Guía Complementaria

MIPP

Marco Internacional para la Práctica Profesional

GTAG®

Global Technology Audit Guide

Fundamentos de TI para auditores internos

Traducción al Español Auspiciada por:

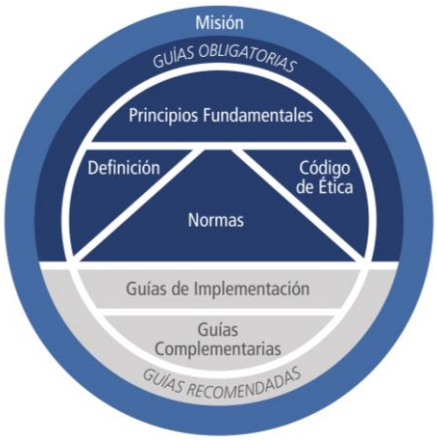
FLAI

FUNDACIÓN LATINOAMERICANA DE AUDITORES INTERNOS

The Institute of Internal Auditors | Global

Acerca del MIPP

El Marco Internacional para la Práctica Profesional® (MIPP) es el marco conceptual que organiza las guías autorizadas emitidas por el Instituto de Auditores Internos (IIA) para los profesionales de auditoría interna de todo el mundo.



Las **Guías Obligatorias** se desarrollan siguiendo un proceso establecido de diligencia debida, que incluye un período de exposición pública para recopilar comentarios de las partes interesadas. Los elementos obligatorios del MIPP son los siguientes:

- Los Principios Fundamentales para el Ejercicio Profesional de la Auditoría Interna.
- La Definición de Auditoría Interna.
- El Código de Ética.
- Las *Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna.*

Las **Guías Recomendadas** incluyen las Guías de Implementación y las Guías Complementarias. Las Guías de Implementación están diseñadas para ayudar a los auditores internos a comprender cómo aplicar y cumplir con los requisitos de las Guías Obligatorias.

Acerca de las Guías Complementarias

Las **Guías Complementarias** proporcionan información adicional, asesoramiento y mejores prácticas para la prestación de los servicios de auditoría interna. Apoyan a las *Normas* al abordar temas puntuales y cuestiones específicas de un sector en mayor detalle que las Guías de Implementación, y cuentan con el aval del IIA a través de un proceso formal de revisión y aprobación.

Guías para la Práctica

Las **Guías para la Práctica** constituyen un tipo de Guía Complementaria que ofrece enfoques detallados, e incluye procesos paso a paso y ejemplos destinados a apoyar a todos los auditores internos. Las Guías para la Práctica se enfocan, entre otros, en los siguientes segmentos:

- Servicios financieros
- Sector público
- Tecnología de la información (GTAG®).

Para ver una descripción general de los materiales de orientación autorizados proporcionados por el IIA, visite www.globaliia.org/standards-guidance.

Contenido

Resumen ejecutivo

En el mundo actual, la tecnología es una parte integral de todas las organizaciones y es lo que sustenta casi todos los datos, todas las transacciones o cálculos y todos los procesos o actividades de negocio. Los auditores internos necesitan contar con un conocimiento básico de los conceptos y operaciones subyacentes de la tecnología de la información (TI). De lo contrario, podrían no comprender cabalmente los objetivos de TI y los riesgos asociados, y podrían no contar con la capacidad de evaluar o auditar el diseño o la efectividad de los controles relacionados.

Esta guía presenta las competencias básicas de TI y los conocimientos que necesita tener todo auditor interno. Asimismo, ofrece análisis y descripciones más completas de las operaciones, estrategias y tecnologías subyacentes de TI. No aborda en detalle los controles de tecnología de la información o cómo auditar la TI, los cuales se analizan en otras guías del IIA. Más precisamente, cubre actividades y conceptos esenciales de TI que todos los auditores internos deben conocer.

Esta guía brinda descripciones generales sobre el gobierno de TI, la relación entre el área de TI y el negocio, y cómo la TI genera valor mediante operaciones continuas, entrega de proyectos, desarrollo de sistemas y soporte, y su supervisión de la calidad y los niveles de entrega de servicios. También cubre aspectos básicos necesarios para tres dominios técnicos críticos: infraestructura, red y aplicaciones, y una revisión general de los desafíos y riesgos aplicables en esas áreas.

Esta guía también tiene como propósito presentar el contenido del Marco de Competencias de TI del IIA (Figura 1) y tratar aspectos de TI cubiertos en el examen de Auditor Interno Certificado (CIA) del IIA, que evalúa el nivel básico de comprensión de TI que los auditores internos necesitan tener.

