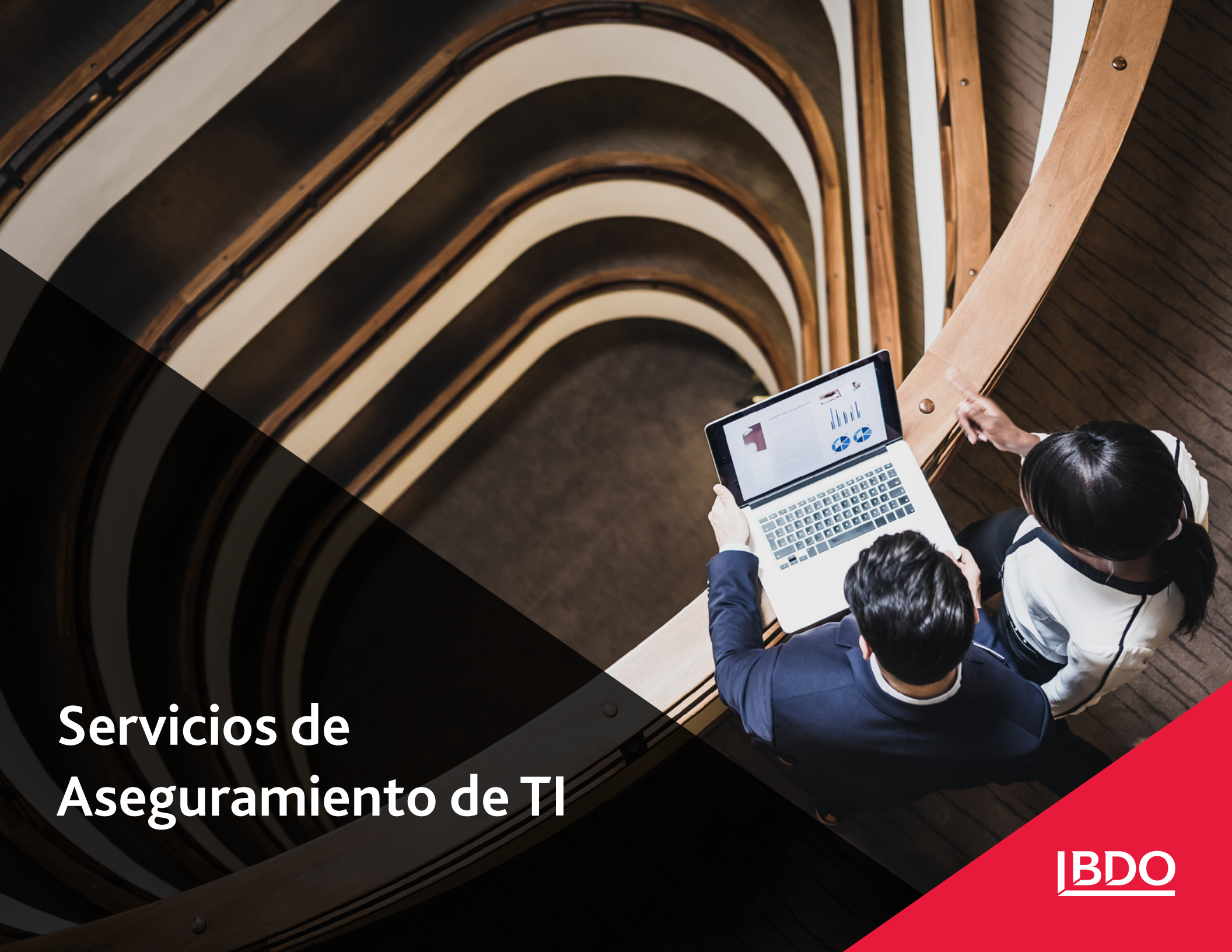


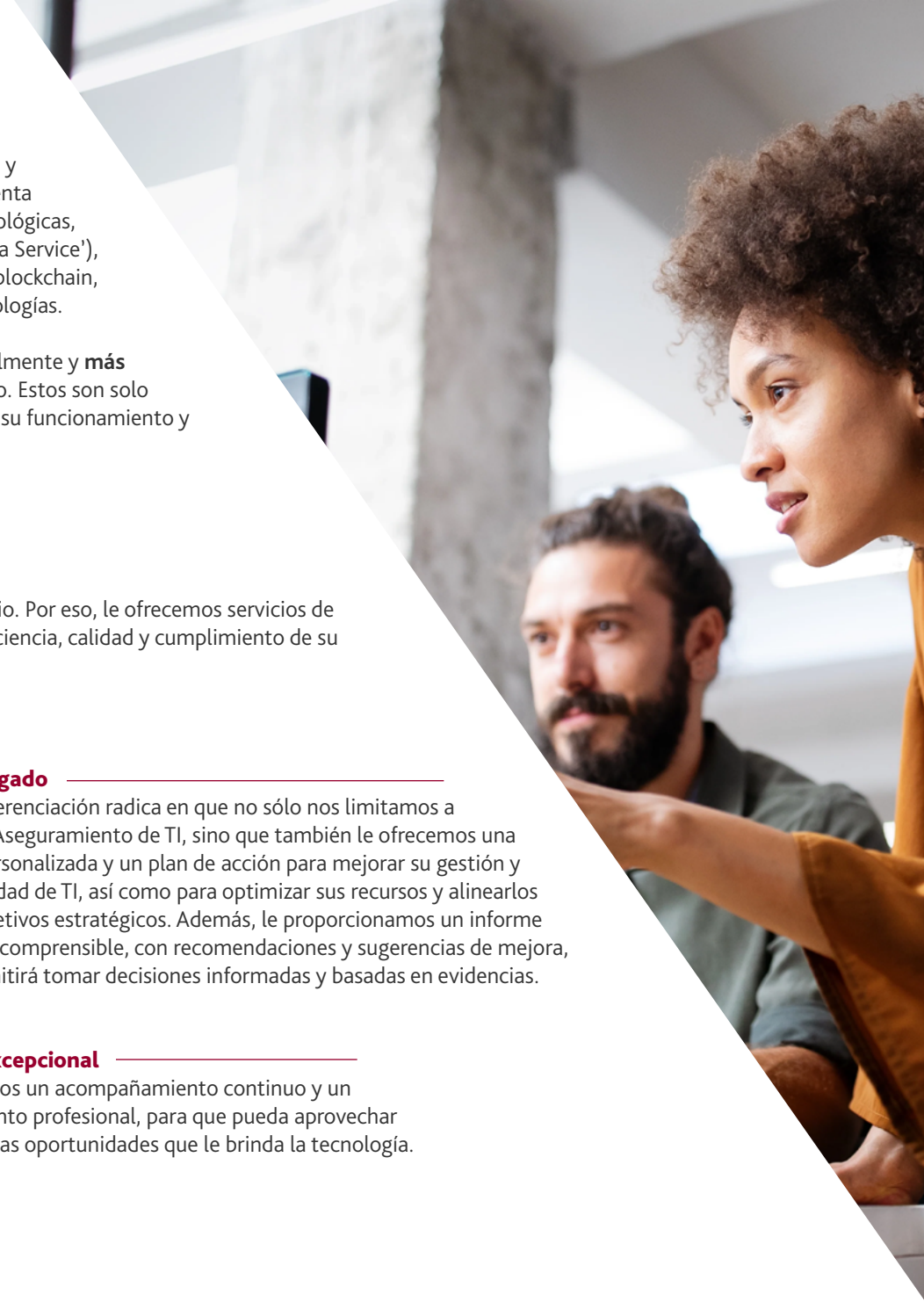
# Servicios de Aseguramiento de TI

BDO

# Servicios de Aseguramiento de TI

Hoy por hoy, las soluciones y herramientas tecnológicas han aumentado exponencialmente y sobre todo con una propagación muy ágil, dinámica y cambiante, lo cual, proyecta y representa muchos beneficios para las organizaciones. Sin embargo, al incrementar las facilidades tecnológicas, tales como gestión en la nube, comercio electrónico, diversas soluciones como servicio ('As a Service'), DevOps, automatización robótica de procesos (RPA), inteligencia artificial (IA), metaverso, blockchain, activos digitales, entre muchos otros, también aumentan los riesgos asociados a estas tecnologías.

**Más del 70%** de las empresas sufren algún tipo de incidente de seguridad informática anualmente y **más del 40%** de los proyectos de TI fracasan por falta de calidad, cumplimiento o aseguramiento. Estos son solo algunos de los riesgos que enfrentan las organizaciones que dependen de la tecnología para su funcionamiento y competitividad.



# ¿Por qué elegir BDO?

En **BDO en Panamá**, sabemos que la tecnología es un factor clave para el éxito de su negocio. Por eso, le ofrecemos servicios de Aseguramiento de Tecnología de Información, que le ayudarán a garantizar la seguridad, eficiencia, calidad y cumplimiento de su entorno de IT, sistemas, procesos y datos.

