Brasil	12.31
Perú	11.93
Jamaica	11.55

PAÍS	CALIFICACIÓN DEL ÍNDICE (0-25)
Ecuador	11.29
Paraguay	11
República Dominicana	10.93
El Salvador	10.76
Guatemala	10.31
Honduras	10.14
Bolivia	10.12
Nicaragua	9.91
Venezuela	9.52
Haití	5.96

Usuarios de internet en México, 2015-19 (millones)



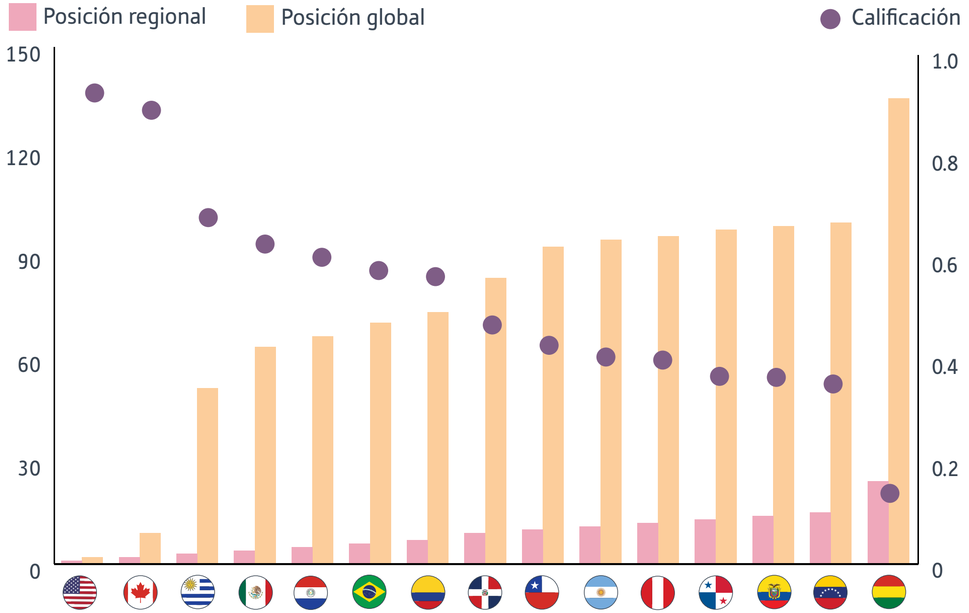
Demanda digital

En 2019 México se posicionó en el octavo lugar en preparación digital dentro de Latinoamérica. Aunque la digitalización ya estaba teniendo lugar' en las esferas empresariales y de gobierno, fue impulsada por un crecimiento sostenido de la adopción de internet del lado de la demanda. De acuerdo con el Interactive Advertising Bureau of Mexico, en 2019, 90% de los usuarios accedieron a internet a través de un teléfono inteligente, cuyo precio disminuyó en un 25% entre 2008 y 2016 en Latinoamérica. Una mejor conectividad y tecnologías más accesibles han llevado a las compañías a adelantar sus planes para la transformación digital para conseguir más clientes y retener a los actuales mediante experiencias de usuario mejoradas.

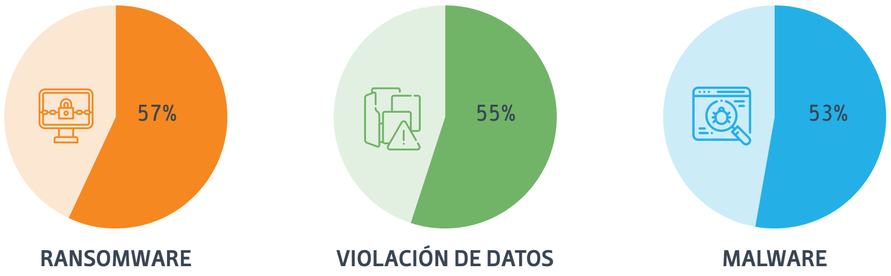
Fuente: *Statista*

La economía cada vez más digitalizada y globalizada ha enfrentado un incremento sostenido en riesgos cibernéticos públicos y privados

Índice global de ciberseguridad, 2018



Principales amenazas cibernéticas en Latinoamérica



Compañías que enfrentaron ciberataques en 2019 (%)

Riesgo elevado

México ha sido consistentemente posicionado como el país que más ciberataques ha sufrido en Latinoamérica y que ha puesto a la ciberseguridad como un aspecto clave en su resiliencia económica y social. El país se convirtió en un miembro del Foro de Respuesta a Incidentes y Seguridad (FIRST por sus siglas en inglés), el cual colabora con la comunidad internacional en ciberseguridad a través del Equipo de Respuesta de Emergencia Informática, creado en 2010. A pesar de estos esfuerzos, México ha visto un incremento en los ciberataques de alto perfil a entidades públicas y privadas. En 2018 el costo promedio de recuperación de una compañía tras sufrir un ciberataque era de 2.5 millones de pesos. Este número incrementó en un 38.4% por un total de 6.5 millones de pesos en 2019.

Fuente: *ITU; ESET Security Report 2020; ESET Security Report 2019*

ESTUDIO DE CASO: Schneider Electric busca cerrar la brecha digital entre las empresas y sus activos

Atendiendo las preocupaciones de ciberseguridad y de desempeño de las compañías en diversos sectores económicos, Schneider Electric, a lo largo de los años, ha desarrollado su oferta EcoStruxure, una plataforma habilitada para el internet de las cosas, plug and play, abierta e interoperable para edificios, centros de datos, infraestructuras e industrias. Mediante el uso de productos conectados, desde Edge Control a aplicaciones, y una amplia gama de servicios de analítica, la plataforma se apalanca de la movilidad, la medición, la nube y la ciberseguridad para entregar tecnologías rápidas y escalables a los clientes. Esto a su vez puede aumentar la eficiencia operacional, sustentabilidad y desempeño de los activos y la productividad de las personas, que se han vuelto elementos cada vez más importantes para las empresas que encaran costos más altos y exigencias en materia de seguridad.

Beneficios de la arquitectura EcoStruxure

- Seguridad
- Conectividad
- Confiabilidad
- Sustentabilidad
- Eficiencia

EcoStruxure para Edificios

- Soluciones para edificios inteligentes
- Maximiza la eficiencia del edificio
- Troncal IP digital
- Gestión de energía y control ambiental
- Poderosas herramientas de integración y control
- Analítica y servicios
- Confort y productividad de personas

EcoStruxure TI

- Planeación y diseño de centros de datos
- Modernización/actualización de centros de datos
- Incremento de la utilización de la infraestructura
- Visibilidad a lo largo de un ecosistema híbrido
- Información del dispositivo, alarmas inteligentes y monitoreo
- Facilidad de despliegue mediante un modelo de suscripción

EcoStruxure para Plantas y Máquinas

- Servicios IoT (Internet de las cosas) que permite manufactura inteligente
- Consciencia operacional en tiempo real
- Rastreo, monitoreo y arreglo de máquinas de forma remota
- Sistemas de automatización que catalizan objetivos de sustentabilidad
- Mejoras de productividad y rentabilidad
- Centralización del registro de datos y ayuda en la toma de decisiones

EcoStruxure Grid

- Desata el potencial de servicios públicos inteligentes
- Enfrenta la complejidad de la red
- Maximiza la eficiencia de la red
- Mitiga los cortes de energía
- Capacidades completas de ciberseguridad
- Transición a micro redes verdes

EcoStruxure Energía

- Capacidad mejorada de gestión de energía
- Eficiencia operacional y confiabilidad
- Seguridad eléctrica y reducción de riesgos
- Eficiencia energética y reducción de costos de operación
- Ciberseguridad reforzada

Schneider Electric en México

75+ años de operaciones

€25.2 mil millones ingresos globales en 2020

130,000+ empleados

2019 apertura de fábrica inteligente en Monterrey

Sede en **Francia**

Fuente: *Schneider Electric*

Resiliencia

El crecimiento económico de México disminuyó a finales de 2019 como resultado de la desaceleración global. Sin embargo, sus fundamentos económicos como la relación entre la deuda pública y el PIB se mantuvieron fuertes.

Antes de la pandemia, la preparación digital del país era similar a la de las economías más grandes de la región.

La preparación digital era más avanzada a nivel empresarial e individual en temas básicos, en materia de facilidad para hacer negocios y de capital humano. Los aspectos más débiles eran la adopción de la infraestructura tecnológica y el ambiente para emprender.

Respuesta

¿Cuál fue la respuesta en general del gobierno ante la pandemia?

¿Cómo evolucionó el comportamiento empresarial como resultado de los cambios en el ambiente operativo de los negocios?

¿De qué forma cambiaron las iniciativas digitales debido a la pandemia?

Recuperación

¿Qué papel jugará la digitalización en la recuperación económica de México?

¿De qué forma evolucionará la preponderancia de la ciberseguridad en los siguientes años?

¿Qué aspectos deben mejorar en temas de infraestructura en México para facilitar una recuperación económica impulsada digitalmente?

Reinvención

¿A qué grado la sofisticación de la manufactura requiere un replanteamiento de las estrategias de digitalización corporativas?

¿Qué segmentos de la economía mexicana deben ser priorizados ante un incremento de las amenazas cibernéticas?

¿Cómo pueden las organizaciones desarrollar estrategias de ciberseguridad más amplias?