La guía también explora algunas tendencias y temas emergentes de TI. Los nuevos riesgos y los cambios continuos del panorama de TI forman parte de la naturaleza inherente y evolutiva de la TI. Como se señaló, las actividades específicas de auditoría de TI, los controles generales y de aplicación relacionados con TI y los temas más avanzados sobre riesgos, controles y técnicas de auditoría de TI se tratan en otra guía del IIA, que también puede complementar el estudio del área de TI en preparación para el Examen CIA o para adquirir más conocimientos generales de TI.

Introducción

Esta guía ayuda a los auditores internos a comprender cómo funciona la TI en general y el papel importante que desempeña en el éxito de una organización. La primera sección analiza los objetivos de TI, su relación con la organización y, en general, el **gobierno de la tecnología de la información**. Las demás secciones detallan los fundamentos de tecnologías y procesos de TI específicos que es preciso que los auditores internos conozcan, se especialicen o no en auditoría de TI.

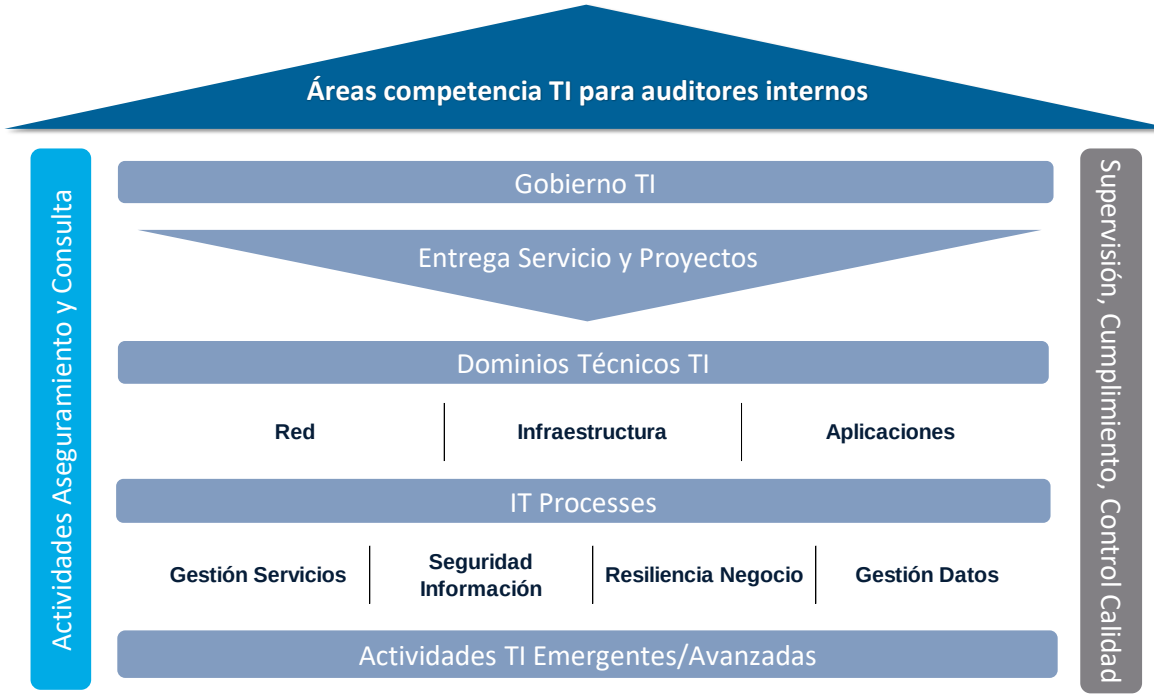
Nota: Los términos en negrita se definen en el glosario del Apéndice B.

Dado que el área de TI es una parte fundamental de toda organización, es crucial que el director ejecutivo de auditoría (DEA) y los auditores internos tengan una comprensión y un conocimiento básicos de la TI y la gestión de los datos críticos en sus organizaciones. La protección de los datos empresariales, el apoyo a las operaciones de TI y la protección de la tecnología son solo algunos de los desafíos que actualmente enfrentan las organizaciones. Si bien estos desafíos pueden parecer abrumadores, quedan más que compensados por las oportunidades potenciales que la TI le brinda a una entidad, pues permite optimizar sus operaciones, innovar en el desarrollo de productos y aprovechar procesos, como el análisis de datos, y tecnologías, como la automatización robótica de procesos (RPA) o la inteligencia artificial (IA).

La TI es imprescindible para la estrategia de una organización, y comprender los impactos que la tecnología puede tener en los procesos de negocio y la gestión de riesgos ayudará a realzar el papel de la auditoría interna como asesor confiable y creador de valor.