### Experiencia

Nuestra amplia experiencia y conocimiento en el ámbito de los servicios de Aseguramiento de TI, así como en nuestra metodología global y herramientas propias y exclusivas, nos permite realizar un análisis integral y detallado de su infraestructura, aplicaciones, datos, redes y entorno general de TI.

### Valor agregado

Nuestra diferenciación radica en que no sólo nos limitamos a realizar un Aseguramiento de TI, sino que también le ofrecemos una asesoría personalizada y un plan de acción para mejorar su gestión y gobernabilidad de TI, así como para optimizar sus recursos y alinearlos con sus objetivos estratégicos. Además, le proporcionamos un informe detallado y comprensible, con recomendaciones y sugerencias de mejora, que le permitirá tomar decisiones informadas y basadas en evidencias.

### Expertos BDO

Contamos con un equipo multidisciplinario, certificado y capacitado y nuestro enfoque innovador.

### Servicio excepcional

Garantizamos un acompañamiento continuo y un asesoramiento profesional, para que pueda aprovechar al máximo las oportunidades que le brinda la tecnología.

# Auditoría de TI

Le ayudamos a evaluar y mejorar la gestión de sus sistemas de información y ambiente general de TI, así como a mitigar los riesgos asociados a la seguridad, la integridad y la disponibilidad de sus datos.

Nuestro servicio consiste en evaluar y verificar el correcto funcionamiento, la seguridad y el cumplimiento de las aplicaciones de su empresa. Nuestro objetivo es ayudarle a identificar y mitigar los riesgos relacionados con la tecnología, así como a mejorar el rendimiento y la eficacia de sus procesos de negocio.

