PwC Bolivia

Servicios de Tecnología

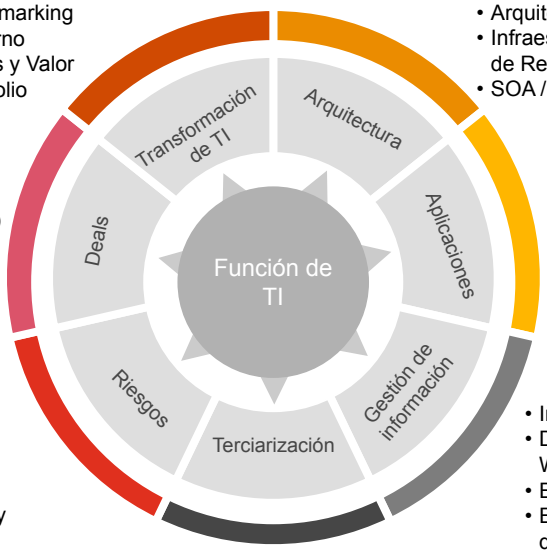
Transformando los desafíos en oportunidades

pwc

Fortalecimiento de la Función de TI

¿Cómo podemos ayudarte?

Brindamos asesoría independiente en el desarrollo de soluciones que le permitan incrementar la eficiencia en los componentes y factores críticos que influyen en la función de TI.



- Estrategia
- Organización y Benchmarking
- Gobierno
- Costos y Valor
- Portafolio

- Data Center
- Tecnologías Emergentes
- Arquitectura de Aplicaciones
- Infraestructura y Arquitectura de Redes
- SOA / BPM

- Diagnóstico TI – Pre Deal
- Divestiture (Desinversión)
- M & A (PMI)
- Mejoras Post Adquisición

- Estrategia y Selección
- Oracle
- SAP
- PMO
- Quality Assurance
- Implementación, Mejoras e Integración

Metodologia

Para brindar eficiencia a nuestros clientes, contamos con la metodología IT Transformation®, enfocada en incrementar la eficiencia de la función de TI y desarrollarla en una capacidad empresarial que le genere competitividad y apoyo en el desempeño de las operaciones centrales de negocio.

- Estrategia y Gobierno de Seguridad
- Gestión de Identidades
- Aseguramiento
- Continuidad del Negocio y Recuperación de TI

- Inteligencia de Negocios
- Data Empresarial & Data Warehousing
- Enterprise Content Management
- Estrategia, Arquitectura y Gobierno de Información

- Servicios Compartidos
- Outsourcing
- Adquisiciones
- Guía de Proveedores
- Servicios de Tercerización

IT Transformation®

Pilares de transformación

- Gestión de la complejidad de TI
- Innovación
- Agilidad en la empresa
- Priorizar el valor generado

Estrategia

- Análisis del contexto de TI
- Capacidades actuales de TI
- Definición del caso de cambio

Diseño

- Diseño del modelo operativo de TI

Construcción

- Construcción y validación de los servicios y procesos
- Construcción y Test de tecnologías e infraestructuras
- Definición de organización y gobierno de TI
- Gestión de personal y capacidades

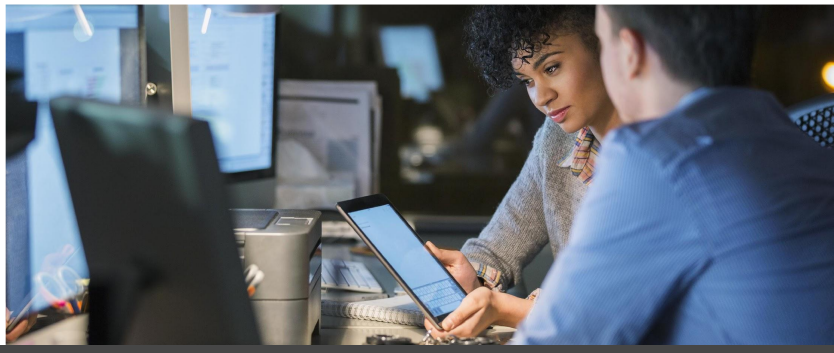
Implementación

- Migración al nuevo modelo operativo de TI

Operación y revisión

- Operaciones de TI y mejora continua

Seguridad de la Información



La seguridad de la información tiene muchas facetas, siendo la meta principal proteger la confidencialidad, integridad y disponibilidad de los activos de información de una organización. Cualquier incidente que afecte a uno de estos componentes puede poner en riesgo rápidamente a toda una organización, exponiéndola a conflictos legales y daño en su imagen corporativa. Nuestra firma apoya a sus clientes a enfrentar problemas complejos desarrollando soluciones concretas de seguridad de información en todos sus niveles.

