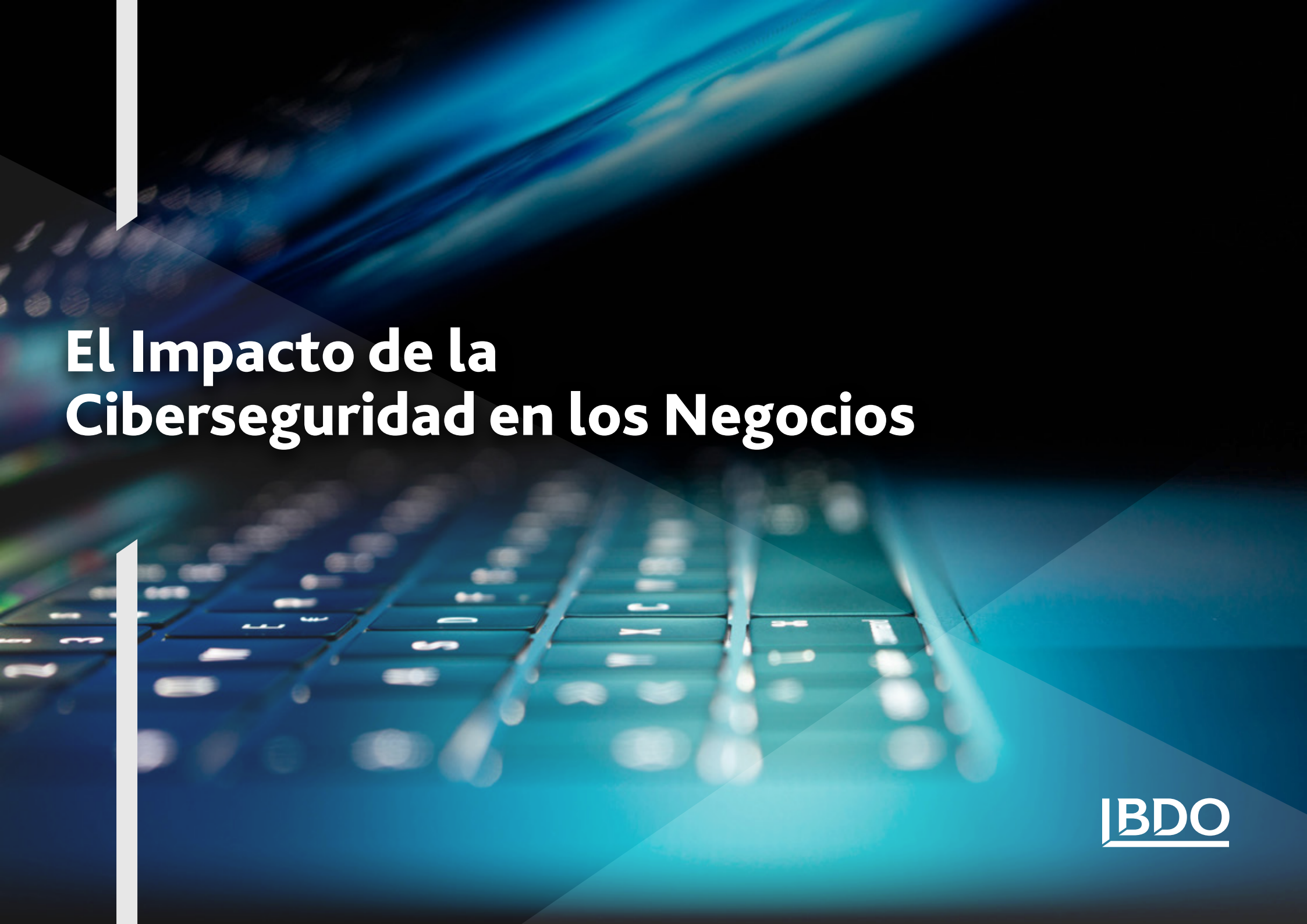