En **BDO en Panamá** le ofrece una solución integral y personalizada, basada en las buenas prácticas y estándares internacionales, para asegurar el cumplimiento de sus objetivos estratégicos y operativos.

**Sub-servicios**

- Diagnóstico de TI
- Auditoría Interna de TI

# Riesgo de TI

Le asesoramos en conocer y gestionar los riesgos que amenazan la seguridad, la continuidad y el valor de sus sistemas de información y entorno general de TI.

Ofrecemos un servicio de evaluación de riesgo tecnológico, que consiste en identificar y valorar los posibles escenarios de amenaza, vulnerabilidad e impacto que podrían afectar los activos de información de su empresa. Nuestro objetivo es ayudarle a establecer una hoja de ruta y gestionar un plan de mitigación y contingencia, que le permita proteger su información y garantizar la continuidad de su negocio.

**BDO en Panamá** le brinda una solución de vanguardia, basada en una metodología probada y reconocida, para realizar un diagnóstico integral y proponer acciones de mejora.

Proveemos una evaluación de riesgo tecnológico a la medida de sus necesidades, con un enfoque atractivo e innovador, que le permitirá obtener una visión clara y completa de su situación actual y futura.

# Gobierno de TI

La evaluación del gobierno de TI le permite medir y mejorar el nivel de madurez de su gestión de Tecnología de Información y Comunicación (TIC), así como alinearlas con la estrategia de su negocio, para obtener el máximo valor de sus inversiones, recursos y procesos de TI.

Le ofrecemos una solución innovadora, basada en normas y buenas prácticas internacionales con un enfoque contemporáneo que le permitirá obtener una visión clara y completa.

# Cumplimiento de TI

Le brindamos una solución integral para asegurar que su infraestructura, sistemas y procesos de tecnología de la información cumplan con los estándares y normativas vigentes, así como con las buenas prácticas del sector. Con nuestro equipo de expertos en cumplimiento de TI, le ayudamos a identificar y mitigar los riesgos asociados al uso de la tecnología, a mejorar el rendimiento y la eficiencia de sus recursos de TI y a optimizar su inversión en innovación.

**Subservicios**

- Leyes y regulaciones de los distintos entes de control y supervisión
- Normas y estándares nacionales e internacionales
- Marcos de referencia de trabajo y buenas prácticas de la industria

# Control Interno de TI

Le ofrecemos una solución con diferenciación para evaluar y mejorar el diseño y la efectividad de los controles internos relacionados con la tecnología de información, tanto a nivel de procesos como de sistemas.

Estudiamos minuciosamente cada detalle en temas de controles internos de TI, asegurando que sus objetivos estratégicos, operativos y financieros se cumplan de manera eficaz y eficiente, minimizando los riesgos de error, fraude o incumplimiento.

# Evaluación de riesgo de Seguridad de la Información (SGSI)

Contamos con una solución integral para identificar y analizar los riesgos que pueden afectar a la confidencialidad, integridad o disponibilidad de la información de su organización, tanto en el entorno de teletrabajo como en el presencial.

Con nuestro equipo de expertos en auditoría, seguridad y gestión de TI, le ayudamos a evaluar y recomendar los controles más eficientes para resguardar y proteger su información, cumpliendo con los estándares y normativas vigentes, considerando el Sistema de Gestión de Seguridad de la Información y las buenas prácticas del sector.

# Evaluación de Riesgo de Ciberseguridad

Casi todas las actividades de las empresas se realizan en línea; tanto las empresas pequeñas como las grandes están expuestas a las ciberamenazas.

La ciberseguridad es un aspecto clave para el éxito de su organización, ya que le permite proteger su información, su reputación y su competitividad. Sin embargo, la ciberseguridad también implica una serie de riesgos que deben ser identificados, analizados y gestionados de forma adecuada y oportuna.

Dado lo anterior, se debe identificar los riesgos, detectar las ciberamenazas y proteger frente a los ciberataques, que son cada vez más dinámicos y sofisticados.

**BDO en Panamá** le ofrece un servicio que le permite conocer el nivel de exposición y vulnerabilidad de su organización frente a las amenazas cibernéticas.