¿Cómo podemos ayudarte?

1 Estrategia de seguridad, riesgo y cumplimiento

- Diagnóstico de seguridad de la información
- Evaluación de tecnología utilizada
- Diseño de estrategia de seguridad de la información
- Cumplimiento de regulaciones
- Gestión de proveedores

2 Gestión de incidentes y amenazas

- Identificación de amenazas
- Ethical Hacking
- Pruebas de seguridad
- Gestión de crisis
- Plan de acción ante incidentes

5 Servicios terciarizados de ciberseguridad y privacidad

- Detección y respuesta ante amenazas
- Gestión de vulnerabilidades
- Gestión de dispositivos y programas
- Evaluaciones a gran escala
- Privacidad como servicio terciarizado

3 Gobierno y privacidad de la información

- Seguridad de la información en el modelo de gobierno
- Políticas y lineamientos de seguridad de la información

4 Implementación de seguridad de la información

- Gestión de acceso
- Infraestructuras y tecnologías de seguridad
- Seguridad en la nube
- Procesos y operaciones

Entrega de la seguridad de información para aumentar valor al negocio

Marco Legal, Privacidad y Análisis Forense	Manejar los asuntos legales	Asegurar cumplimiento y protección	Análisis Forense
Gestión de Identidades y Accesos	Asegurar Viabilidad	Planificar para el futuro	Implementar la solución
Infraestructura, Redes y Aplicación	Arquitectura en Seguridad	Gestionar los controles de Seguridad	Asegurar la Información
Estrategia y Gestión de la Seguridad	Definir el entorno	Asegurar la Gestión	Cobertura de la Gestión
Aseguramiento de Riesgo de la Información	Evaluar el Riesgo	Alinear el Proceso	Analizar la brecha
Agenda de seguridad para el negocio	La seguridad como socio estratégico para el negocio	La seguridad como propulsor del negocio	La seguridad como un negocio dirigido

Valor para el negocio

Beneficios derivados del servicio

- Efectividad de costos y prevención de incidentes.
- Conciencia de riesgos y personal enfocado en mitigarlos.
- Confianza generada por la estrategia de seguridad y acciones tomadas.

Selección de sistemas y QA en Implementación

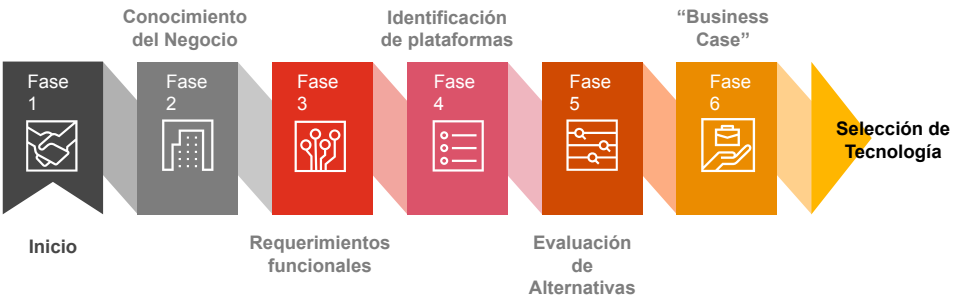
1. SELECCIÓN DE SISTEMAS

Nuestro servicio incluye

- Análisis de situación actual.
- Determinación de situación futura esperada.
- Detección de oportunidades de mejora.
- Diseño de alternativas estratégicas de cambio.
- Detalle de requerimientos funcionales y técnicos.
- Elaboración del Request for information (RFI) y Request for Proposal (RFP) para envío a proveedores.
- Evaluación administrativa, técnica, funcional y económica de alternativas.
- Selección de solución de software y de la tecnología que la soporta.