Línea del tiempo del Covid-19 en México en 2020

30 DE ENERO
El gobierno implementa el Plan de Preparación y Respuesta, creado por el Comité Nacional para la Seguridad en Salud

10 DE MARZO
El banco central, Banco de México (Banxico), interviene para proteger el peso. La Comisión de Cambios incrementa el tamaño de las subastas de cambios extranjeros de $20 mil millones a $30 mil millones de dólares

14 DE MARZO
Se cancelan eventos deportivos y cívicos en las escuelas

20 MARZO – ABRIL
Se cierran las escuelas durante un mes hasta el 20 de abril, posteriormente esta fecha se extiende al 1 de junio y así de manera sucesiva

24 DE MARZO
El Presidente anuncia que México se encuentra en la fase 2 del plan de contingencia, efectivo hasta el 30 de abril. Las reuniones en público y eventos de más de 100 personas quedan prohibidas.

30 DE MARZO
Se declara una emergencia nacional de salud. Todas las actividades no esenciales quedan prohibidas, se prohíben las reuniones de más de 50 personas y se le pide a la población permanecer en casa a menos de que sea absolutamente necesario salir

12 DE ABRIL
El gobierno establece el Centro Nacional de Contingencias para combatir el Covid-19

13 DE ABRIL
Sonora se convierte en el primer estado en imponer toque de queda

16 DE ABRIL
Se anuncian restricciones de viaje en el país entre zonas de alto y bajo contagio

Fuente: *WHO; Gobierno de México; Banco de México*

Línea del tiempo del Covid-19 en México en 2020

21 DE ABRIL
El gobierno declara que México ha entrado en la fase 3 de su plan de contingencia en el cual se prohíben todas las reuniones en público y que pide a la población no abrazarse o saludar de mano

17 DE ABRIL
AMLO promete $2.5 mil millones para distribuirse en mayo para apoyar la economía

26 DE ABRIL
IDB Invest y el Consejo Mexicano de Negocios anuncian un acuerdo para facilitar el financiamiento a las cadenas de producción mexicanas y el apoyo a micro, pequeñas y medianas empresas

13 DE MAYO
La Secretaría de Economía anuncia un plan de 3 fases para reabrir la economía, comenzando el 18 de mayo

22 DE MAYO
GM anuncia que comenzará a abrir dos de sus cuatro plantas en la Ciudad de México

1 DE JUNIO
Los Cabos en Baja California Sur recibe a los primeros turistas extranjeros después de la cuarentena

15 DE SEPTIEMBRE
Banxico anuncia la extensión de sus medidas para proveer liquidez y promover un desempeño ordenado de los mercados financieros hasta febrero 2021

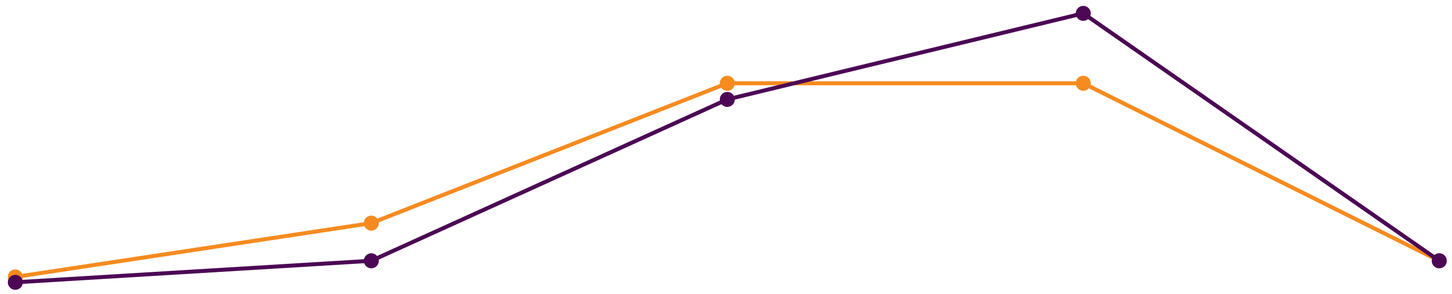
29 DE NOVIEMBRE
El presidente Andrés Manuel López Obrador (AMLO) anuncia la compra de 77.4 millones de dosis de la vacuna de AstraZeneca, 34.4 millones de dosis de Pfizer, 35 millones de Cansino y 34.4 millones a través de COVAX. Las vacunas serán universales y gratuitas

25 DE DICIEMBRE
México se convierte en el primer país de Latinoamérica en comenzar una campaña masiva de vacunación

Fuente: *WHO; Gobierno de México; Banco de México*

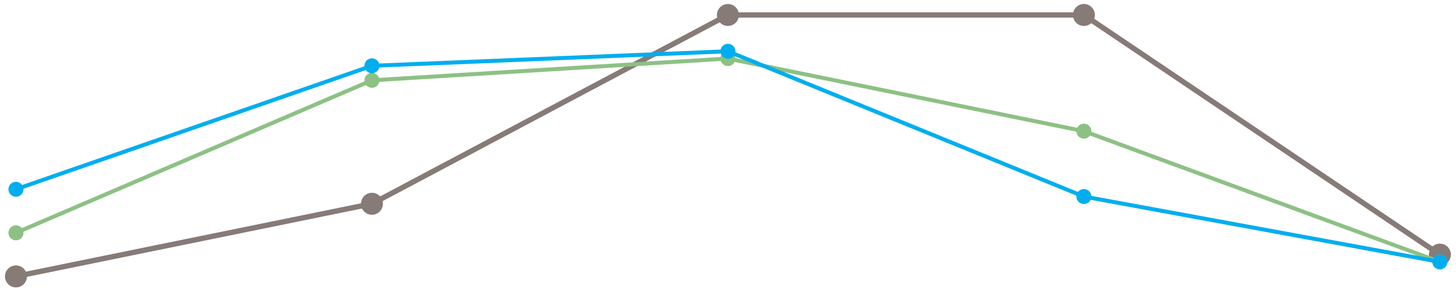
La pandemia ha forzado a las empresas a adaptarse a nuevos modelos de negocios y acelerar sus planes de transformación digital

Índice de Transformación Digital 2020



	REZAGADOS DIGITALES	SEGUIDORES DIGITALES	EVALUADORES DIGITALES	ADOPTADORES DIGITALES	LÍDERES DIGITALES
Mundo	3%	13%	39%	39%	6%
México	2%	6%	36%	52%	6%

Progreso histórico de la transformación digital en todo el mundo, 2016-20



	REZAGADOS DIGITALES	SEGUIDORES DIGITALES	EVALUADORES DIGITALES	ADOPTADORES DIGITALES	LÍDERES DIGITALES
2020	3%	13%	39%	39%	6%
2018	9%	30%	33%	23%	5%
2016	15%	32%	34%	14%	5%

Digitalización generalizada

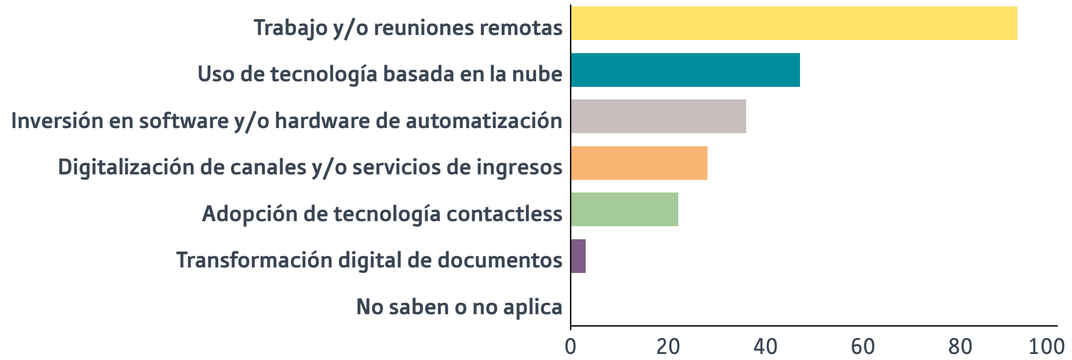
La pandemia de Covid-19 ha tenido un efecto radical en el ambiente económico de México, forzando a las compañías a adaptarse a restricciones impredecibles y nuevos modelos de negocio a través de iniciativas de transformación digital. Siendo la continuidad del negocio y la resiliencia la prioridad número uno, las organizaciones de diferentes tamaños y de diferentes industrias tuvieron que acelerar sus planes estratégicos de años a meses, catalizando la digitalización de las interacciones de cadena de valor de los clientes además de las operaciones corporativas internas. En el mundo, aproximadamente 8 de cada 10 negocios aceleraron la adopción de al menos una tecnología digital, de acuerdo con Dell Technologies.