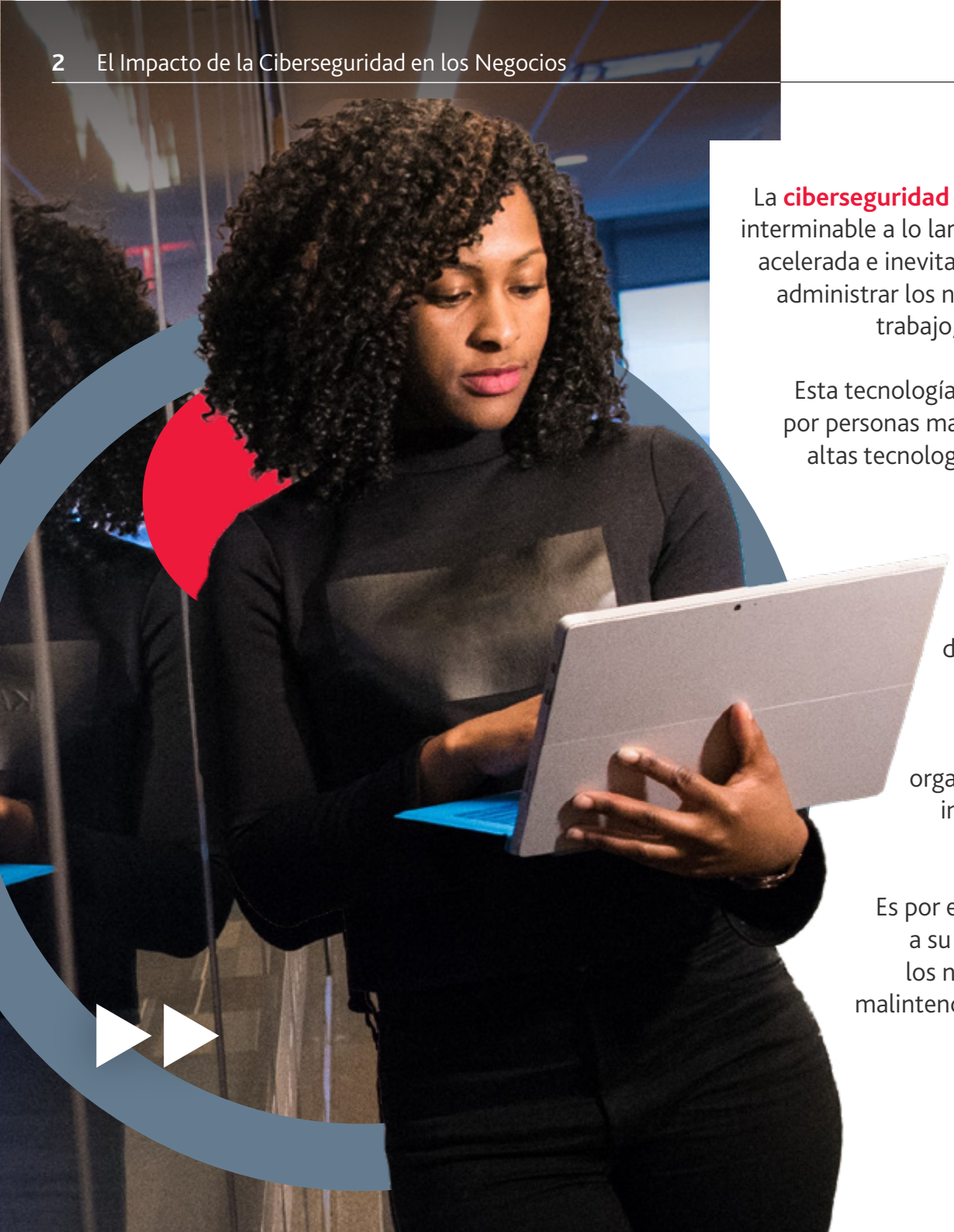