La Figura 1 muestra áreas de TI significativas cuyos fundamentos los auditores internos deben conocer.

Figura 1: Competencias de TI del IIA para Auditores Internos



Fuente: Instituto de Auditores Internos.

Conformidad con el Código de Ética y las *Normas* del IIA

Aunque esta guía no entra en detalles específicos sobre la realización de una auditoría de TI, el contenido general ayudará a los auditores internos a cumplir con el principio de competencia del Código de Ética del IIA y múltiples *Normas* del IIA, específicamente la Norma 1200 - Aptitud y cuidado profesional, que establece: "Los **trabajos** deben cumplirse con aptitud y cuidado profesional adecuados", y la Norma 1210 - Aptitud, que establece: "Los auditores internos deben reunir los conocimientos, las aptitudes y otras competencias necesarias para cumplir con sus responsabilidades individuales. La **actividad de auditoría interna** colectivamente, debe reunir u obtener los conocimientos, las aptitudes y otras competencias necesarias para cumplir con sus responsabilidades". Los auditores internos deben tener suficiente conocimiento de los **riesgos** y controles clave de TI y las técnicas de auditoría basadas en tecnología disponibles para realizar el trabajo asignado.

Recursos adicionales

Esta guía hará referencia a Normas de otros órganos rectores. Las *Normas* del IIA se señalarán como tales e incluirán el número de Norma.

Al asignar auditores a un trabajo que puede requerir aptitudes y habilidades específicas, como una auditoría con componentes de TI, la Norma 2230 - Asignación de recursos del trabajo, establece: "Los auditores internos deben determinar los recursos adecuados y suficientes para lograr los objetivos del trabajo, basándose en una evaluación de la naturaleza y complejidad de cada trabajo, las restricciones de tiempo y los recursos disponibles". La interpretación de esta Norma establece que "Adecuado se refiere a la combinación de conocimientos, habilidades y otras competencias necesarias para realizar el trabajo". Fortalecer el conocimiento general de la TI ayudará al departamento de auditoría interna y al auditor interno individual a obtener las habilidades necesarias para realizar auditorías relacionadas con la TI.

Si un departamento de auditoría interna carece de personal con las habilidades necesarias para realizar una auditoría que abarque aspectos del entorno de TI, puede optar por subcontratar o co-contratar los trabajos. Al hacerlo, la actividad de auditoría interna retiene la responsabilidad de la auditoría en su conjunto. La Norma 2340 - Supervisión del trabajo, establece: "Los trabajos deben ser adecuadamente supervisados para asegurar el logro de sus objetivos, la calidad del trabajo y el desarrollo del personal".

Relación con el negocio y gobierno general de TI

La tecnología es compleja y cambia rápidamente; sin embargo, las organizaciones esperan que sus servicios de TI sean seguros, eficientes, confiables, actualizados y rentables.

Esta sección cubrirá la TI entendiéndola como una unidad de negocios multifuncional que es un proveedor de servicios esencial para la organización. La relación entre la organización y el área de TI debe entenderse claramente, y el gobierno de TI debe configurarse de modo que ofrezca valor

a las partes interesadas. Además, la gerencia de TI debe garantizar que los servicios y proyectos de TI entregados sean supervisados para verificar la calidad y el cumplimiento de las leyes y regulaciones, que son cada vez más dispares y dinámicas.

En las actividades de la organización y de los negocios, la TI se ha vuelto indispensable para crear valor, permitir servicios competitivos, innovar y respaldar estrategias críticas, y dar soporte a dispositivos y aplicaciones internos. La TI ya no es un silo de actividad que opera con un contacto limitado entre empleados, clientes y socios. Las interfaces y transacciones de negocio, ya sean de empresa a empresa (B2B) o de empresa a consumidor (B2C), están habilitadas por tecnologías y operaciones de TI, puesto que los dispositivos (por ejemplo, PC, teléfonos móviles, computadoras portátiles, tabletas) son parte de la vida diaria en el trabajo y el hogar.

Habilitación del negocio: el objetivo de la TI

El objetivo primordial de la TI es la habilitación del negocio, que requiere una sólida relación y comprensión de la función de negocios de la organización. La tecnología permite casi todos los procesos de negocio clave y la gerencia de TI debe alinearse con las estrategias de negocio de la organización. Debe haber transparencia entre la organización y el área de TI con respecto a los costos, los niveles de servicio, las opciones y lo que optimiza y proporciona el mayor valor a las unidades de negocios y a la empresa en general.