Fuente: *Dell Technologies*

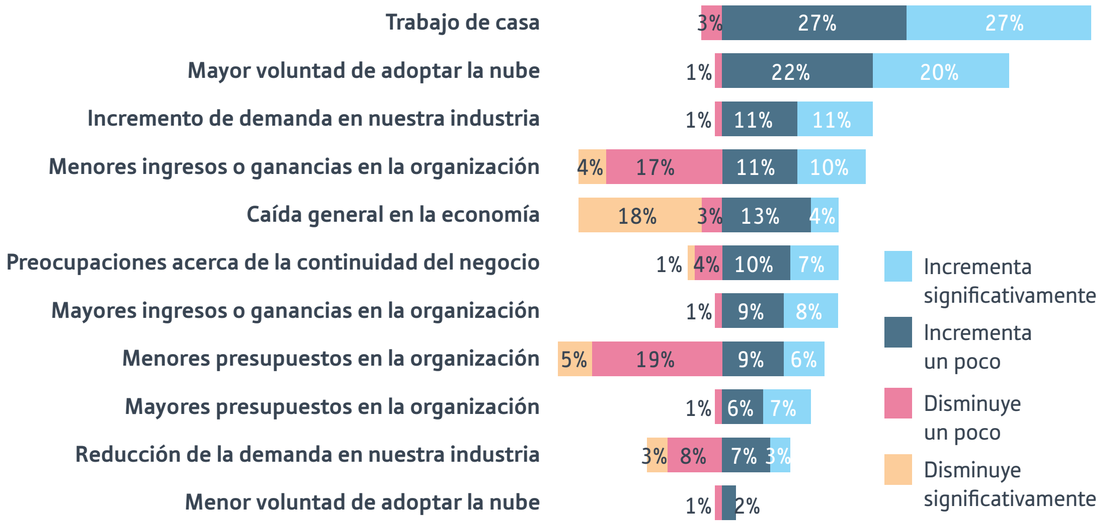
El comportamiento de los consumidores y las prioridades de las empresas han dado forma a las iniciativas digitales en diferentes industrias

OXFORD BUSINESS GROUP

Medidas de transformación digital en empresas mexicanas en 2020
(% de respondientes)



El impacto del Covid-19 en la transformación digital de las compañías a nivel global



Prácticas de transformación digital que se aceleraron más durante la pandemia

- Trabajo remoto
- Edge computing
- Experiencias digitales para clientes o empleados
- Gestión de datos
- Expansión del alcance digital de las empresas
- Servicios digitales bajo demanda

Principales barreras para la transformación digital

- Cultura digital incipiente
- Carencia de habilidades en los equipos de TI internos
- Preocupaciones respecto a la seguridad y privacidad
- Falta de presupuesto y recursos
- Falta de crecimiento económico ligado a la pandemia
- Incapacidad de extraer valor de los datos
- Falta de una estrategia digital coherente
- Legislación o cambios legislativos
- Falta de liderazgo TI

Prioridades de transformación digital en crecimiento

- Ciberseguridad
- Infraestructura 5G
- Software de privacidad
- Ambiente de múltiples nubes
- Inteligencia artificial
- Registros contables digitales
- Mezcla de realidad virtual y realidad aumentada

Enfoque digital

Las empresas mexicanas, las cuales habían sido más lentas en adoptar el uso de tecnologías digitales debido a la baja tasa de adopción de los consumidores, comparado con muchas empresas globales, tuvieron que fomentar su competitividad a través de la adopción acelerada de herramientas digitales durante la pandemia. De acuerdo con el estudio de EY de 2021: Barómetro de Confianza del Capital Global, 76% de las compañías mexicanas encuestadas dijeron que la pandemia incrementó su enfoque estratégico e inversión en la transformación digital; 89% de las empresas reconocieron que estaban llevando a cabo un programa de transformación de negocio y tecnológico significativo. Aproximadamente 32% piensan que su agenda de transformación digital corporativa se desempeñó mejor en la pandemia, comparada con sus competidores.

Schneider Electric

Fuente: *OBG Covid-19 CEO Survey 2020; Flexera*

ESTUDIO DE CASO: Schneider Electric demuestra su preparación para afrontar nuevas formas de trabajo

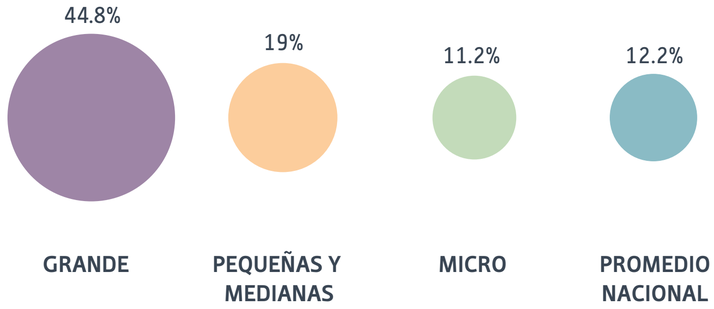
Cambios en los hábitos de trabajo

Mientras que millones de empleados trabajaron de forma remota, la pandemia provocó un incremento en el enfoque de productividad y en la gestión de redes por software (Software-defined networking, SDN) para maximizar el desempeño fuera de la oficina. En México, alrededor de 12% de las empresas tenían una infraestructura de oficina implementada en casa hacia finales del 2020, las grandes corporaciones contaban con una cantidad desproporcionadamente mayor de trabajadores remotos. A pesar de que esto tuvo el beneficio de proteger a los empleados de una infección, la respuesta digital también ha expuesto las vulnerabilidades en ciberseguridad, dado que los agresores buscan explotar los vacíos generados por el uso de dispositivos y redes no seguras por parte de los empleados. A medida que los modelos de trabajo completamente remotos o híbridos se normalicen posterior al Covid-19, las compañías tendrán que priorizar sus capacidades en ciberseguridad.

La Política de Trabajo Flexible de Schneider Electric

- Da prioridad a una cultura de trabajo inteligente basada en objetivos y alto desempeño, que de forma simultánea acoge una mejor integración del trabajo y vida y promueve el bienestar de los empleados
- Aplica a todos los empleados de Schneider Electric en México y Centroamérica, los departamentos de Gestión de Energía y Cadena de Suministro Global, con excepción de los empleados sindicalizados. Cumple con la legislación laboral de la región
- Es responsabilidad del empleado el entender la política y discutir sus requerimientos con su gerente directo para determinar su elegibilidad, de acuerdo con su cargo y las necesidades específicas del negocio o los departamentos. La participación no es una opción garantizada y debe ser compatible con los modelos de trabajo flexible.
- El empleado debe tener conectividad de internet en casa, utilizar Microsoft Teams, Avaya u otras herramientas aprobadas por la compañía de acuerdo con el cargo del empleado, y debe cumplir con las regulaciones de seguridad para instalaciones eléctricas y tener un espacio dedicado en casa reservado específicamente para el trabajo.

Implementación del trabajo remoto en las compañías mexicanas



Tipos de asistencia de la compañía

- El pago de Asistencia para Configuración ofrece a los empleados una opción rentable para acondicionar su espacio de trabajo (p. ej. compra de escritorio, silla, etc. mediante un pago único de 2500 pesos mexicanos, el cual se entrega como asistencia para quienes trabajan 3 días en casa bajo un modelo fijo o híbrido. Aplica únicamente para los marcos A y B y el marco fijo D, sin excepciones
- El Pago Mensual de Trabajo Flexible es un pago recurrente para que los empleados compensen los gastos generados por los modelos de trabajo flexible (p. ej. electricidad, internet, etc.) mediante un pago mensual de 450 pesos mexicanos netos, entregado para los empleados que trabajan 3 días bajo un modelo fijo o híbrido. Aplica para los marcos híbridos A y B y el marco fijo D únicamente, sin excepción.
- Ambos pagos de asistencia son aplicables solo para los grados nueve e inferiores, se distribuye de forma electrónica mediante una tarjeta electrónica una vez que termine el proceso de validación del modelo trabajo.

Tipos de Modelo de Trabajo Flexible

Modelo de trabajo híbrido: Trabajo desde casa y oficina bajo diferentes escenarios

Marco A
Cuatro días de trabajo remoto y un día flexible de trabajo en la oficina por semana. Estos empleados no tienen una estación de trabajo fija en la oficina.

Marco B
Tres días de trabajo remoto y dos días flexibles de trabajo en la oficina por semana. Estos empleados no tienen una estación de trabajo fija en la oficina.

Marco C
Dos días de trabajo remoto y tres días flexibles de trabajo en la oficina por semana. Estos empleados no tienen una estación de trabajo fija en la oficina.

Modelo de trabajo fijo: Trabajo permanente desde algún sitio, bajo diferentes escenarios

Marco D
Trabajo remoto permanente desde casa.
Estos empleados no tienen una estación de trabajo fija en la oficina.

Marco E
Trabajo permanente desde oficina o planta. Esto involucra cargos que por su naturaleza requieran que los empleados se encuentren presentes físicamente cada día laboral en la oficina o en la planta. Dependiendo del sitio, estos empleados pueden o no tener una estación de trabajo fija.

Marco F
Trabajo remoto desde cualquier lugar, tales como oficinas corporativas, plantas, oficinas de clientes, etc. Estos empleados no tienen una estación de trabajo fija en la oficina. Este marco aplica para funciones de servicio de ventas y campo.

Fuente: *INEGI*

Resiliencia

El crecimiento económico de México disminuyó a finales de 2019 como resultado de la desaceleración global. Sin embargo, sus fundamentos económicos como la relación entre la deuda pública y el PIB se mantuvieron fuertes.

Antes de la pandemia, la preparación digital del país era similar a la de las economías más grandes de la región.

La preparación digital era más avanzada a nivel empresarial e individual en temas básicos, en materia de facilidad para hacer negocios y de capital humano. Los aspectos más débiles eran la adopción de la infraestructura tecnológica y el ambiente para emprender.

Respuesta

A pesar que el estímulo fiscal federal tuvo un alcance limitado, el banco central actuó de forma rápida, y el sistema político descentralizado permitió respuestas de salud pública y fiscales de manera local.

Para salvaguardar la resiliencia y agilidad de los negocios, las compañías aceleraron sus agendas de desarrollo estratégico y adopción digital.

Alineado con los cambios en las prácticas de negocios y las expectativas de los consumidores, las compañías mexicanas han incorporado de forma inmensa la digitalización a sus estrategias corporativas en adelante.

Recuperación

¿Qué papel jugará la digitalización en la recuperación económica de México?

¿De qué forma evolucionará la preponderancia de la ciberseguridad en los siguientes años?

¿Qué aspectos deben mejorar en temas de infraestructura en México para facilitar una recuperación económica impulsada digitalmente?