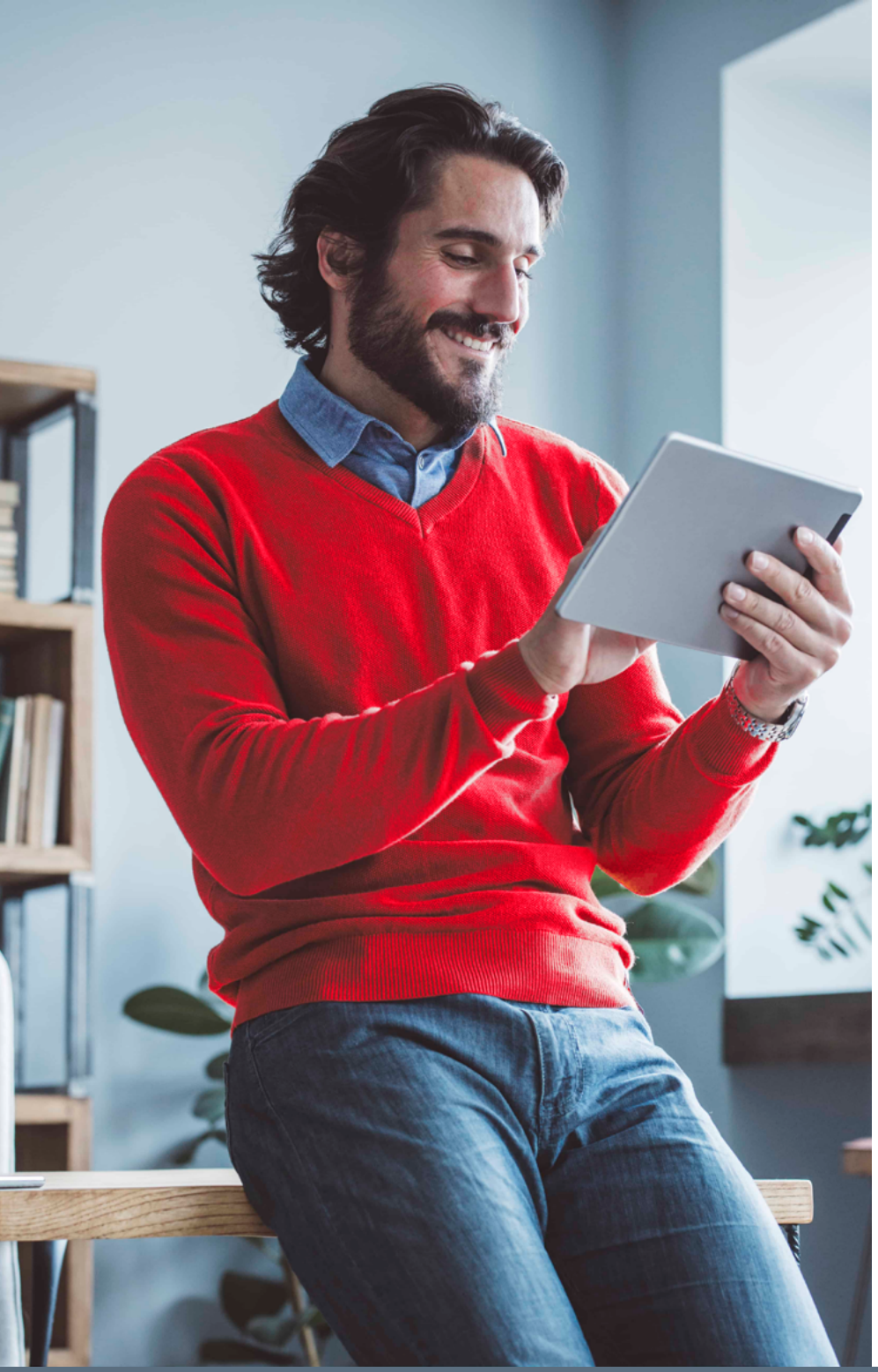
# Cumplimiento de IT SOX

La Ley Sarbanes-Oxley (SOX) exige que las organizaciones certifiquen la exactitud de sus estados financieros, con el respaldo de sus altas autoridades ejecutivas y de un informe independiente de un Auditor Externo quien evalúa la efectividad de sus sistemas de control interno.

Le ofrecemos una solución integral para asegurar que su infraestructura, sistemas y procesos de tecnología de la información cumplan con los requisitos y estándares de la Ley Sarbanes-Oxley (SOX), que busca mejorar el gobierno corporativo y la transparencia de los reportes financieros.

Nuestros servicios incluyen los principales aspectos:

- Introducción a la metodología para las organizaciones que deben cumplir por primera vez.
- Estrategia de definición del alcance, incluyendo aplicaciones, procesos y controles SOX.
- Desarrollo de RCM (Matrices de Riesgos y Controles).
- Análisis del diseño e implementación (idoneidad) de riesgos y controles de los procesos.
- Pruebas de los controles (efectividad).
- Evaluación de la gestión de accesos de usuarios y segregación de funciones.
- Identificación de las deficiencias y definición de planes de remediación.
- Recomendaciones y mapa de ruta para la optimización y racionalización de controles.



# Informes SOC

En un mundo cada vez más digitalizado y conectado, la confianza en la seguridad y disponibilidad de los sistemas de información es vital para el éxito de cualquier negocio. Sin embargo, muchos proveedores de servicios de TI no cuentan con los estándares necesarios para garantizar la calidad y eficiencia de sus procesos y operaciones.

Los Informes SOC (Service Organization Control) son informes de auditoría independientes que evalúan el diseño y la efectividad de los controles internos de una organización de servicios, enfocados en la seguridad, disponibilidad, integridad, confidencialidad y privacidad de la información, transmitiendo a sus clientes, socios y reguladores confianza, transparencia y credibilidad.

**Subservicios**

- **Informe SOC 1.** Evalúan los controles internos de TI relacionados con los controles, procesos y estados financieros de la organización de servicios.
- **Informe SOC 2.** Evalúan los controles internos de TI relacionados con los criterios de confianza establecidos por el Instituto Americano de Contadores Públicos Certificados (AICPA).
- **Informe SOC 3.** Son versiones resumidas y públicas de los Informes SOC 2, que pueden ser utilizados para fines de mercadeo y transparencia.
- **Informe SOC de Asesoría y acompañamiento** en la implementación y mejora de los controles internos de TI, basados en las normas y estándares internacionales, incluyendo Seguridad de la Información, Ciberseguridad, Gobierno y Gestión, etc.