¿Cómo podemos ayudarte?

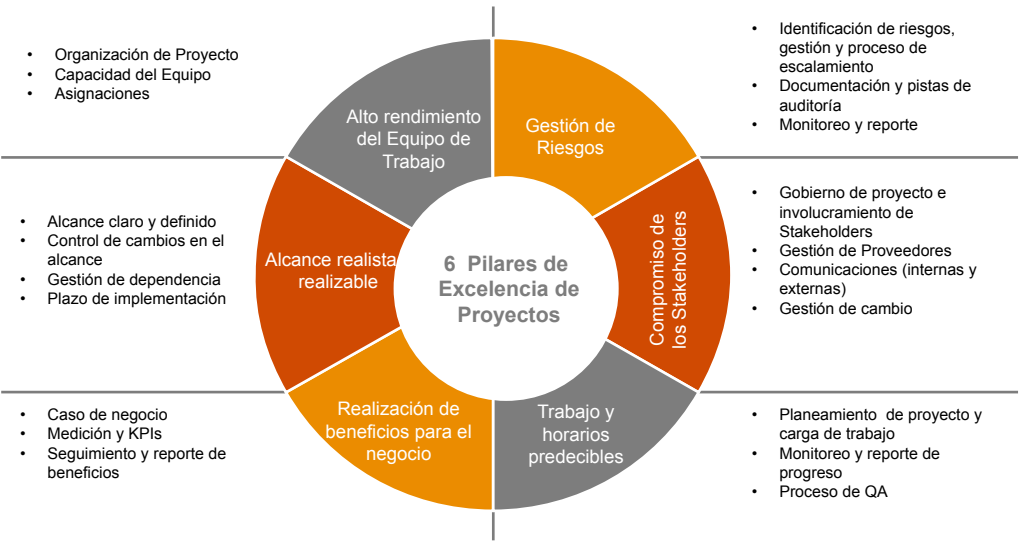
Proceso de Selección de Aplicaciones de Negocio



IT Sourcing®

2. QUALITY ASSURANCE EN IMPLEMENTACIÓN DE SISTEMAS

Quality Assurance de Implementaciones ERP



Beneficios de la selección de sistemas

- Enfoque estratégico y generación de valor al seleccionar tecnología.
- Evaluación especializada de tecnologías disponibles y selección de proveedores.
- Selección de sistemas que le permitan generar eficiencia operativa y financiera.
- Eficacia al realizar inversiones y obtener beneficios esperados.

Beneficios del QA

- Procesos definidos de acuerdo con las posibilidades de la herramienta y consideración de las mejores prácticas.
- Aseguramiento en la calidad del proceso de implementación identificando riesgos y presentando recomendaciones para mitigarlos.
- Intervención de especialistas técnicos funcionales enfocados en contribuir al éxito del proyecto.
- Permanente asistencia en la gestión del proyecto, incrementando la eficiencia e identificando los impactos y beneficios generados.

Plan de Continuidad

Los negocios transformados globalmente, la pandemia COVID-19, disrupciones y mayor uso de tecnologías de la información significan nuevos riesgos de interrupción de negocio. Es importante contar con un plan de continuidad de negocio (BCP) que le permita hacer frente a estos desafíos y ser resiliente.

¿Qué es BPC?

Es un plan que entra en acción frente a eventos que interrumpen la operación del negocio, generando una serie de procedimientos que permiten restablecer las operaciones críticas en el menor tiempo posible. Posteriormente, una vez resuelta la emergencia, se inicia otra serie de procedimientos que apoyan en devolver las operaciones a su normalidad.