Reinvención

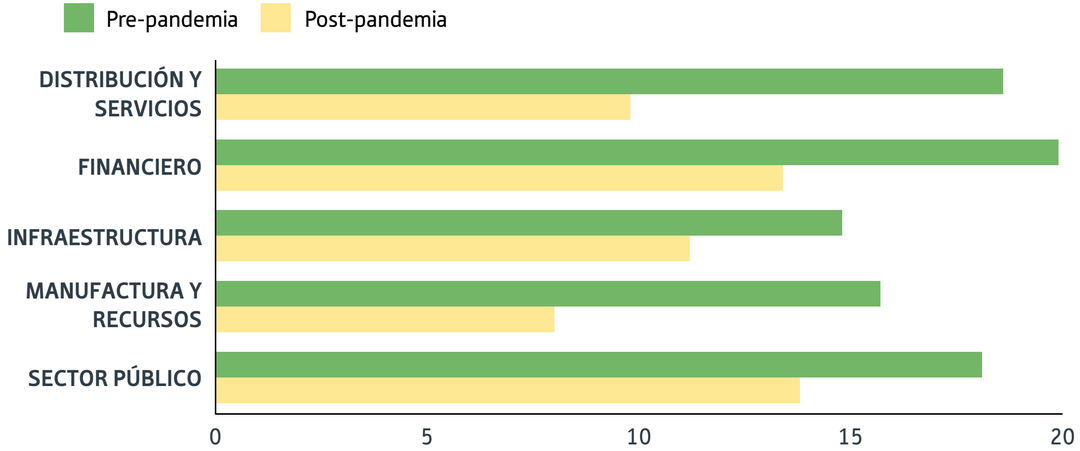
¿A qué grado la sofisticación de la manufactura requiere un replanteamiento de las estrategias de digitalización corporativas?

¿Qué segmentos de la economía mexicana deben ser priorizados ante un incremento de las amenazas cibernéticas?

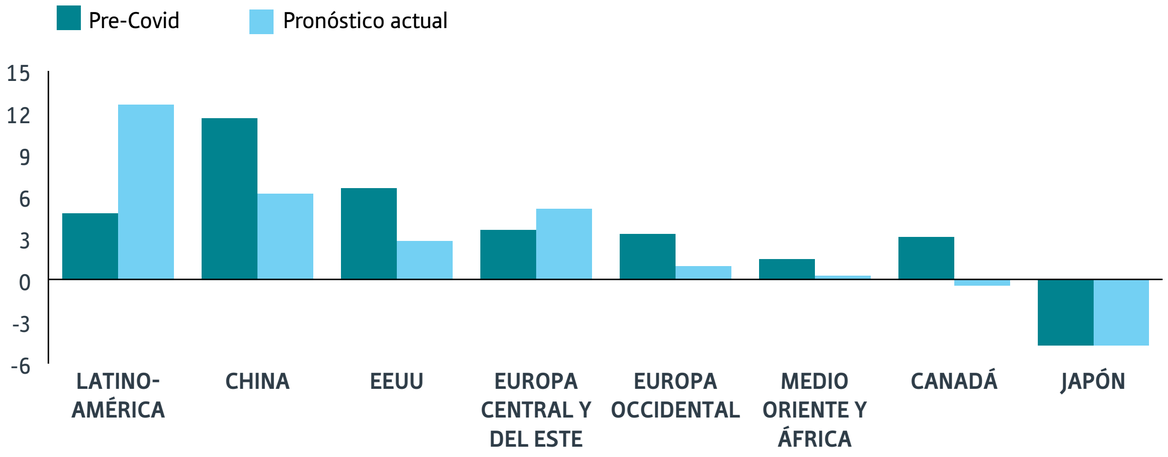
¿Cómo pueden las organizaciones desarrollar estrategias de ciberseguridad más amplias?

A pesar de que se espera que el crecimiento en gasto en TI disminuya en muchos mercados, en Latinoamérica se proyecta una aceleración en los siguientes años

Crecimiento en gasto en transformación digital global (%)



Gasto en TI por región, 2020- pronóstico 2024 (% anual de cambio)



Crecimiento de TI en Latinoamérica, 2020-21

(Hardware, software y servicios TI)

	2020 ($ corriente)	2020 ($ constante)	2021 ($ constante)
LatAm	-11.3%	5.5%	7.7%
México	-13.3%	-1.7%	10.0%
Perú	-15.3%	-12.2%	9.0%
Colombia	-6.7%	5.4%	3.0%
Brasil	-12.0%	12.2%	5.0%
Chile	-6.9%	6.3%	5.5%
Argentina	-11.4%	24.1%	10.4%

Inversión digital

El gasto global en tecnologías y servicios digitales previó un crecimiento de 10.4% en 2020, equivalente a unos $1.3 billones de dólares. Como resultado del comportamiento del consumidor, se ha previsto que la inversión en la transformación digital alcance una tasa de crecimiento anual compuesto de 15.5% global entre 2020 y 2023, alcanzando un gasto total en el periodo de $6.8 billones, de acuerdo con el International Data Corporation (IDC). Esta inversión contrasta radicalmente con la inversión no digital, la cual proyecta una contracción de 1.4% en el mismo lapso. El IDC pronostica que esta tendencia llevará a que aproximadamente el 65% del PIB global sea proveniente de fuentes digitales para el 2022.

Fuente: *IDC*

OXFORD BUSINESS GROUP

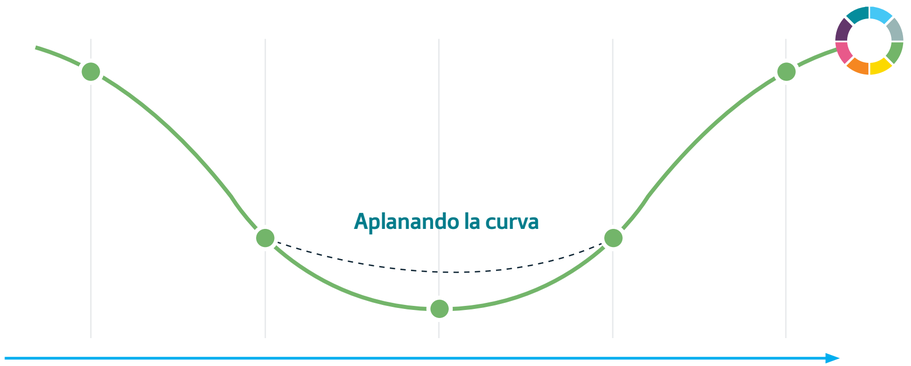
El gasto de las empresas a largo plazo busca aprovechar las inversiones digitales e incrementar la competitividad

Predicciones Digitales Globales de IDC

- El aumento digital permanecerá competitivo. Para el 2023, 75% de las organizaciones tendrán planes de transformación digital amplios, 27 % más que en 2020
- Una gestión y liderazgo digital más madura: para el 2023, 60% de los de los líderes en las organizaciones G2000 habrán cambiado de procesos a resultados, creando modelos operativos más ágiles e innovadores
- El surgimiento y expansión de plataformas digitales y ecosistemas extendidos: para el 2025, 75% de los líderes de empresas aprovecharán las capacidades digitales para fortalecer las cadenas de valor en los nuevos mercados, industrias y ecosistemas
- La digitalización en primer lugar: para el 2021, 60% de las empresas invertirán para digitalizar la experiencia y capacidades de los empleados
- Reinvención del modelo de negocio: en 2021 al menos 30% de las organizaciones acelerarán la innovación para apoyar la reinvención de los modelos operativos y las estructuras de negocio para blindar a futuro a las empresas
- Prioridades de sustentabilidad: en 2022 la mayoría de las compañías generará mayor valor al combinar capacidades impulsadas digitalmente y proyectos sustentables
- Culturas nativamente digitales: para el 2025, 50% de las empresas implementarán una cultura organizacional optimizada basada en prioridades centradas en el cliente e impulsadas por datos
- Plataformas de innovación de negocios: para el 2023, 60% de las compañías G2000 construirán sus propias plataformas de innovación de negocio para apoyar el crecimiento y la innovación

Marco de 5 pasos desde la crisis hacia la recuperación

ENFOQUE EN NEGOCIOS	Continuidad de negocio	Optimización de costo	Resiliencia del negocio	Inversión dirigida	Iniciativa a futuro
SITUACIÓN ECONÓMICA	**Crisis del Covid-19**	**Desaceleración económica**	**Recesión**	**Repunte del crecimiento**	**La nueva normalidad**



93% México 87% Mundo	Proporción de empresas que coinciden en que una mezcla híbrida de centros de datos/nube público- privados es la arquitectura ideal para su organización	
60% México 50% Mundo	Proporción de empresas que ya han implementado o están en proceso de implementar una infraestructura de hiperconvergencia	
50% México 37% Mundo	Proporción de compañías que vieron un incremento en el uso de la nube privada	

Cambiando la dinámica del trabajo

Basado en las lecciones aprendidas durante la pandemia, el IDC estima que el 80% de las empresas globales habrán puesto un mecanismo para hacer la transición hacia una infraestructura y aplicaciones centradas en la nube para finales del 2021. La transición hacia una fuerza de trabajo híbrida acelerará el 80% de la adopción del edge computing en la mayoría de las industrias para el 2023.

El Índice de Nube Empresarial de Nutanix publicado en abril del 2020, demuestra que en muchos aspectos México estaba más adelantado en el cómputo de nube que el promedio global. Para el índice se encuestaron compañías en Asia Pacífico, Europa, África, y el Medio Oriente.