Debido a su presencia fundamental en la organización y a que opera como un negocio dentro de un negocio, el liderazgo de TI debe tener un "asiento en la mesa" para comprender mejor las iniciativas, estrategias, prioridades y cambios de negocio. El área de TI debe participar en la etapa de inicio de los proyectos para proporcionar información significativa sobre las decisiones de negocio clave que requerirán soporte de TI ya sea en forma directa o indirecta.

El director de información (*chief information Officer,* CIO) debe habilitar a la organización mientras equilibra y optimiza tácticamente la dirección de las estrategias y arquitecturas de TI.

Gobierno de TI

La TI debe administrarse de manera amplia para asegurar la entrega óptima de servicios (como redes, infraestructura y aplicaciones) a la organización y al cliente final. La TI también debe crear valor y respaldar el éxito de la organización. Un buen gobierno de TI ayuda a cumplir estos objetivos. Los elementos y componentes clave del gobierno de TI incluyen:

Recurso

Para obtener más información sobre el proceso de gobierno de TI, consulte la guía GTAG del IIA, "Auditoría del gobierno de TI."

- *Alineación estratégica –* proporciona dirección, servicios, proyectos y objetivos para respaldar los objetivos de negocio de la organización y maximizar el retorno de la inversión (ROI).
- *Gestión de riesgos –* determina que existan los procesos y las políticas para garantizar que los riesgos se aborden adecuadamente.
- *Entrega de Valor –* garantiza que se brinde el máximo servicio de TI en toda la organización.
- *Gestión de Recursos –* proporciona una dirección de alto nivel para la obtención y el uso de recursos de TI para garantizar la capacidad adecuada y supervisar el nivel empresarial de financiación al área de TI.
- *Configuración organizacional –* aborda los roles, funciones y relaciones de reporte necesarias, que permiten que el área de TI satisfaga las necesidades de la organización, y garantiza el abordaje de los requisitos a través de una evaluación formal y la definición de prioridades.
- *Establecimiento de políticas –* garantiza que se implementen las normas, políticas y marcos de la industria para abordar los requisitos regulatorios, de cumplimiento y de riesgo de la organización.

TI como negocio

La TI no es solo un centro de costos, es una función de toda la empresa que actúa como un negocio interno. En la mayoría de las organizaciones, un CIO y/o un director de tecnología (*chief technology Officer,* CTO) son responsables de administrar y garantizar la entrega de servicios de TI y el acceso a los datos en toda la empresa. Las organizaciones también pueden tener un director de seguridad de la información (*chief information security Officer,* CISO) para supervisar la seguridad de TI y, a menudo, un director de protección de datos (*data protection Officer,* DPO) dedicado, un director de datos (*chief data Officer,* CDO) y/o un director de privacidad (*chief privacy Officer,* CPO) para supervisar los datos y aspectos de cumplimiento. Cabe señalar que los últimos tres roles a menudo se encuentran fuera de la organización de TI. La función de estos roles es más importante que el título real, ya que las organizaciones pueden usar diferentes títulos y/o combinar roles.

La gerencia de TI debe comprender la organización a la que da soporte, sus procesos críticos, prioridades y objetivos estratégicos. Los CIO deben considerar a sus pares organizacionales y las unidades de negocio relacionadas como clientes. En muchas organizaciones grandes, la TI sigue un modelo de “asociación” en el que el CIO administra y supervisa múltiples fuentes de proveedores de servicios internos y externos que se espera que brinden una experiencia fluida a la organización.

Como cualquier negocio, los servicios de TI deben entregarse de manera oportuna, confiable, segura y de acuerdo con los requisitos legales y regulatorios. El área de TI también debe proteger los datos y los activos de información contra violaciones de la confidencialidad, integridad y disponibilidad. Esto puede ser un desafío, ya que la mayoría de los equipos de TI admiten dispositivos y aplicaciones internos, así como también se coordinan con proveedores de servicios externos o subcontratados (incluidos los proveedores de "nube") y consultores.

La decisión de realizar tareas internamente en lugar de subcontratar puede ser una cuestión de estrategia empresarial (p. ej., proteger la propiedad intelectual, mantener el control de las actividades básicas o alcanzar economías de escala), requisitos presupuestarios y de personal, o alguna combinación de dichos factores.

Outsourcing de elementos de TI a la nube

El *outsourcing* de elementos de TI a partes externas y/o el uso de la nube es ahora una práctica frecuente, con diferentes modelos y combinaciones para elegir. Los servicios típicos subcontratados total o parcialmente a proveedores externos incluyen: SaaS (software como servicio), PaaS (plataforma como servicio) e IaaS (infraestructura como servicio). En la sección "Red de TI" de esta guía se brindan más detalles sobre la funcionalidad y características de estos modelos de servicio.