Nuestra metodología

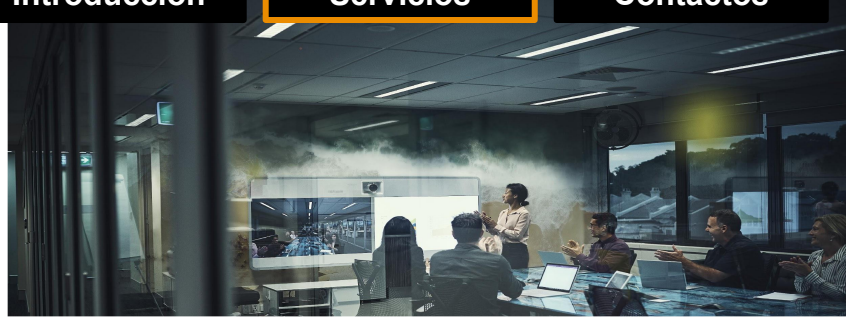
PwC posee una metodología probada de diseño, construcción e implantación de BCP, que utiliza un set integrado de herramientas que aseguran un enfoque consistente en las necesidades de nuestros clientes.

Ciclo de Aseguramiento de la Continuidad del Negocio

Beneficios derivados del servicio

- Fortalecer la capacidad y eficiencia de la gestión de crisis.
- Disminuir las pérdidas e interrupciones para el negocio mediante la continuidad del servicio TI.
- Proteger la información, uno de los principales activos del negocio.
- Proteger la imagen de la organización y evitar pérdidas de clientes.

Modelo de Gobierno y Control de TI



Un adecuado modelo de gobierno de TI permite a las empresas impulsar la mejora del desempeño de la función de TI y lograr una alineamiento estratégico con el negocio, proporcionando marcos de referencia para la toma de decisiones basada en generar valor que apoye el cumplimiento efectivo de los objetivos estratégicos.

¿Cómo podemos ayudarte?

PwC ha desarrollado un marco referencial en el que se ha integrado la gestión de TI orientada al negocio, desde el impacto de factores externos e internos hasta la aplicación del control a la función de TI., permitiéndonos desarrollar un modelo de gobierno adecuado para su empresa.

IT Governance Framework®

El elemento central de nuestro marco de referencia IT Governance Framework® es el marco de Gobierno de TI, que se compone de tres niveles: Gobierno de TI, Gestión de TI y Producción de TI.

Gobierno de TI

Apoyamos a nuestros cliente en el diseño de un marco organizacional apropiado para la función de TI con decisiones, roles y responsabilidades, y definir qué funciones tiene en las áreas de actividad (dominios).

Gestión de TI

Nos aseguramos que la gestión de TI se encamine a tomar decisiones periódicas en el marco de la gobernanza definido, para alinear la función de TI con el negocio y gestionarla de forma sostenida.

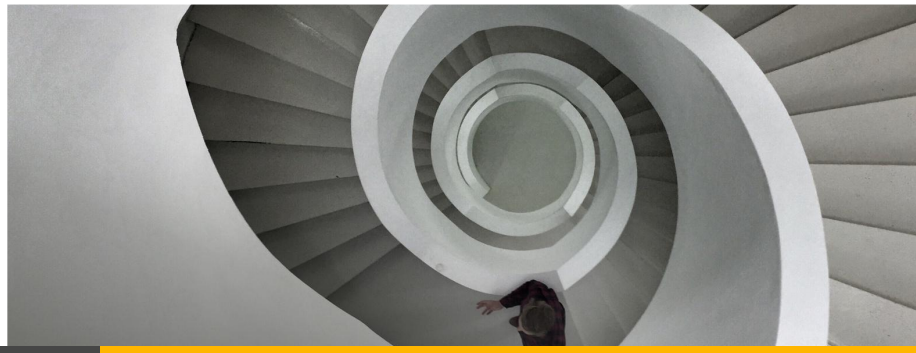
Producción de TI

Las decisiones tomadas (basadas en el modelo de gobierno definido) se representan en la implementación estructurada de proyectos, alineados a estándares, mejores prácticas y el marco de control y operación de TI.

Beneficios de contar con un modelo de gobierno de TI claramente definido

- Fortalecimiento de la alineación de la estrategia de TI a la estrategia de negocio.
- Mejora en la gestión de TI, que genera un incremento del valor del negocio y confianza de socios.
- Incremento de eficiencia en la gestión y operatividad de la función de TI, en todos sus aspectos importantes.
- Adecuada definición de responsabilidades y roles, que permite facilitar y fortalecer la toma de decisiones.

Gestión de Riesgos Tecnológicos



¿Para qué gestionar los riesgos?