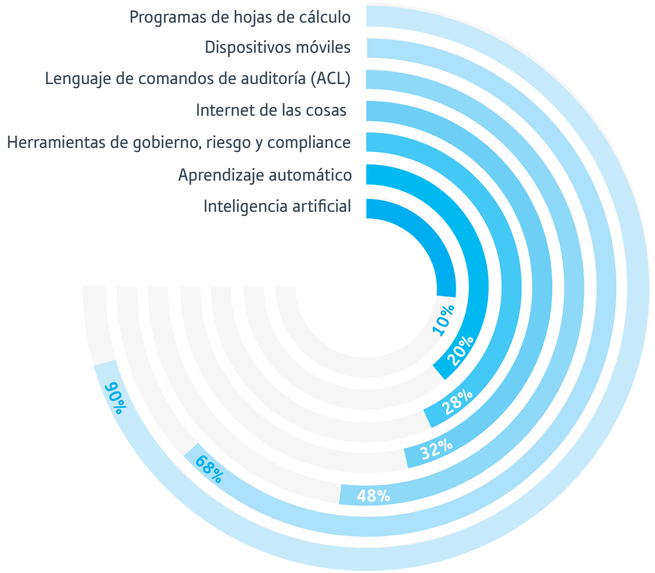
Schneider Electric

Fuente: *IDC; Nutanix*

OXFORD BUSINESS GROUP

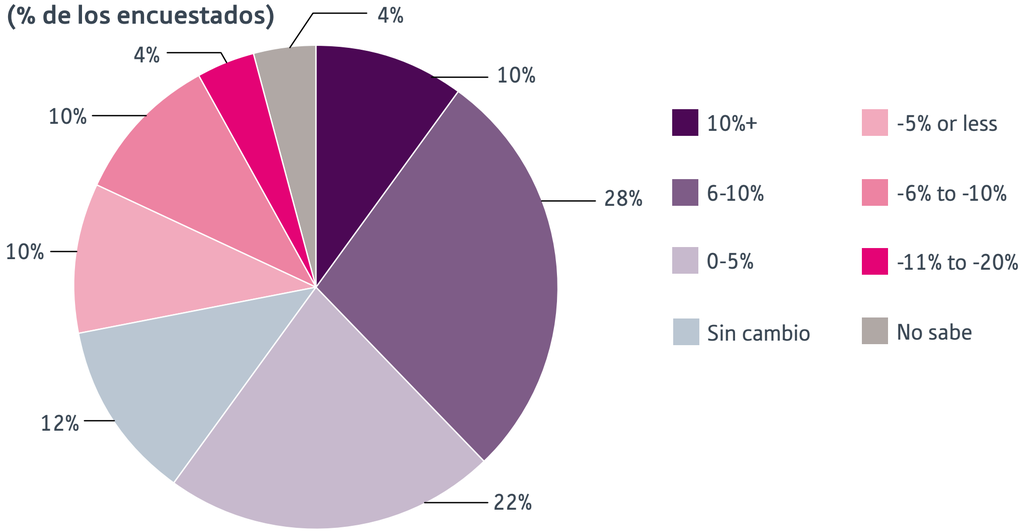
La ciberseguridad ha emergido como la principal prioridad para las compañías que buscan manejar los riegos financieros y de reputación

Tecnologías de gestión de riesgos en México

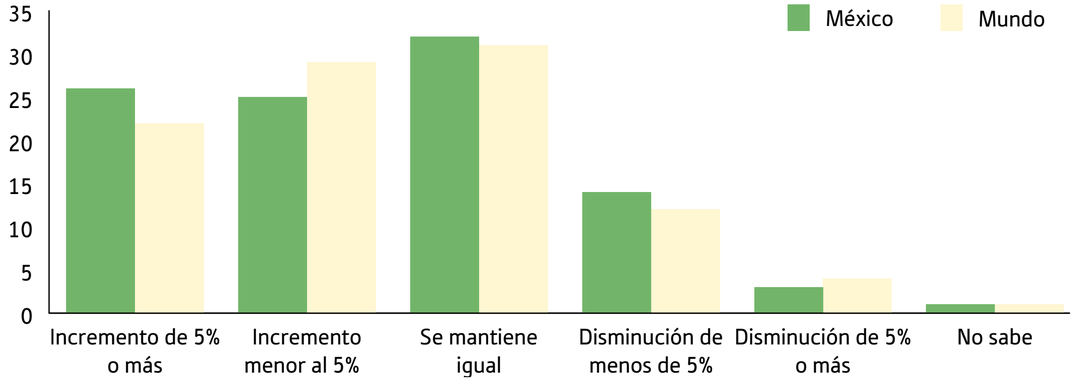


% de compañías encuestadas

Cambios en los presupuestos de ciberseguridad en compañías mexicanas, 2021 (% de los encuestados)



Cambios esperados de la fuerza laboral en ciberseguridad, agosto 2021-2022 (% de los encuestados)



En enfoque: Amenazas de ciberseguridad relacionadas a usuarios en México

Iceberg Digital, un estudio realizado por la agencia de ciberseguridad Kaspersky en 2020 mostró los puntos naturales de entrada para los cibercriminales revelando que:

- 35% de los usuarios de internet en México permitieron que los navegadores guardaran sus contraseñas para tiendas online, 13% para servicios de banco, 55% para redes sociales y 54% para cuentas de correo
- 6% de los usuarios en México nunca ha cambiado su contraseña, mientras que el 14% no recuerda la última vez que lo cambió

Amenazas variadas

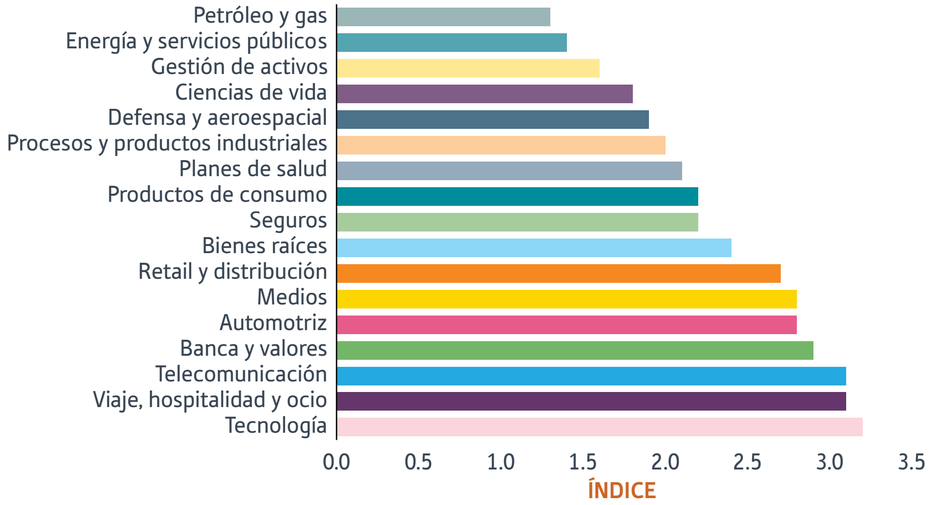
De acuerdo a un estudio de ESET, México experimentó el tercer número más alto de ciberataques en Latinoamérica en 2020, representando el 16.94% del total de ataques en la región. Sin embargo, existen diversas barreras para que las empresas mexicanas desplieguen sus programas de ciberseguridad; de acuerdo a una encuesta de PwC: falta de conocimiento (46%), falta de presupuesto (25%) y escasez de talento (12%). Las vulnerabilidades cibernéticas se han multiplicado a la vez que las amenazas se han hecho más sofisticadas y el uso de dispositivos y redes inseguras por parte de empleados que trabajan remotamente se han vuelto más comunes. En un contexto de trabajo remoto, los cibercriminales están cada vez más atacando a los empleados para obtener el control a través del acceso remoto a redes corporativas.

Fuente: *PwC*

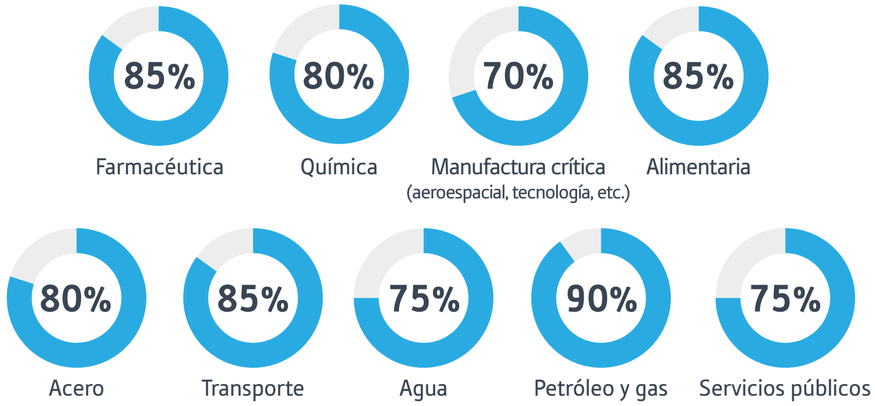
OXFORD BUSINESS GROUP

Las amenazas y vulnerabilidades emergentes de infraestructura crítica han llevado a mejores niveles de seguridad y compliance