Esto refuerza la necesidad de que el CIO administre la TI como un negocio y sea competitivo con otras posibles opciones de fuentes externas de tecnología.

Como parte de la gestión de TI como negocio, la organización de TI debe gestionar y mantener acuerdos de nivel de servicio (*service level agreements,* SLA), proporcionar y supervisar indicadores clave del desempeño (*key performance indicators,* KPI) e indicadores clave de riesgo (*key risk indicators,* KRI) y contratar a administradores de relaciones para gestionar los servicios ofrecidos internamente, externamente y a la organización como cliente.

Desde la perspectiva de la auditoría interna, es preciso comprender cómo se entrega la tecnología en una organización, por quién y para quién, a fin de evaluar la mayoría de los procesos, funciones, sistemas o proyectos. Incluso las evaluaciones estratégicas requerirán una buena comprensión de la tecnología que respalda la dirección del negocio de una organización.

Supervisión de procesos: prestación de servicios de TI y gestión de cartera de proyectos

La función de TI entrega procesos y servicios a la organización a través de operaciones de TI (soporte de procesos de negocios), desarrollo de sistemas, infraestructura de TI y seguridad de la información (SI). Es esencial supervisar la entrega de estos procesos y servicios en colaboración con las gerencias que no son de TI. El gobierno de TI proporciona las estrategias, los mecanismos y las medidas para ofrecer valor de negocio, fomenta una asociación con la organización y ayuda a garantizar el establecimiento y la supervisión de los objetivos de propiedad conjunta.

Además de brindar procesos, servicios e infraestructura de TI clave, la función de TI administra y entrega una cartera de proyectos en apoyo de la organización (es decir, desarrollo o adquisición de software) o en apoyo de la dirección general de TI (es decir, proyectos de infraestructura o diseño de arquitectura). La entrega de proyectos a tiempo, dentro del alcance y conforme al presupuesto es un desafío importante tanto para la función de TI como para la función de negocio.

La supervisión del proceso establece la responsabilidad y ayuda a garantizar que los entregables satisfagan las necesidades de la organización y del cliente.

Supervisión continua: necesidades/actividades de calidad y cumplimiento

La gerencia de TI debe monitorear y asegurar que se entregue el nivel apropiado de calidad a sus clientes y a la organización. Esto incluye no solo el diseño, la entrega y la implementación de servicios que satisfagan el cumplimiento normativo y legal, sino también asegurar los requisitos operativos continuos.

La gerencia de TI debe supervisar que se responda a las necesidades de calidad y cumplimiento de manera general y garantizar la mejora continua y la flexibilidad a medida que cambian los requisitos de negocio. Si bien la calidad y el cumplimiento deben integrarse en todos los procesos y proyectos de TI, ambos deben monitorearse en toda la empresa y en asociación con las expectativas de nivel de servicio del negocio.

El control de la calidad y confiabilidad de los servicios es imperativo para que la gerencia se asegure de que los procesos se gestionen de acuerdo con las expectativas del consejo y la alta dirección. Este aseguramiento no puede proporcionarse sin un seguimiento continuo y una resolución oportuna de las deficiencias operativas y de control.

Desafíos y riesgos para el gobierno de TI y la relación de TI y el negocio

La función de TI requiere un gobierno amplio, alineación con la organización y la necesidad de ser eficiente, confiable y oportuna en la entrega de servicios efectivos a sus clientes. Los auditores internos deben comprender que muchos desafíos y riesgos de TI comienzan en el nivel de gobierno y estrategia, seguidos de una entrega y una supervisión eficaz y competitiva de los niveles generales de servicio y calidad. Los auditores internos también deben tener un conocimiento básico de los desafíos y riesgos comunes de TI al evaluar, examinar o revisar el gobierno de TI y las relaciones con el negocio, que pueden incluir, entre otros:

- *La estrategia y dirección de TI no están alineadas con la estrategia de la empresa u organización.* A menudo, la hoja de ruta tecnológica está diseñada para mejorar el modelo de negocio y las operaciones actuales o se centra en iniciativas de infraestructura de TI, pero no está preparada para habilitar o facilitar posibles objetivos o modelos de negocio futuros. Si no se tiene en cuenta la adaptabilidad y la flexibilidad, podrían plantearse obstáculos a la competitividad y la innovación.