# Prevención de Riesgo de Fraude de TI

**El 85% de las empresas** han sufrido algún tipo de fraude de TI en los últimos dos años. **El 90% de estos fraudes** se deben a la falta de controles adecuados de seguridad de la información. El riesgo de fraude de TI es una amenaza real y creciente para las organizaciones de todos los sectores y tamaños, que puede causar pérdidas económicas, daño reputacional, sanciones legales y riesgos operativos.

- Realizamos un diagnóstico de la situación actual de la organización en materia de prevención de riesgo de fraude de TI, identificando las áreas de mayor riesgo, los tipos de fraude más frecuentes y los factores que los propician.
- Recomendamos un plan de acción para prevenir y combatir el riesgo de fraude de TI, basado en las buenas prácticas internacionales y adaptado a las necesidades específicas de la organización.

# Gestión de Riesgo de Terceros (TPRM)

**El 75% de las empresas** dependen de proveedores externos para realizar sus actividades de TI. **El 65% de estas empresas** han sufrido algún tipo de incidente de seguridad de la información por parte de sus proveedores en los últimos tres años.

En un mundo cada vez más interconectado y globalizado, la gestión de riesgo de terceros se ha convertido en un factor clave para el éxito de las organizaciones que utilizan servicios de TI externos, tales como nube, software, hardware, telecomunicaciones, entre otros. Sin embargo, muchas organizaciones no cuentan con los mecanismos adecuados para evaluar, monitorear y controlar el desempeño y la seguridad de sus proveedores de TI, lo que puede generar vulnerabilidades, incumplimientos, pérdidas y daños reputacionales.

- Gestionamos de forma eficiente y efectiva el riesgo asociado a sus proveedores de TI.
- Realizamos un análisis de la situación actual de la organización en materia de gestión de riesgo de terceros, identificando los proveedores de TI críticos, los riesgos inherentes y residuales, los controles existentes y las brechas de gestión.
- Recomendamos un marco de gestión de riesgo de terceros, basado en las buenas prácticas internacionales y adaptado a las necesidades específicas de la organización.

# Evaluación de la Continuidad del Negocio (SGCN)

En **BDO** sabemos que la continuidad del negocio es vital para cualquier organización. Por tal motivo, le ofrecemos un servicio de evaluación de la continuidad del negocio, enfocado en tecnología, que le permite identificar y gestionar los riesgos que pueden afectar a sus sistemas, procesos y datos.

Nuestro servicio consiste en los siguientes aspectos principales:

- Realizar un Análisis de Impacto al Negocio (BIA) para determinar los requisitos de recuperación de los servicios críticos de tecnología.
- Recomendar un Plan de Continuidad del Negocio (BCP) que establezca las estrategias, roles y responsabilidades para garantizar la continuidad de las operaciones ante una interrupción.
- Recomendar un Plan de Recuperación en caso de Desastres (DRP) y pruebas periódicas del Plan de Continuidad para verificar su efectividad y actualizarlo según las necesidades del negocio.
- Brindar asesoría y acompañamiento durante la implementación y el mantenimiento del Sistema de Gestión de Continuidad del Negocio.

## Atestiguamiento SWIFT

Sabemos que la seguridad de las transacciones financieras es clave para el desarrollo de su institución. Por eso, ofrecemos un servicio de evaluación del cumplimiento del Programa de Seguridad del Cliente (CSP) de SWIFT, la Sociedad para la Comunicación Financiera Interbancaria Mundial.

Nuestro servicio consiste en los principales aspectos:

- Realizar un diagnóstico de la situación actual de su organización respecto al cumplimiento de los controles obligatorios y controles recomendados del Marco de Controles de Seguridad del Cliente (CSCF) actualizado de SWIFT.
- Recomendar un plan de acción para implementar las medidas correctivas y preventivas necesarias para alcanzar el nivel de cumplimiento deseado.
- Verificar y validar el cumplimiento de los controles mediante auditorías independientes y certificadas por SWIFT.
- Brindar acompañamiento y orientación en el proceso de autoevaluación y reporte anual del CSP de SWIFT.

## AML (Anti-Money Laundering) - Cumplimiento de TI

El lavado de activos es una amenaza global que afecta a la integridad y la reputación de las entidades financieras. Por eso, ofrecemos un servicio de AML (Anti-Money Laundering) desde la perspectiva de evaluación del cumplimiento de TI, que le permite cumplir con las normativas nacionales e internacionales en materia de prevención y detección de operaciones de blanqueo de capitales.

Nuestro servicio consiste en los principales aspectos siguientes:

- Realizar un diagnóstico de la situación actual de su sistema de AML, evaluando su diseño, implementación, funcionamiento y eficacia.
- Evaluar y analizar las propiedades, características, seguridad y disponibilidad del software de monitoreo utilizado, incluyendo su entorno de TI.
- Analizar la gestión integral del sistema de AML, considerando las reglas definidas, controles automatizados en ejecución, interfaces de comunicación entre aplicaciones y repositorios de datos y las distintas parametrizaciones, controles configurables y tareas programadas alrededor del software.
- Identificar y priorizar las brechas y oportunidades de mejora en su sistema de AML, considerando los riesgos inherentes y residuales de su negocio.
- Evaluar la gestión de notificaciones, seguimiento y resolución en relación con el software de monitorio, así como el volumen y precisión de resultados y reportes de transacciones y operaciones relacionados.
- Recomendar las buenas prácticas y tendencias del sector sobre la gestión del software de monitoreo como solución integral.