Madurez digital promedio por sector, 2019



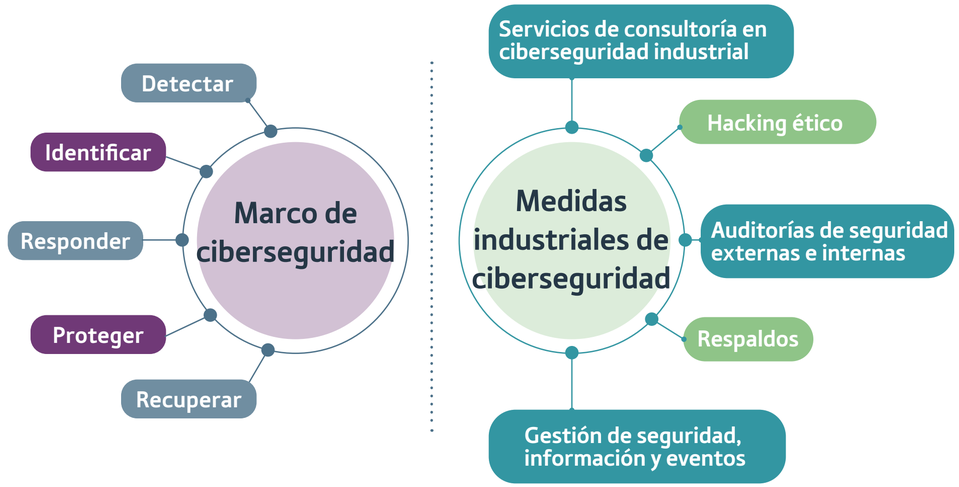
Nivel de vulnerabilidad en ciberseguridad industrial en México



Soluciones existentes utilizadas en México

- Para mitigar los ciberataques, las empresas del sector industrial han impulsado sus esfuerzos en ciberseguridad, desplegando los firewalls más actualizados y desarrollando estrategias de defensa más proactivas que incorporan la detección, el monitoreo y la evaluación

- Las plataformas de nube distribuidas están jugando un papel crítico dado que permiten a las compañías de cualquier tamaño crear marcos en los cuales los sistemas de control se distribuyen a lo largo de muchos servidores con medidas de seguridad independientes, previniendo que las filtraciones de seguridad tomen el control de todo en sistema y comprometan la infraestructura crítica. De acuerdo a la consultora BDO, las empresas de petróleo y gas invertirán más de $20 mil millones en seguridad para el 2023.



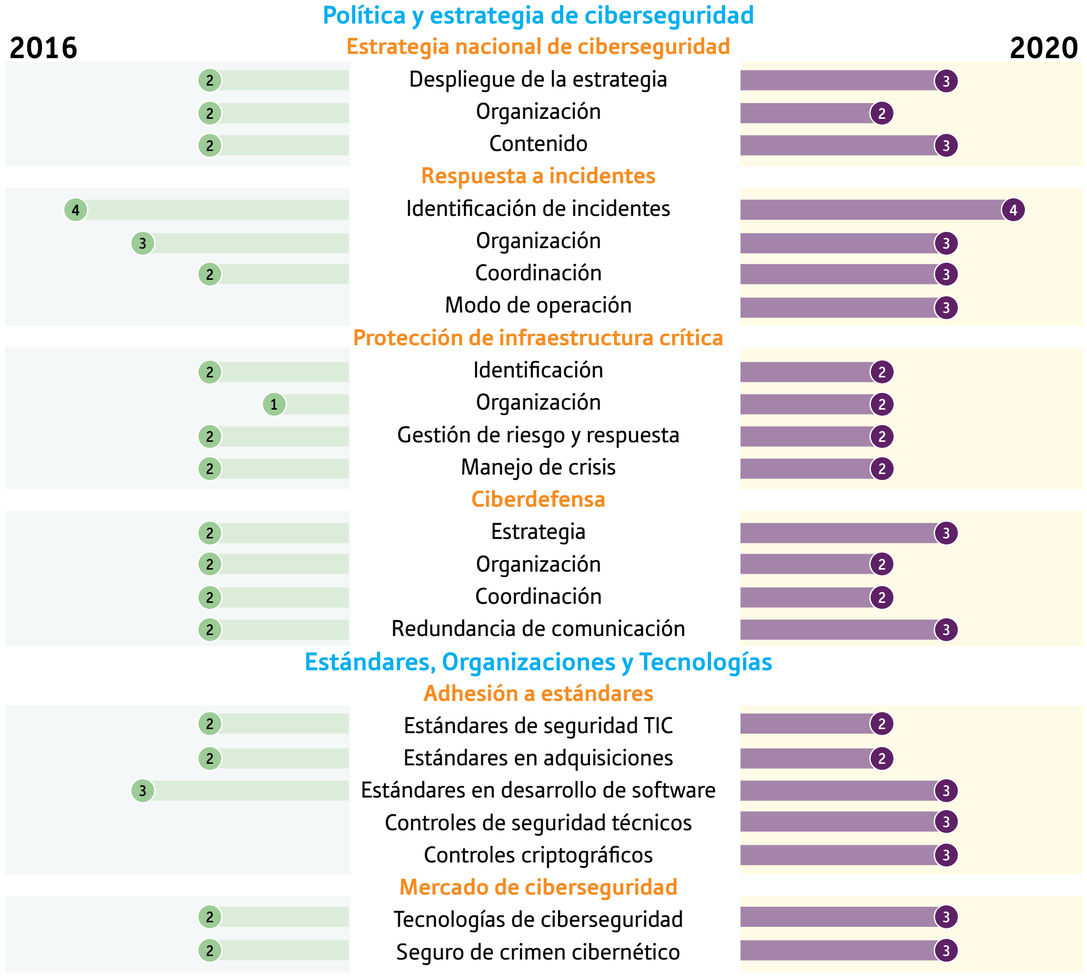
Un riesgo existencial creciente

Motivados por intereses políticos o económicos, los riesgos cibernéticos se han vuelto más frecuentes, mientras que el número de organizaciones críticas o esenciales también ha crecido. En 2019 un ciberataque en Pemex afectó alrededor de 5% de las computadoras personales de la compañía. Los atacantes pidieron $5 millones de rescate a la compañía petrolera. Los ataques pueden tomar diferentes formas incluyendo ransomware, y phishing, llevando a negación de servicio y robo. Esto puede generar una serie de resultados costosos como la pérdida de control de datos confidenciales o propietarios, impactos negativos en la operación, daño a la reputación con grupos involucrados, investigaciones de cuerpos policiales y daños físicos a las instalaciones.

Fuente: *Deloitte; Centro de Ciberseguridad Industrial*

Nuevo enfoque en generar conciencia sobre ciberseguridad y la mejora de estándares de manejo de riesgo

Nivel de madurez por área de política, 2016 vs 2020 (escala 0 a 5)



Datos importantes

Estrategia Nacional de Ciberseguridad de México

- Lanzada en 2017 en colaboración con la Organización de Estados Americanos
- Objetivo principal: reconocer el papel de las TIC como un factor político, social y económico para el desarrollo; identificar los riesgos asociados con el uso de tecnologías y desarrollar una cultura de ciberseguridad
- Alineada con la campaña de prevención nacional promovida por la Policía Federal, la estrategia busca generar conciencia acerca del uso responsable de las nuevas tecnologías para reducir los crímenes cibernéticos
- El Centro Nacional de Respuesta a Incidentes Cibernéticos se estableció para prevenir y mitigar ciberataques

Sinergias público-privadas

- Con la rápida digitalización y el nuevo Tratado México Estados Unidos y Canadá (T-MEC), es crítico un marco regulatorio fuerte de ciberseguridad y un incremento en la colaboración público-privada
- El T-MEC subraya las capacidades nacionales en ciberseguridad y la cooperación intergubernamental centrada en la protección de la infraestructura crítica y métodos de ciberseguridad basados en riesgo
- El sector privado y los inversionistas internacionales han promovido la formación de una Agencia Nacional de Ciberseguridad y una colaboración más estrecha para intercambiar buenas prácticas entre entidades relevantes

Dinámicas cambiantes

De acuerdo con un estudio del Banco Interamericano de Desarrollo, México ha experimentado una mejoría gradual en su nivel de madurez en la mayoría de las métricas de ciberseguridad entre 2016 a 2020, particularmente en aquellas relacionadas con la consciencia en ciberseguridad, educación, entrenamiento y habilidades. Un estudio de la Guardia Nacional de México mostró que en el periodo entre diciembre 2019 y febrero 2020 hubo una reducción del 12% en la actividad maliciosa de internet, esto se revirtió durante la pandemia, cuando los ciberataques se incrementaron en 14% comenzando en marzo. Esta tendencia ha hecho que se vuelva prioritario para el gobierno mejorar los estándares en ciberseguridad y los controles técnicos, así como la promoción del desarrollo de un mercado de ciberseguridad más robusto a nivel nacional.

Fuente: *Inter-American Development Bank*

Resiliencia

El crecimiento económico de México disminuyó a finales de 2019 como resultado de la desaceleración global. Sin embargo, sus fundamentos económicos como la relación entre la deuda pública y el PIB se mantuvieron fuertes.

Antes de la pandemia, la preparación digital del país era similar a la de las economías más grandes de la región.

La preparación digital era más avanzada a nivel empresarial e individual en temas básicos, en materia de facilidad para hacer negocios y de capital humano. Los aspectos más débiles eran la adopción de la infraestructura tecnológica y el ambiente para emprender.

Respuesta

A pesar que el estímulo fiscal federal tuvo un alcance limitado, el banco central actuó de forma rápida, y el sistema político descentralizado permitió respuestas de salud pública y fiscales de manera local.

Para salvaguardar la resiliencia y agilidad de los negocios, las compañías aceleraron sus agendas de desarrollo estratégico y adopción digital.

Alineado con los cambios en las prácticas de negocios y las expectativas de los consumidores, las compañías mexicanas han incorporado de forma inmensa la digitalización a sus estrategias corporativas en adelante.