Una efectiva gestión de riesgos permite realizar iniciativas tecnológicas de valor para las empresas, que le permita enfrentar y/o anteponerse a los problemas y desafíos que puedan surgir en el uso de la tecnología, incluyendo:

- Los sistemas no cumplen con las expectativas, calidad, eficiencia y objetivos de TI.
- Cuestiones legales relacionadas con sistemas, privacidad y protección de datos.
- Gestionar la privacidad y seguridad de la información.
- Generar confiabilidad a empleados y clientes en el uso de sistemas.
- Falta de habilidad en tomar decisiones, cambiar y aprovechar nuevas oportunidades digitales.
- Asegurar que los proveedores de sistemas y servicios cumplan con la calidad esperada.

¿Cómo podemos ayudarte?

Contamos con una metodología de análisis de riesgos que nos permite evaluar las amenazas y problemas que enfrentan nuestros clientes relacionados a la tecnología, para posteriormente diseñar medidas y acciones que permitan mitigar los riesgos identificados.

Gestión de Riesgos tecnológicos

Nuestro enfoque

Nuestro enfoque especializado IT Risk Diagnostic® nos permite evaluar los riesgos en procesos clave de la función de TI, fortaleciendo el diseño de medidas y consideración de aspectos críticos.

Beneficios derivados del servicio

- Resiliencia empresarial y capacidad de respuesta frente a eventos inoportunos.
- Inversiones en proyectos de tecnología que generan beneficios y consideran desde un principio la mitigación de riesgos.
- Identificación de oportunidades de mejora y optimización en el control de los sistemas.
- Generación de valor y mayor confiabilidad a accionistas, proveedores y clientes.

Evaluación Seguridad ASFI

Verificamos las actividades de control (existencia y efectividad) respecto a los requerimientos establecidos en el **"Reglamento para la Gestión de Seguridad de la Información"** y evaluamos en qué medida el cliente regulado está alineado con lo estipulado por el ente regulador, **durante los doce meses precedentes.**

Ámbito	Descripción
Existencia normativa	Se verificará la existencia y suficiencia de controles (actividades de control) y que los mismos, cumplan al menos los requeridos por el ente regulador (ASFI).
Efectividad operativa	Se verificará la efectividad de los controles (actividades de control) establecidos por la Fundación mediante la selección de muestras para ejecutar pruebas que permitan concluir sobre su efectividad.
Capacidad de capital humano	Se verificará que se cuente con el personal necesario para aplicar los controles identificados
Herramientas de tecnología	Se verificará la existencia de herramientas tecnológicas en los procesos de control (según sea aplicable)

Secciones aplicables del "Reglamento para la gestión de Seguridad de la Información" para la evaluación:

Sección	Descripción
2	Planificación estratégica, estructura y organización de los recursos de Tecnología de la Información (TI)
3	Administración de Seguridad de la Información
4	Administración de Control de Accesos
5	Desarrollo, mantenimiento e implementación de Sistemas de Información
6	Gestión de operaciones de Tecnologías de Información
7	Gestión de Seguridad en Redes y Comunicaciones
9	Gestión de incidentes de seguridad de la información
10	Continuidad del negocio
11	Administración de servicios y contratos con terceros relacionados con Tecnología de la Información
12	Rol de la Auditoría Interna

La estructura del Reglamento de Gestión de Seguridad de la Información, considera:

Evaluaciones SWIFT

El SWIFT Customer Security Controls Framework (CSCF) consta de 3 objetivos principales, 8 principios y 31 controles que constituyen requisitos que deben cumplir las entidades que se conectan a la red SWIFT para reducir el riesgo de ciberataques que afecten al intercambio de mensajes en la plataforma.

El cumplimiento del CSCF no es solo para entidades bancarias, sino para todas aquellas entidades que se conectan a la red de SWIFT

Se debe presentar una certificación anualmente

Todos los usuarios deben dar fe antes de la fecha de vencimiento de la versión de controles actual, confirmando el pleno cumplimiento de los controles de seguridad obligatorios a más tardar el 31 de diciembre, y deben volver a dar fe al menos una vez al año a partir de entonces.

¿Qué sucede si no presento mi atestación?