# Segregación de Funciones – SoD

La segregación de funciones es un principio fundamental para el control interno y la prevención de fraudes. Por eso, ofrecemos un servicio que le permite evaluar y mejorar el diseño y la implementación de su gestión y matriz de SoD en sus sistemas de información.

Nuestro servicio consiste en:

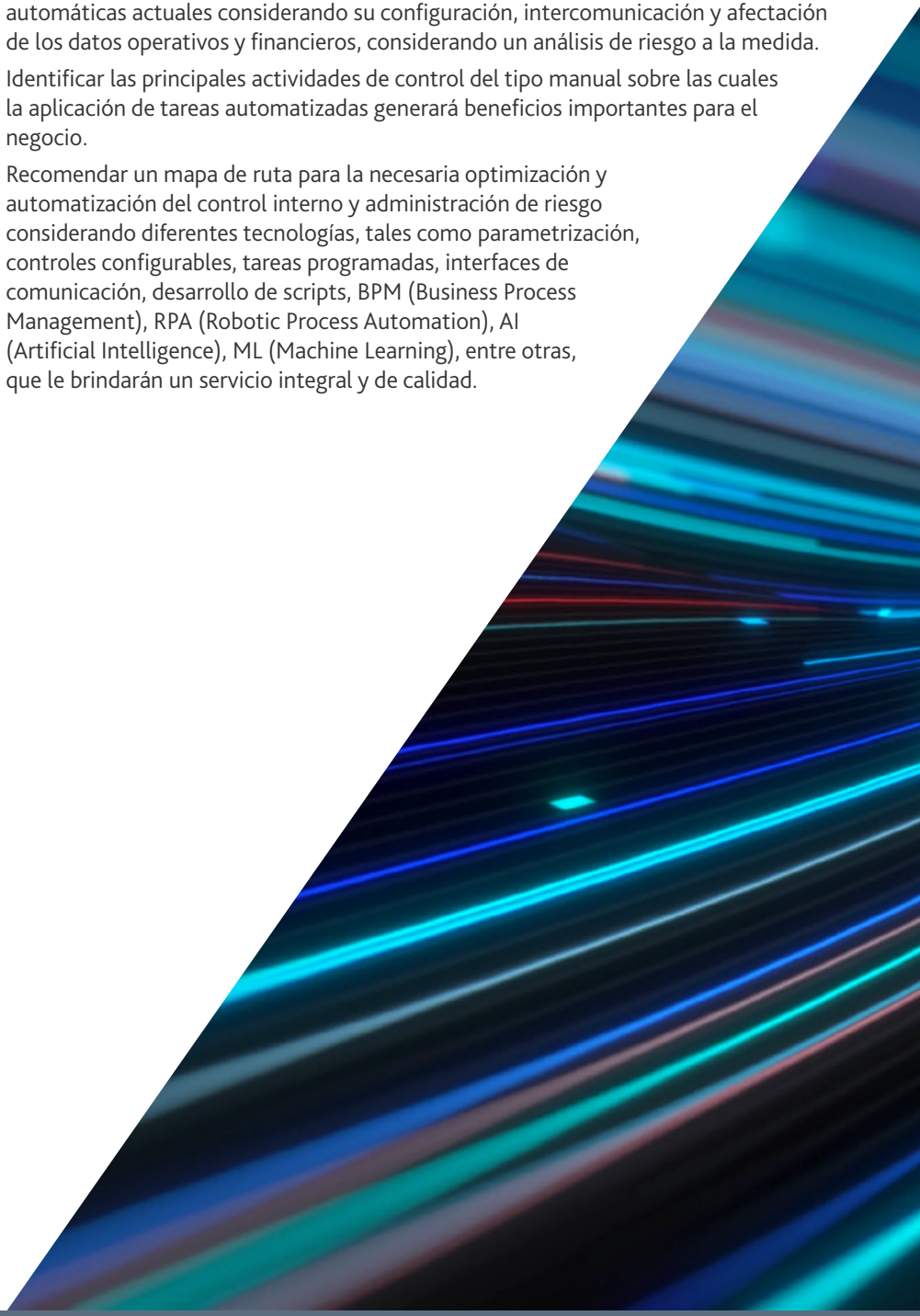
- Realizar un análisis de riesgos de SoD, identificando las posibles incompatibilidades y conflictos de interés entre las funciones y los roles asignados a los usuarios de los sistemas de información.
- Elaborar, evaluar o recomendar una matriz de SoD, definiendo las funciones críticas y los roles adecuados para cada proceso de negocio, así como las reglas de segregación y mitigación de riesgos.
- Identificar brechas y oportunidades de mejora, considerando el nivel de madurez y situación actual y definiendo según la necesidad de cada organización la hoja de ruta conforme al estado futuro deseado.
- Capacitar y asesorar a su personal en el cumplimiento y la gestión del control interno de segregación de funciones, así como en las buenas prácticas y tendencias de la industria.