Recuperación

Se espera que el gasto en digitalización incremente sustancialmente en Latinoamérica en comparación con otras regiones, con el sector de TI de México proyectado para un crecimiento de 10% en 2021.

La digitalización en México ha generado indirectamente una mayor conciencia acerca de la necesidad de invertir en ciberseguridad.

Si bien existen soluciones de ciberseguridad en México, las compañías están apenas poniéndose al día, especialmente en sectores críticos de la economía como del petróleo, el gas, la energía y los servicios públicos

Reinvención

¿A qué grado la sofisticación de la manufactura requiere un replanteamiento de las estrategias de digitalización corporativas?

¿Qué segmentos de la economía mexicana deben ser priorizados ante un incremento de las amenazas cibernéticas?

¿Cómo pueden las organizaciones desarrollar estrategias de ciberseguridad más amplias?

OXFORD BUSINESS GROUP

ESTUDIO DE CASO: Schneider Electric alinea su portafolio de ciberseguridad para enfrentar las amenazas actuales y a futuro

A través de una combinación de políticas, metodologías y profesionales calificados y certificados, Schneider Electric se ha posicionado como un aliado en ciberseguridad para las empresas en todas las industrias. Cumpliendo con los estándares IEC62443, la compañía ha desarrollado una estrategia de varias capas y múltiples tecnologías para salvaguardar los sistemas críticos mediante su evaluación, gestión y monitoreo de acuerdo con la Metodología de Schneider Electric de Ciclo de Vida del Portafolio.

Metodología de Schneider Electric de Ciclo de Vida del Portafolio

Evaluar

Evaluar y revisar sistemas para detectar brechas y riesgos y revelar malas prácticas en seguridad; medir las competencias del equipo de seguridad y proveer servicios de respuesta en emergencias

- Política y procedimiento
- Inventario de activos
- Análisis de brechas (GAP análisis)
- Riesgo y amenaza
- Compliance

Diseño

Diseño e incorporación de arquitectura de sistemas en acuerdo con los estándares de la industria más actuales

- Defensa a profundidad
- Arquitectura segura
- Gestión de activos
- Política y procedimiento
- Nivel de garantía de seguridad

Implementar

Diseño, desarrollo y mantenimiento de infraestructura crítica mediante una plataforma de seguridad de "defensa a profundidad" que ofrece autenticación centralizada, autorización y auditoría de sistema, protección contra malware, control de dispositivo y whitelisting; respaldos programados y encriptación de archivos y carpetas además de monitoreo de desempeño de redes y sistemas

- Política y procedimiento
- Hardware y software
- Endurecimiento de sistema
- Integración de soluciones
- Transferencia de conocimiento

Monitorear

Monitorear y detectar ataques y aplicar soluciones para asegurar un funcionamiento fácil de los dispositivos y del sistema como un todo

- Seguridad de firewall
- Gestión de dispositivos
- Gestión de amenazas unificado
- Sistema de detección e intrusión a la red
- Gestión de información de seguridad y eventos

Mantener

Revisar y actualizar la protección de ciberseguridad y asegurar que los sistemas y habilidades estén actualizados y probados regularmente para maximizar la seguridad

- Actualizaciones de sistema
- Parches de seguridad
- Consciencia y entrenamiento
- Respuesta a incidentes
- Prueba de penetración

Entrenar

Dar programas de entrenamientos básicos a avanzados a la medida específica de los equipos de seguridad. Educar a los equipos acerca de prácticas de seguridad e introducir una cultura de seguridad que lleva a una rápida respuesta hacia las amenazas y la continuidad de negocio.

Consciencia de seguridad → Ingeniero en seguridad → Administrador de seguridad → Experto avanzado

Cada 14 segundos ocurre un ataque de ransomware en el mundo

En menos de 5 minutos un dispositivo promedio de internet de las cosas puede ser atacado después de entrar en línea

Fuente: *Schneider Electric*

ESTUDIO DE CASO: El incremento en las vulnerabilidades impulsan la demanda de servicios completos e integrales de seguridad

El incremento en amenazas generan demanda para soluciones de protección en ciberseguridad más estricta en todos los negocios y tipos de industrias. Dado que cualquier estrategia de ciberseguridad es sólo tan fuerte como el eslabón más débil, es crítico identificar y mitigar riesgos al aplicar estándares y buenas prácticas a lo largo de la línea de defensa, que incorpora personas, procesos y tecnología.

Personas: Una fuerte protección cibernética requiere una fuerza de trabajo educada y consciente, dado que las personas son la primera y última línea de defensa para la compañía. Por lo tanto, es crucial crear y comunicar una cultura de seguridad a lo largo de la compañía, apoyada por un entrenamiento continuo.

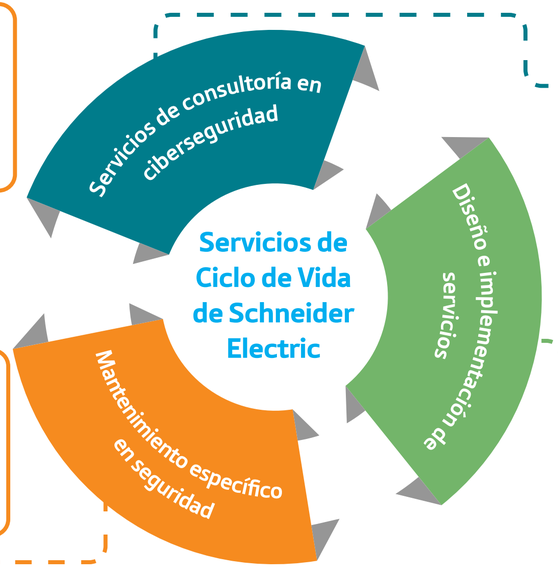
Procesos: Para identificar y eliminar riesgos cibernéticos, las compañías deben establecer y adherirse a buenos procesos, prácticas y políticas. Estos deben comenzar con evaluaciones periódicas y consistentes de riesgo y amenazas y análisis de brechas.

Tecnología: La defensa cibernética es tan fuerte como la tecnología desplegada para gestionar y controlar las operaciones. Las compañías deben proteger lo que desarrollan y despliegan, además de asegurar que la tecnología de los proveedores de la cadena de suministro es segura.

Beneficios
- Disponibilidad 24/7 de servicios de seguridad gestionados
- Rápida respuesta a incidentes y pruebas de penetración
- Disminución en esfuerzo y riesgo para aplicar parches y actualizaciones de antivirus
- Acceso seguro y automatizado a parches de sistema operativo y actualizaciones de antivirus probadas y calificadas

Soluciones
- Arquitectura de seguridad y desarrollo de políticas
- Modernización e implementación de seguridad
- Programa de mantenimiento priorizando al cliente

Entrenamiento en ciberseguridad
- Dar empoderamiento al personal para llevar a cabo operaciones seguras en la planta y procesos
- Impulsa la confidencialidad, integridad y disponibilidad de equipo
- Reduce la probabilidad de incidentes en ciberseguridad resultado del error humano
- Entrenamiento disponible, con módulos enfocados en tecnología



Beneficios
- Un plan completo de seguridad y ciberseguridad hecho conforme al perfil de la compañía
- Protección de ciberseguridad sin tener un impacto negativo en las operaciones del día a día
- Acceso a expertos que saben cómo combinar TI y TO

Soluciones
- Arquitectura de ciberseguridad por parte del North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)
- Metodología de evaluación NERC CIP
- Desarrollo de arquitectura de seguridad y políticas

Beneficios
- Las comunicaciones de red con control seguro protegen el tráfico de la red
- El control de integridad y revisión del software de aplicación asegura que las versiones más actuales y los parches estén siempre aplicados
- Un mejor desempeño de activos y gestión de productividad aseguran un desempeño óptimo de la red, seguridad aumentada, acceso seguro a datos y actualizaciones de software oportunas

Soluciones
- Gestión de parches centralizada, autentificación, autorización y auditoría
- Red diseñada para operaciones seguras y monitoreo de desempeño de sistema
- Protección de malware de punto final con prevención de pérdida de datos integrada, control de dispositivos, listas blancas y prevención de intrusión de anfitrión
- Checklist de conformidad NERC CIP

$3.8 millones costo promedio de una violación de datos

67% incremento en violaciones de datos en los últimos 5 años

70% de los empleados de compañías no entienden la ciberseguridad

92% del malware se propaga por correo electrónico

95% de los servidores HTTP son vulnerables ataques de intermediario (Man-in-the-middle attack)

Fuente: *Schneider Electric*

La gestión de riesgos y protección de ciberseguridad son ahora cruciales para asegurar las operaciones industriales sustentables

OXFORD BUSINESS GROUP

Las oportunidades y carencias de la ciberseguridad industrial en México

Debilidades
- Falta de un marco de ciberseguridad industrial
- Falta de un portafolio de soluciones y proveedores de servicio en la ciberseguridad industrial
- Falta de entendimiento por parte de los negocios respecto a su resiliencia en ciberseguridad

Fortalezas
- Demanda de instituciones públicas (industria, gobernación y defensa)
- Grandes innovaciones de productos en ciberseguridad industrial
- Crecimiento en profesionales calificados dentro de la ciberseguridad industrial
- Existencia de equipos de respuesta de emergencia informática, específicamente dentro de la ciberseguridad industrial

Amenazas
- Legislación lenta
- Falta de talento en ciberseguridad en la manufactura industrial
- El 5G y una conectividad más rápida podrían escalar la velocidad de los ataques

Oportunidades
- Incremento en demanda de ciberseguridad para la industria 4.0 y el internet de las cosas
- Posicionamiento estratégico dentro del sector de ciberseguridad industrial