SWIFT se reserva el derecho de informar a los supervisores locales sobre los usuarios que no hayan certificado el cumplimiento de todos los controles de seguridad obligatorios (o que se conecten a través de un proveedor de servicios que no cumpla con los requisitos).

Usted incumple la política si:

- No tiene una certificación válida: no envió una certificación o su certificación ha caducado
- No cumple con los controles obligatorios
- Se conecta a través de un proveedor de servicios no conforme
- No completó una evaluación externa obligatoria de SWIFT

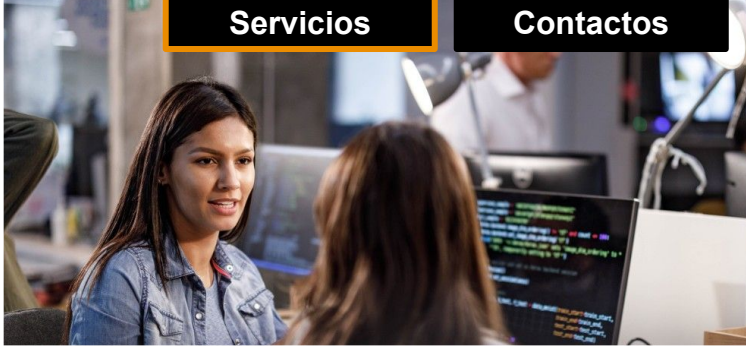
Marco de control CSCF:

01	Asegurar el entorno	• Restringir el acceso a internet • Segregar los sistemas críticos del entorno general IT • Reducir la superficie de ataque y vulnerabilidades • Asegurar físicamente el entorno
02	Conocer y limitar el acceso	• Prevenir el compromiso de credenciales • Gestionar identidades y segregar las funciones
03	Detectar y responder	• Detectar actividad anómala en el sistema o en los registros de transacciones • Planificar la respuesta ante incidentes y la compartición de información

¿Cómo puede ayudar PwC?

- ❖ Evaluación de riesgos y análisis de deficiencias
- ❖ Remediación
- ❖ Pruebas técnicas
- ❖ Certificación y aseguramiento

Evaluaciones Cybersecurity



Nuestra experiencia puede ayudarle a crear operaciones resilientes y reducir el riesgo cibernético. Podemos ayudarlo a obtener la claridad que su negocio necesita para permitirle adaptarse con confianza a los nuevos desafíos y oportunidades.

Nuestros servicios están diseñados para:

- Mejorar la conciencia de seguridad de los miembros del equipo
- Mejorar sus procesos
- Reducir debilidades tecnológicas
- Impulsar posición de seguridad en la nube
- Mejorar continuamente su seguridad

Nuestro equipo de inteligencia de amenazas de nuestra Red Global, recopila información sobre las herramientas, técnicas y procesos utilizados por los atacantes del mundo real.

Utilizamos esta información para evaluar el conjunto completo de controles de defensa, incluidas las áreas de personas y procesos que a menudo se pasan por alto.

Beneficios derivados del servicio

- Nuestros servicios ayudan los miembros de su equipo a tomar acciones apropiadas relacionadas con la seguridad cuando sea necesario.
- Nuestros servicios relacionados con la gestión de riesgos y la gobernanza lo ayudan a mejorar los procedimientos de seguridad con información contextual obtenida del análisis de las fuentes de datos.
- Nuestros servicios de pruebas de penetración aplican metodologías de prueba personalizadas para identificar vulnerabilidades de seguridad y problemas que podrían ser explotados por actores de amenazas del mundo real.
- Nuestros servicios avanzados de pruebas de penetración ayudan a las organizaciones a comprender cómo defenderse de los ataques cibernéticos, cómo obtener acceso a una aplicación crítica o robar credenciales privilegiadas
- Nuestros servicios de seguridad en la nube lo ayudan a establecer las medidas que necesita para la seguridad en la nube. Tenemos en cuenta el perfil de riesgo de su empresa, así como el nivel de protección que necesitan sus sistemas y datos

Gestión de Roles y Perfiles

Si usted ha planificado implementar SAP o ya lo tiene instalado en su organización, PwC lo asesora con el objetivo de que su sistema posea un adecuado diseño de roles y perfiles de accesos indebidos, mejorando la eficiencia y generando un adecuado ambiente de control en su empresa.