- *El liderazgo de TI no tiene un "asiento en la mesa" cuando se está desarrollando la estrategia de negocio, o no forma parte del proceso de toma de decisiones sobre la dirección comercial y las opciones que se están considerando.* La TI puede quedar excluida en el desarrollo de estrategias de negocio. No propiciar la participación de la seguridad de la información y la TI en las etapas iniciales de planificación podría traducirse en un mayor riesgo de sufrir consecuencias adversas, como costos adicionales, menor desempeño, multas y sanciones regulatorias e incluso una mayor amenaza de exposición indebida de datos/información.
- *El uso de "TI deshonesta".* El concepto de TI fraudulenta, también conocido como "TI en las sombras", se produce cuando alguien en la organización utiliza tecnología que no está autorizada o ni siquiera es conocida por el área de TI. Este es un riesgo significativo cuando una organización tiene múltiples unidades de negocios, ubicaciones, campus o subsidiarias.

  Instancias comunes pueden incluir una unidad de negocios que compra y/o usa aplicaciones o programas (por ejemplo, una macro de Excel), plataformas o infraestructura como servicio para satisfacer mejor sus necesidades percibidas, pero sin consultar a los líderes de TI y/o seguir los protocolos de gobierno adecuados antes de proceder con la implementación. Ya sea que el protocolo adecuado se evite deliberadamente o no, esto indica un gobierno de TI deficiente y una relación subóptima entre la función de negocio y la función de TI. Las unidades de negocio de una organización deben trabajar junto con la función de TI para que toda la organización siga un proceso definido para evaluar, incorporar y administrar hardware y software.

- *La organización percibe la TI como un impedimento para seleccionar la mejor solución u optimizar el abastecimiento de un servicio de TI.* La tensión potencial entre la función de TI y la función de negocio en cuanto a qué servicios se proporcionan mejor de forma interna o externa puede ser un gran desafío. Un método para superar este desafío es que la función de TI indique el costo o asigne tarifas y un retorno sobre la inversión o ROI (potencial de ahorro de costos) por sus servicios y consultas. Otorgar a la organización de TI interna la capacidad de completar una licitación al igual que un proveedor externo, le permite a la organización tener una comparación lado a lado para su elección de trabajar con una solución o servicio de un proveedor externo versus elegir una solución o servicio desarrollado internamente.
- *Las soluciones tecnológicas en uso se encuentran obsoletas o mal mantenidas.* Asegurarse de que el software y los componentes de la infraestructura estén actualizados y sean compatibles es esencial para contar con una operación de TI confiable. Las funciones de negocio y de TI deben cooperar para establecer ventanas de mantenimiento adecuadas para garantizar que las actualizaciones, los parches y otras actividades críticas de actualización se financien y se realicen de manera oportuna. No mantener la tecnología actualizada puede resultar en una "deuda tecnológica": una falta de inversión en TI, ya sea financiera o en actualizaciones, que contribuye a ineficiencias, riesgos (particularmente en torno a la seguridad de la información) u oportunidades perdidas

que pueden acumularse con el tiempo. Los niveles no reconocidos de deuda tecnológica pueden llevar a decisiones mal informadas y, a menudo, son la causa fundamental de problemas operativos o estratégicos. Es posible aceptar, planear o incluso construir deuda tecnológica, pero al hacerlo, los riesgos e impactos deben ser formalmente entendidos y aceptados por la gerencia apropiada.

- *Falta de claridad y/o propiedad del riesgo formal de TI.* Las organizaciones pueden ver los riesgos relacionados con TI como responsabilidad del CIO o de la función de TI. Sin embargo, la mayoría de los riesgos relacionados con TI son propiedad y deben ser aceptados por la función de negocio adecuada. Si se comprende cabalmente quién posee y asume la responsabilidad de los riesgos, la función de negocio tendrá mayor aptitud para financiar los esfuerzos de mitigación de riesgos de TI y asociarse con el área de TI para crear valor y optimizar las decisiones.
- *Gobierno o gestión de proyectos ineficaces o poco efectivos.* Los proyectos de TI críticos para el negocio deben completarse a tiempo, dentro del alcance y conforme al presupuesto. El gobierno de proyectos es fundamental para garantizar que todos los proyectos cuenten con la prioridad y los recursos adecuados, y se entreguen de manera oportuna y eficaz. La gestión de proyectos ayuda a garantizar que los aspectos críticos de cada uno de ellos sean transparentes para todas las partes interesadas, lo que les brinda a los responsables una comprensión clara y precisa del estado, los problemas, los riesgos y los entregables. También significa una gestión más eficaz de la "variación del alcance", o la tendencia a que los requisitos de un proyecto se incrementen con el tiempo.