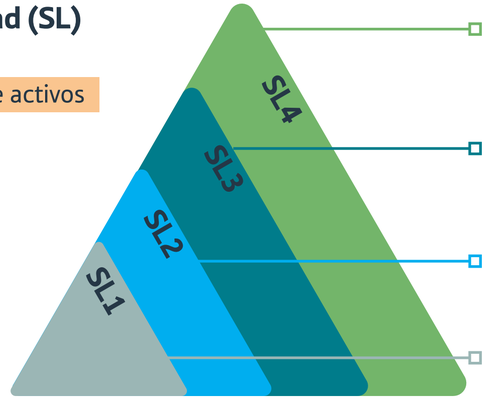
NIVEL DE MADUREZ

Niveles de Seguridad (SL) IEC 62443

Operador propietario de activos *(Secciones 2-1, 2-3, 2-4)*

Integrador de sistemas *(Secciones 2-4, 3-2, 3-3)*

Proveedor de productos/soluciones *(Secciones 3-3, 4-1, 4-2)*



- **SL4** — Protección contra violación de datos intencional usando medios sofisticados con recursos extendidos, habilidades específicas de sistema y alta motivación
- **SL3** — Protección contra violación de datos intencional usando medios sofisticados con recursos moderados, habilidades específicas de sistema y motivación moderada
- **SL2** — Protección contra violación intencional de datos usando medios simples y bajos recursos, habilidades genéricas y baja motivación
- **SL1** — Protección contra violación casual o por coincidencia

Datos Importantes: Estructura de Gestión de Riesgo

En una organización industrial, el riesgo financiero es manejado por el CFO, mientras que los riesgos operacionales son manejados por los cargos de liderazgo. El riesgo en ciberseguridad, sin embargo, con frecuencia queda a cargo del Jefe de Servicios Informáticos (CIO), siendo el Jefe de Seguridad Informática (CISO) quien le reporta al CIO. En la mayoría de las organizaciones, las unidades de negocio y sus operaciones dependen del CISO para gestionar el riesgo cibernético, quien a su vez les reporta a otros niveles senior, dado que los ciberataques representan amenazas a las operaciones, el capital intelectual y a la reputación.

Las preocupaciones de ciberseguridad más grandes para las empresas mexicanas

55% ransomware

51% ciberataques

A quienes culpan las empresas mexicanas por las violaciones en ciberseguridad

57% delincuentes cibernéticos

56% hackers

Un panorama cambiante

El surgimiento de la industria 4.0 en las organizaciones ha llevado a la existencia de ambientes industriales más complejos y se han vuelto comunes los costosos ataques o disrupciones a la infraestructura crítica. Se ha hecho un llamado para que las plantas de ensamblaje, los complejos petroquímicos y las redes eléctricas, reduzcan el riesgo, protejan sus activos heredados y mejoren su preparación cibernética en general. Esto hace aún más importante la habilidad para gestionar, detectar y protegerse contra ciberataques corporativos. El ataque de ransomware a la Colonial Pipeline en mayo del 2021 en Estados Unidos, por ejemplo, hizo noticia alrededor del mundo, después de las repercusiones de la escasez de combustible en la costa este.

Fuente: *PwC; Schneider Electric*

A pesar de que los riesgos a futuro involucran a todas las industrias, algunos sectores son más vulnerables a los ciberataques

SERVICIOS FINANCIEROS

- De acuerdo con una encuesta realizada en conjunto por La Organización de Estados Americanos y La Comisión Nacional Bancaria y de Valores, más del 40% de los ciberataques a instituciones financieras en México tuvieron éxito
- Las medidas de respuesta y recuperación costaron a las instituciones afectadas cerca de $107 millones en 2018, o aproximadamente 1% a 1.7% del EBITDA (ganancias previo interés, impuestos, depreciación y amortización) en 2017
- La mayoría de los incidentes de alto perfil incluyen ataques al Sistema de Pagos Electrónicos Interbancarios (SPEI) de México a principios de 2018 y el ataque de ransomware WannaCry en 2017

En foco

El ransomware ha surgido como una amenaza de ciberseguridad clave, atacando los archivos de la víctima y bloqueándolos hasta que se paga un rescate. El ransomware ha evolucionado desde correos de spam atacando computadoras individuales, a ataques sofisticados en grandes organizaciones con demandas de rescate muy grandes, casi siempre en bitcoin. Chainalysis, una empresa de ciberseguridad reveló que los rescates pagados en bitcoin incrementarion en un 311% en 2020 a alrededor de $350 millones, en aquel entonces.

INFRAESTRUCTURA CRÍTICA

- La mitad de los sistemas críticos de México enfrentaron infecciones por malware durante 2018, de acuerdo a la empresa en ciberseguridad Kaspersky. De manera similar, tan solo en agosto de 2019, un tercio de las computadoras industriales en México fueron atacadas, principalmente a través de internet, dispositivos extra o correo electrónico.
- Históricamente, la infraestructura crítica ha sido aislada con enfoque en seguridad operacional. En particular, los ambientes ICS/SCADA no han sido considerados como unidades con seguridad crítica y continúan estando conectados a redes de oficina o incluso a internet, lo que multiplica las posibles amenazas. Mientras tanto las tecnologías de la industria 4.0 y las redes internas corporativas continúan creciendo sin las contramedidas necesarias.
- La interdependencia y áreas de influencia de la infraestructura crítica es mucho mayor que la de las empresas comunes y por lo tanto los incidentes tienen mucho mayor impacto en todo lo directa o indirectamente relacionado con la compañía. A pesar de que las incidencias cibernéticas atacando a infraestructura crítica se ha vuelto más frecuente, los impactos financieros que comúnmente reportan las compañías, por mucho subestiman los verdaderos riesgos.
- Los sistemas de automatización y control industrial se usan para impulsar la infraestructura crítica del mundo, y los impactos a esta industria son difíciles de medir dado que los costos por incidente no reflejan la magnitud de las consecuencias o la urgencia en ser atendidos.

Las implicaciones de la ciberseguridad comercial e industrial

Industrial: Espionaje y disrupción a sistemas de control industrial

Stuxnet – sitio de Natanz Irán (2021)
Shamoon – Saudi Aramco (2012)

Retail: Robo de datos de tarjeta de crédito

Target – violación de datos mediante ataque a sistema de aire acondicionado (2014)
Home Depot – Violación de datos (2014)

Gobierno: Violación de información confidencial

US OPM - 18 millones de datos personales violados (2015)

Educación: Hacking y robo de datos de usuario

Universidad de California – Ataque de ransomware (2021)

Fuente: *OAS; Kaspersky*

Resiliencia

El crecimiento económico de México disminuyó a finales de 2019 como resultado de la desaceleración global. Sin embargo, sus fundamentos económicos como la relación entre la deuda pública y el PIB se mantuvieron fuertes.

Antes de la pandemia, la preparación digital del país era similar a la de las economías más grandes de la región.

La preparación digital era más avanzada a nivel empresarial e individual en temas básicos, en materia de facilidad para hacer negocios y de capital humano. Los aspectos más débiles eran la adopción de la infraestructura tecnológica y el ambiente para emprender.

Respuesta

A pesar que el estímulo fiscal federal tuvo un alcance limitado, el banco central actuó de forma rápida, y el sistema político descentralizado permitió respuestas de salud pública y fiscales de manera local.

Para salvaguardar la resiliencia y agilidad de los negocios, las compañías aceleraron sus agendas de desarrollo estratégico y adopción digital.

Alineado con los cambios en las prácticas de negocios y las expectativas de los consumidores, las compañías mexicanas han incorporado de forma inmensa la digitalización a sus estrategias corporativas en adelante.

Recuperación

Se espera que el gasto en digitalización incremente sustancialmente en Latinoamérica en comparación con otras regiones, con el sector de TI de México proyectado para un crecimiento de 10% en 2021.

La digitalización en México ha generado indirectamente una mayor conciencia acerca de la necesidad de invertir en ciberseguridad.

Si bien existen soluciones de ciberseguridad en México, las compañías están apenas poniéndose al día, especialmente en sectores críticos de la economía como del petróleo, el gas, la energía y los servicios públicos

Reinvención

Conforme se vuelve más prevalente la industria 4.0, las compañías deben repensar sus estrategias en ciberseguridad para proteger sistemas más sofisticados y prácticas de negocio altamente integradas.

La diversificada economía de México implica que sus vulnerabilidades cibernéticas son igualmente variadas. Quizás sea necesaria mayor protección para sectores fundamentales, como los servicios financieros y la infraestructura crítica.

Una forma más holística de gestionar y analizar el riesgo en ciberseguridad beneficiaría mucho a las compañías.

6 Aportes Clave

1

La economía de México había experimentado un crecimiento lento antes de la pandemia antes de la pandemia como resultado de una desaceleración en la economía global y su economía enfocada a la exportación.

2

Las compañías que operan en México y en la región aprovecharon los cambios en las prácticas de negocio y los patrones de los consumidores para digitalizar las operaciones.

3

Dada la historia de México con los ciberataques, ya se han implementado algunas soluciones. Sin embargo, hay mucho margen para implementar soluciones más integrales.

4

Conforme la economía de México incrementa en sofisticación y se integra más a las cadenas de suministro globales, crecerá la importancia de proteger su perfil en cambio constante.

5

Las estrategias de negocio han evolucionado como resultado de la digitalización, que a cambio ha generado más conciencia acerca de investigar en soluciones de ciberseguridad.

6

En adelante, la exposición variada de amenazas cibernéticas según el sector, requerirá priorización para enfrentar por completo los riesgos.

Designed by Brash
www.brash.agency