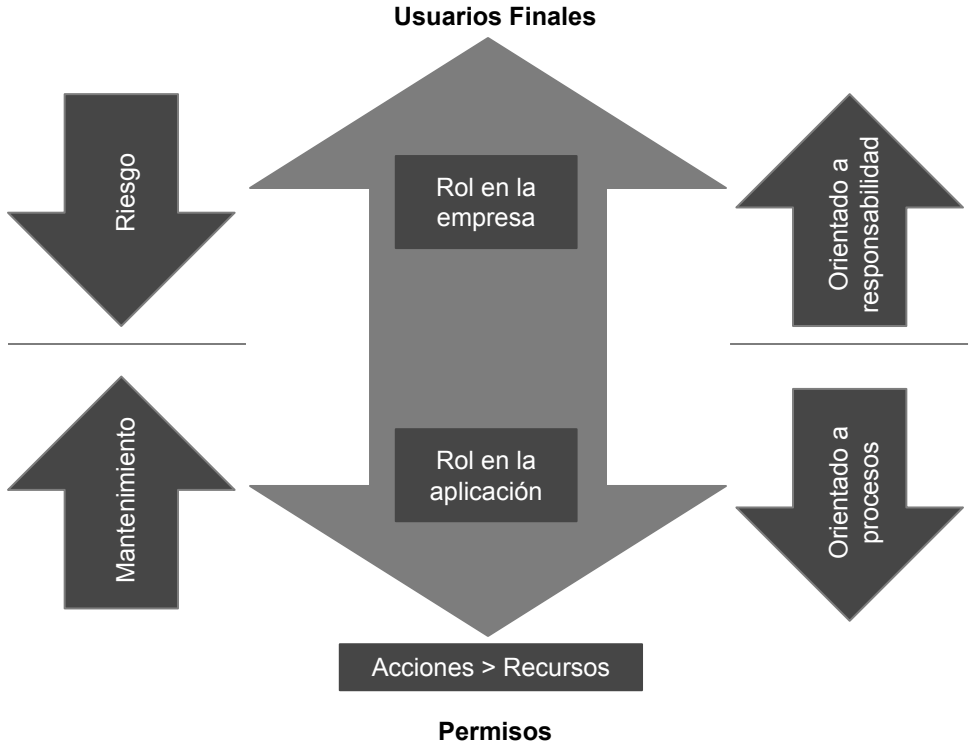
Nuestra visión

Es un hecho comprobado por nuestra firma, en diversos proyectos realizados, que la correcta asignación de roles y perfiles de acceso de SAP en las organizaciones se degrada con el tiempo o nunca fue bien implementada desde un comienzo, sino que se privilegió la puesta en producción del nuevo sistema para cumplir los plazos establecidos.

Una de las actividades críticas para mantener un adecuado ambiente de control y minimizar el riesgo de acceso no autorizado es que se otorgue a los usuarios de la compañía sólo las autorizaciones de acceso que ellos necesitan de acuerdo con el cargo funcional que desempeñan, para así establecer controles apropiados para mantener la integridad global de su sistema SAP.