  Desde una perspectiva de auditoría interna, la participación en la totalidad de los proyectos clave – desde el desarrollo del caso de negocio hasta el seguimiento del proyecto y la entrega final – puede ser un factor crítico de éxito y un valor añadido. Sin embargo, cuando participa en un proyecto de principio a fin, la función de auditoría interna debe mantener su conformidad con la Norma 1100 – Independencia y Objetividad, entendiendo que la dirección es la responsable en última instancia de la toma de decisiones y la entrega. Esta Norma establece que "La actividad de auditoría interna debe ser independiente, y los auditores internos deben ser objetivos en el cumplimiento de su trabajo."

Infraestructura de TI

La infraestructura de TI se refiere al hardware y software que respalda la gestión de la información y los datos de una organización. Los componentes principales de la infraestructura de TI incluyen hardware, software, almacenamiento/bases de datos (DB) y una red. Desde el punto de vista de TI de una organización, es importante considerar la infraestructura como un todo, así como cada elemento como un componente. Esta sección cubre algunos de temas de infraestructura en profundidad y ofrece una descripción general de los componentes principales.

Componentes principales

Hardware de TI

El hardware consta de servidores físicos, máquinas mainframe y periféricos, que generalmente se encuentran en salas de servidores empresariales o centros de datos. Estos pueden estar alojados en las instalaciones, fuera de las instalaciones, subcontratados a un tercero, en la nube o una combinación de estas modalidades. El hardware de TI también incluye dispositivos de usuario final (por ejemplo, computadoras portátiles y de escritorio) que se utilizan para acceder a información y datos empresariales, impresoras, componentes de red y dispositivos de almacenamiento, entre otros. El hardware de una organización suele estar conectado a una red de TI.

Sistemas Operativos (OS)

Un sistema operativo (OS) es una colección de programas (código fuente) que administran los componentes de computadoras y las operaciones de computación para ofrecer un resultado para el usuario. El software del sistema operativo proporciona un medio para administrar y acceder a los recursos de hardware de TI y actúa como interfaz o plataforma entre el usuario final y el hardware en la red. Algunos tipos incluyen:

- Sistemas operativos de servidor, que están diseñados para procesar las solicitudes de varios equipos de usuario final en la red de TI de la empresa. Ejemplos: IBM AS/400, Windows Server o Red Hat Linux.
- Sistemas operativos de cliente, que generalmente admiten un solo usuario y están diseñados para dispositivos de usuario final. Ejemplos: Windows y Mac OS, así como sistemas operativos portátiles o móviles.
- El firmware, a diferencia de los sistemas operativos estándar, tiene el código incrustado en el hardware. Es común ver firmware en dispositivos como electrodomésticos, dispositivos médicos o enrutadores y firewalls de código abierto.

Software Empresarial y de Aplicación

El software empresarial, a veces llamado software de planificación de recursos empresariales (*enterprise resource planning,* ERP), permite a una organización captar y conectar la información y el contenido de sus diversos procesos de negocio y promueve decisiones de gestión eficientes por parte de la organización. El software de nivel empresarial incluye SAP, Oracle ERP, Microsoft Dynamics, JD Edwards ERP y otros.

El software de aplicación es un software específico para casos de uso y, por lo general, realiza una sola función e incluye programas de procesamiento de texto, hojas de cálculo y software de procesamiento de gráficos.

Almacenamiento y Bases de Datos

Los repositorios de la información de negocios de una organización, administrados con frecuencia por software especializado, permiten a los usuarios de la red acceder y, cuando sea necesario, modificar y adjuntar información empresarial.

La Red

Una red es dos o más componentes de hardware de TI conectados con el fin de compartir información.

Servidores

Un servidor es un programa o dispositivo informático que proporciona funcionalidad para otros programas o dispositivos, denominados clientes. Los diferentes tipos de servidores incluyen servidores web, servidores de bases de datos, servidores de archivos, servidores de impresión y servidores de aplicaciones, entre otros. También se conoce comúnmente como servidor el hardware real (computadora física), que generalmente es una computadora poderosa con la capacidad de procesar grandes cantidades de datos y, a menudo, se dedica a una función específica, como el correo electrónico de la organización, archivos, aplicaciones, etc. y/o sitio web. En el contexto empresarial general, un servidor puede describir el software o el hardware, pero es más probable que describa la combinación de los dos, ya que ambos son necesarios para proporcionar funcionalidad.

Sistemas Operativos de Servidor

Los servidores más comunes en la actualidad ejecutan el sistema operativo Windows patentado de Microsoft, IBM AS/400 o Linux, un sistema operativo de código abierto modificable.

La figura 2 describe varias características de los dos sistemas operativos.