# Evaluación de Procesos de Negocio Automatizados

Le brindamos un servicio de Evaluación de Procesos de Negocio Automatizados, que consiste en analizar y examinar los flujos de trabajo de su empresa mediante el involucramiento de la Tecnología de Información y Comunicación.

Nuestro servicio consiste en:

- Identificar los procesos principales y relevantes de la organización que tienen impacto sobre la información operativa, administrativa y financiera de la organización.
- Evaluar el flujo de entrada, proceso, salida, custodia y reporte de la información clave del negocio, incluyendo los procedimientos, actividades y controles preponderantes.
- Verificar el grado de automatización actual de los procesos de negocio, el nivel de utilización de la tecnología e involucramiento de procedimientos manuales mediante participación humana.
- Detectar brechas y oportunidades de mejora sobre las actividades de control automáticas actuales considerando su configuración, intercomunicación y afectación de los datos operativos y financieros, considerando un análisis de riesgo a la medida.
- Identificar las principales actividades de control del tipo manual sobre las cuales la aplicación de tareas automatizadas generará beneficios importantes para el negocio.
- Recomendar un mapa de ruta para la necesaria optimización y automatización del control interno y administración de riesgo considerando diferentes tecnologías, tales como parametrización, controles configurables, tareas programadas, interfaces de comunicación, desarrollo de scripts, BPM (Business Process Management), RPA (Robotic Process Automation), AI (Artificial Intelligence), ML (Machine Learning), entre otras, que le brindarán un servicio integral y de calidad.



# Evaluación específica de plataformas y marcos de trabajo (AUP)

El servicio de Procedimientos Previamente Acordados (AUP), consiste en la realización de procedimientos específicos de auditoría, evaluación de riesgo, cumplimiento y gobierno de IT, previamente convenidos con la gerencia de las organizaciones. Llevamos a cabo procedimientos, los cuales han convenido el auditor, la empresa y partes interesadas, informando sobre los resultados obtenidos.

**Desde nuestra experiencia le ofrecemos las siguientes capacidades y especializaciones:**

- Plataformas
  - Sistemas On-premise, ERP, EBS, CLOUD, SAAS
  - Hardening DBMS – Sistema Gestor de Base de Datos
  - Hardening SO – Sistema Operativo
  - SOC – Centro de Operaciones de Seguridad (Firewalls, IPS, IDS, Antimalware, Antivirus, SIEM, EDR, MDM & BYOD)

- Marcos de trabajo (frameworks nacionales e internacionales)
  - IaAM - Gestión de Identidad y Acceso
  - Gestión de virtualización de servidores
  - Migración de sistemas de información
  - Licenciamiento de Software
  - DevOps (Desarrollo y Operaciones) y metodologías ágiles
  - Inspección física y Ambiental de data center (IDC – TIER)
  - Protección de Datos Personales
  - Canales digitales
  - Requerimientos de entidades de control, supervisión y certificación -EDI, e-commerce, pagos electrónicos, Telered

## Certificación de Sistemas Contables

Debido a la importancia de cumplir con las regulaciones, decretos ejecutivos y resoluciones que exige la autoridad DGI - Dirección General de Ingresos y certificar sus libros contables electrónicos, presentamos los objetivos de la Certificación Contable del Sistema Magnético:

- Revisar los aspectos legales y contables del contable, utilizado por las compañías, incluyendo los formatos que harán las veces de registro de diario y del mayor general.
- Verificar controles internos que aseguren la contabilización apropiada y oportuna de todas las actividades y transacciones.
- Verificar que la tecnología aplicada para la gestión de los libros electrónicos contables integre de forma apropiada los siguientes aspectos:
  I. Los registros queden grabados de manera irreversible e inalterable.
  II. La conservación del registro contable sea realizada por el plazo que señale la ley.
  III. La recuperación del registro contable sea eficiente y eficaz.
  IV. Los procedimientos de verificación o prueba de los equipos utilizados, sea efectiva.
- Emitir la Certificación como Contadores Públicos Autorizados - CPA para ser presentada ante la autoridad en procesos de solicitud, verificación o investigación.

Desde **BDO en Panamá**, no solamente le emite la certificación del sistema contable, sino también, un informe detallado de control interno conteniendo el alcance de procedimientos evaluados, pruebas realizadas y resultados obtenidos, así como las recomendaciones y sugerencia de mejora que le permitirán afinar su gestión de la tecnología en relación con su sistema contable y optimizar los resultados de control interno.

# Documentación de planificación y métodos de TI

Le brindamos un servicio de Documentación de planificación y métodos de TI, el cual consiste en elaborar y actualizar los documentos que regulan y orientan la gestión y el uso de la tecnología en su organización.