Beneficios derivados del servicio

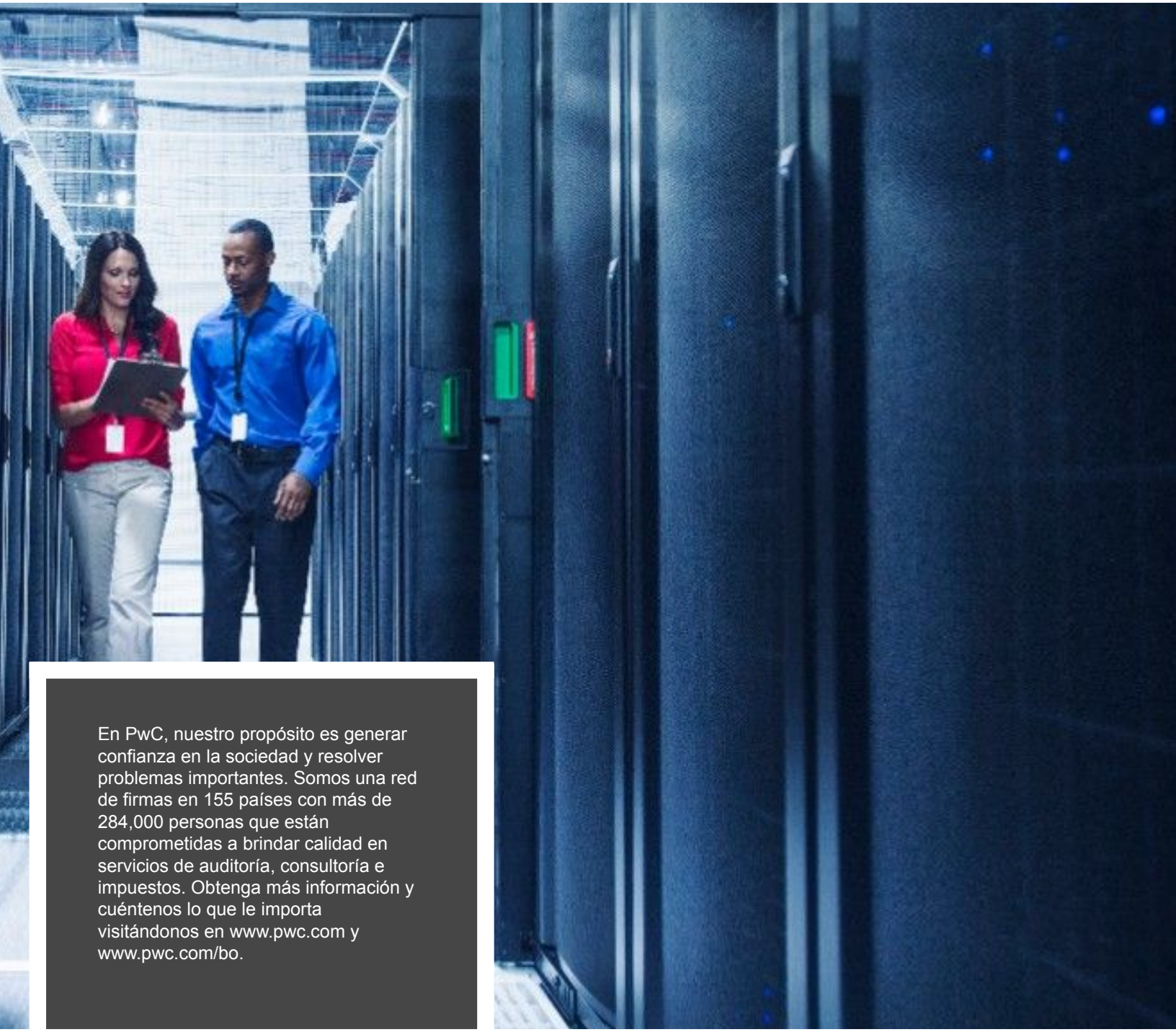
- Compatibilizar los accesos otorgados con las funciones de cada persona.
- Mantener un adecuado nivel de acceso con relación a funciones consideradas críticas y que representan un mayor riesgo para la organización.
- Evitar conflictos de segregación de funciones, por las cuales dos o más funciones, en forma conjunta, no debieran ser accedidas para su ejecución por un mismo usuario.
- Advertir sobre el grado de cumplimiento del licenciamiento para evitar posibles contingencias legales.



Contactos

Sergio Fischer
Socio Líder
sergio.fischer@pwc.com
Tel: (591-3) 344-4311
Calle I, Equipetrol Norte Esq. Viador Pinto, Edif. Omnia Dei piso 1

Erlan Ibañez
Socio de Servicios de Consultoría
erlan.ibanez@pwc.com
Tel: (591-3) 344-4311
Calle I, Equipetrol Norte Esq. Viador Pinto, Edif. Omnia Dei piso 1



En PwC, nuestro propósito es generar confianza en la sociedad y resolver problemas importantes. Somos una red de firmas en 155 países con más de 284,000 personas que están comprometidas a brindar calidad en servicios de auditoría, consultoría e impuestos. Obtenga más información y cuéntenos lo que le importa visitándonos en www.pwc.com y www.pwc.com/bo.

pwc.com/bo