El Impacto de la Ciberseguridad en los Negocios

BDO



La **ciberseguridad** ha sido parte siempre de nuestras organizaciones, ha sido una batalla interminable a lo largo del tiempo, pero su transformación se está haciendo cada vez más acelerada e inevitable debido a la proliferación de recursos tecnológicos necesarios para administrar los negocios, generar nuevos productos, soportar los nuevos esquemas de trabajo, mejorar la experiencia del cliente y aumentar el valor en el mercado.

Esta tecnología crea nuevos riesgos y vulnerabilidades que está siendo aprovechadas por personas malintencionadas que se han convertido también en organizaciones con altas tecnologías y mecanismos de primer nivel que integran inteligencia artificial y aprendizaje automatizado.

Estamos creando una dependencia con la tecnología y los servicios informáticos que está llevando a los negocios a tener brechas de seguridad que hace unos años no existían sobre todo con la llegada de los servicios en la nube, teléfonos inteligentes, internet de las cosas e inteligencia artificial.

El alcance de las amenazas está en constante crecimiento y las organizaciones no están exentas. Los riesgos a los que estamos expuestos impactan a las pequeñas, medianas y grandes organizaciones de forma similar sin importar la industria en la que se encuentren.

Es por ello, que no contar con una estrategia de seguridad cibernética acorde a su tamaño o industria evita que puedan controlar o mitigar los riesgos a los nos enfrentamos, siendo un objetivo fácil para aquellas organizaciones malintencionadas que esperan con ansias la oportunidad de afectar el negocio.

¿CÓMO PROTEGERSE?

Contar con una estrategia robusta de ciberseguridad permite a su organización alinearse con el negocio y la tecnología para implementar los mecanismos apropiados para controlar o mitigar los riesgos propios de la transformación digital y tecnológica a la que nos enfrentamos hoy en día.

Se trata de los niveles apropiados de protección contra cualquier delito cibernético ya sea en forma de ataques para acceder, modificar o eliminar la información, obtener un beneficio a través de los colaboradores, o detener las operaciones diarias.
Al diseñar esta estrategia cibernética, debe considerar la inclusión de la infraestructura tecnológica, redes y comunicaciones, aplicaciones, información, nube, capacitación, concientización y resiliencia.

¿QUÉ ESTAMOS HACIENDO ACTUALMENTE?

Con el crecimiento de la tecnología, las organizaciones se han visto en la obligación de incluir, a grandes velocidades, mecanismos de ciberseguridad que hace pocos años no se tenían visualizados.

- Incorporación de nuevas regulaciones que han acelerado el proceso, cumplimos con los requisitos, pero no agregamos valor a la organización.
- Las empresas están haciendo un esfuerzo desmedido para promover la ciberseguridad en la alta dirección.
- Diseñan e incorporan la gestión de protección de datos con el uso de los componentes que existen actualmente en la organización sin contar con mecanismos más sofisticados.
- Incorporan a la gestión de riesgos la tecnología y ciberseguridad; sin embargo, se están tratando todas las tecnologías de la misma forma.
- Implementan herramientas de seguridad de uso frecuente sin considerar que hay nuevas modalidades de ataque que requieren nuevas tecnologías o nuevos mecanismos de monitoreo y detección.
- Realizan pruebas de penetración y vulnerabilidades para implementar soluciones de corto plazo que limitan la visión a futuro sobre las nuevas capacidades de los atacantes.
- Atienden la gestión actual con personal limitado sin contar con servicios de terceros para atender las necesidades a gran escala.

TENDENCIAS Y AGENDA 2023 DESDE EL PUNTO DE VISTA DE CIBERSEGURIDAD

- Crecimiento constante del panorama regulatorio
- Concientizar a la organización en todos sus niveles
- Monitoreo continuo, detección anticipada y respuesta ante incidentes
- Gestionar los riesgos de terceros
- Analizar comportamientos en los sistemas e infraestructura
- Cifrado permanente de los datos e información
- Automatización a través de un enfoque basado en riesgos
- Uso de inteligencia artificial
- Respuestas técnicas y sobre todo organizativas
- Desarrollo seguro de software
- Filosofía Zero Trust
- Incorporar el concepto de ciber resiliencia a la gestión de continuidad organizacional
- Migración de los servicios críticos a la nube
- Incorporar certificaciones que garanticen los controles apropiados
- Establecer un marco de gobierno formal para el área de ciberseguridad
- Apalancar las actividades sobre servicios gestionados a través de terceros especializados

"Actualmente las organizaciones no saben cómo identificar y gestionar los riesgos asociados a los nuevos esquemas de trabajo tecnológico y transformación digital.

Su actuación no se ha proliferado de la misma forma que han crecido estas tecnologías, lo que si hacen las modernas estructuras malintencionadas".

CONTACTO

CESAR CLAVEL
Director de Advisory

cesar.clavel@bdo.com.pa

Edificio BDO
Urb. Los Ángeles, Ave. El Paical
Tel: +507 279 9700

F&F Tower, Piso 30
Calle 50 y 56 Este
Tel: +507 280 8800

www.bdo.com.pa
www.bdo.global