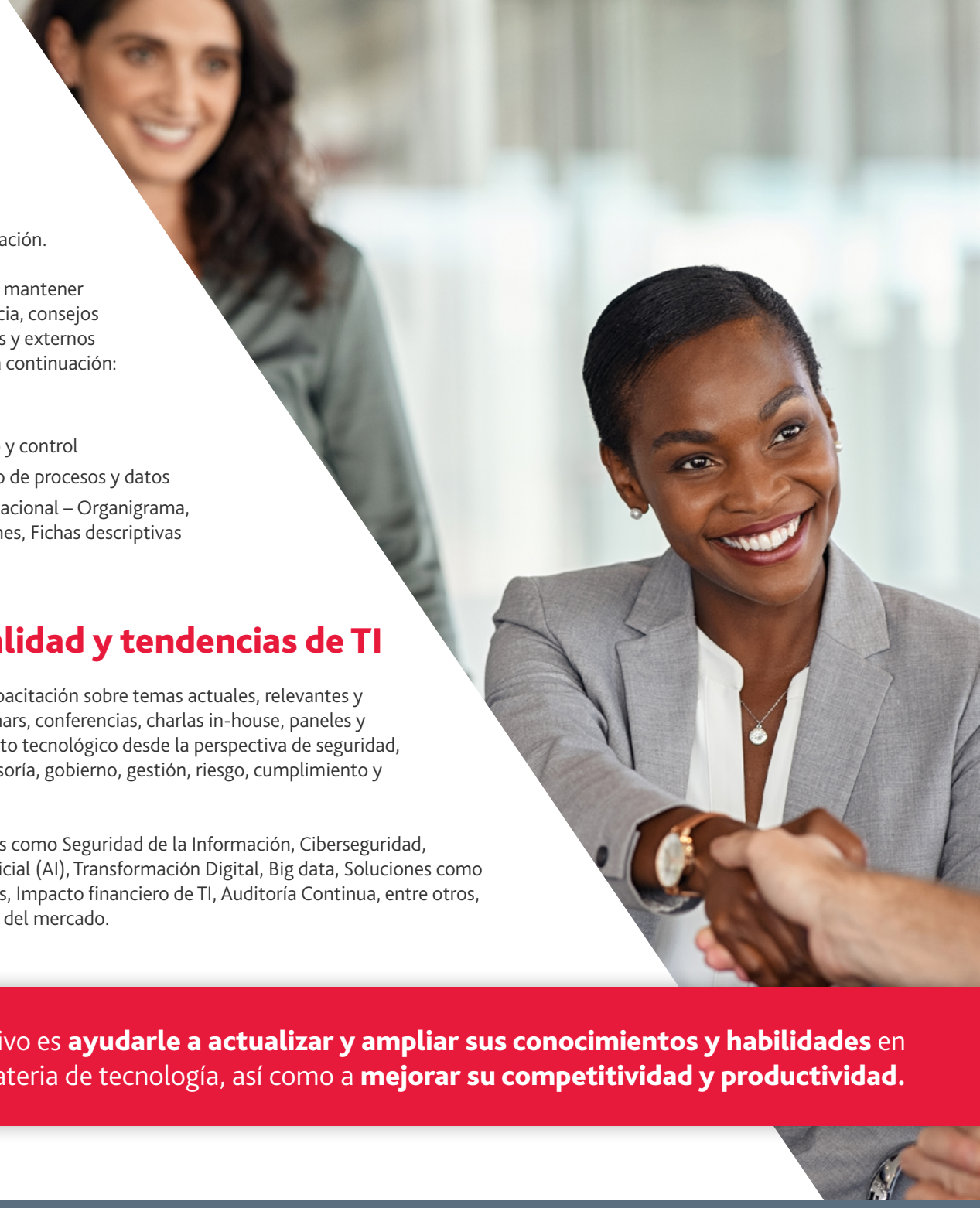
Dentro de los documentos relevantes que se torna necesario elaborar y mantener actualizados a partir del requerimiento de la administración, alta gerencia, consejos directivos, comités, entidades de control y regulación, revisores internos y externos y demás partes relacionadas, se encuentran algunos de los principales a continuación:

- Políticas de Tecnología de Información
- Políticas de Seguridad de la Información
- Procedimientos de TI/SI
- Planes
- Manuales
- Instructivos
- Matrices de riesgo y control
- Diagramas de flujo de procesos y datos
- Estructura organizacional – Organigrama, Manual de funciones, Fichas descriptivas de posiciones

# Capacitación sobre tópicos de actualidad y tendencias de TI

Gracias a nuestra amplia experiencia podemos brindar el servicio de capacitación sobre temas actuales, relevantes y emergentes, que consiste en impartir cursos, talleres, seminarios, webinars, conferencias, charlas in-house, paneles y conversatorios, sobre los temas más novedosos e innovadores del ámbito tecnológico desde la perspectiva de seguridad, confidencialidad, privacidad, disponibilidad, continuidad, auditoría, asesoría, gobierno, gestión, riesgo, cumplimiento y cntrol interno.

Nuestra propuesta de valor abarca una amplia variedad de tópicos, tales como Seguridad de la Información, Ciberseguridad, Cloud computing, RPA (Robotic Process Automation), Inteligencia Artificial (AI), Transformación Digital, Big data, Soluciones como servicio ('As a Service'), Organizaciones de Servicios, Gestión de terceros, Impacto financiero de TI, Auditoría Continua, entre otros, que le permitirán estar al día de las últimas novedades y oportunidades del mercado.



Nuestro objetivo es **ayudarle a actualizar y ampliar sus conocimientos y habilidades** en materia de tecnología, así como a **mejorar su competitividad y productividad.**

## CONTÁCTENOS

**DARÍO GONZÁLEZ**
Socio Líder de Auditoría y Aseguramiento
dario.gonzalez@bdo.com.pa

**MARVIN CABEZAS**
Gerente Senior de Auditoría y Aseguramiento de TI
marvin.cabezas@bdo.com.pa

**www.bdo.com.pa**