Figura 2: Comparación de los Sistemas Operativos Windows y Linux

	Windows OS	Linux OS
Licencia	■ Todas las instancias de sistemas operativos propiedad de Windows deben tener licencia.	■ Algunos sistemas operativos basados en Linux vendidos por proveedores pueden tener una tarifa de licencia asociada.
Experiencia de usuario	■ Interfaces de texto de usuario (TUI) e interfaces gráficas de usuario (GUI).	■ Interfaces de texto de usuario (TUI) e interfaces gráficas de usuario (GUI).
Acceso al código fuente	■ Microsoft Windows es un sistema operativo propietario. Este modelo le da a Microsoft una ventaja competitiva en el mercado. ■ El público en general no tiene acceso al código fuente del sistema operativo de Microsoft.	■ El sistema operativo Linux está construido con tecnologías de código abierto. Esto significa que el código fuente puede ser inspeccionado, estudiado, modificado, mejorado y distribuido por cualquier persona.

Seguridad	■ La seguridad del sistema operativo Windows se centra en tres áreas: o Gestión de identidades y accesos: permisos, propiedad de objetos, herencia de permisos, derechos de usuario y auditoría de objetos. o Protección contra amenazas: protege los puntos terminales de las amenazas cibernéticas, detecta ataques avanzados y violaciones de datos, automatiza los incidentes de seguridad y mejora la postura de seguridad. o Protección de la información: aborda las amenazas de robo de datos o la exposición de computadoras perdidas, robadas o dadas de baja de manera inapropiada.	■ Debido a su naturaleza de código abierto, los usuarios pueden revisar el código fuente e identificar cualquier debilidad de seguridad. ■ En comparación con el sistema operativo Windows, el sistema operativo Linux generalmente tiene menos vulnerabilidades de seguridad y tiene menos estructuras desprotegidas.

Mainframes

Un mainframe es una computadora (hardware) diseñada para albergar las bases de datos comerciales, servidores de transacciones y aplicaciones que requieren un mayor grado de seguridad y disponibilidad que el que se encuentra comúnmente en máquinas de menor escala. Estas máquinas siguen siendo de uso popular por parte de grandes organizaciones debido a su confiabilidad y estabilidad.

Los mainframes procesan grandes cantidades de datos, como estadísticas de países e industrias, y tareas similares que implican un procesamiento de transacciones masivas y de gran volumen. Industrias como la banca y los seguros dependen de los mainframes para procesar el enorme volumen de transacciones generado por la industria financiera. En sectores como el cuidado de la salud, el transporte y los servicios públicos, los mainframes ayudan a procesar grandes volúmenes de datos y brindan soporte para los estrictos requisitos de cumplimiento.

Los mainframes suelen ser el tipo de infraestructura preferido cuando se requieren grandes volúmenes de usuarios simultáneos. La industria de la aviación y los viajes aéreos es un buen ejemplo porque las reservas en línea y las agencias de viajes, las simulaciones de vuelo y los sistemas de navegación requieren aplicaciones de gran ancho de banda y dependen en gran medida de las capacidades de los mainframes.

Hay dos conceptos principales de procesamiento de transacciones para mainframes: procesamiento de trabajos por lotes y procesamiento de transacciones en línea:

- Los trabajos por lotes se procesan sin la intervención del usuario; consiste en el procesamiento de grandes volúmenes de información a granel en lugar de entradas individuales. Los lotes, que a veces pueden incluir cientos o miles de transacciones, suelen estar pre-secuenciados para ejecutarse en una ventana de tiempo específica durante los períodos de menor actividad. Los resultados de los trabajos procesados por lotes suelen ser resúmenes de información, como ventas diarias, procesamiento de pedidos y actualizaciones de inventario.

- El procesamiento de transacciones en línea (*online transaction processing,* OLTP) se aplica a datos que generalmente requieren una respuesta inmediata y en tiempo real, y la interacción del usuario con el mainframe suele ser muy breve y simultánea con el procesamiento. OLTP es beneficioso para los servicios que deben estar disponibles continuamente y donde la integridad de los datos y la información son de gran importancia. Este concepto se aplica a transacciones en cajeros automáticos y compras con tarjeta de crédito o débito.

Algunos de los principales fabricantes de mainframes son IBM y Fujitsu.

Sistemas Operativos de Mainframe

Debido a la gran cantidad de datos que procesa un mainframe, sus componentes internos, incluida la memoria interna, la capacidad de procesamiento, los periféricos internos y externos, el almacenamiento y el sistema operativo, deben ser lo suficientemente eficientes y complejos como para ofrecer un estándar de rendimiento confiable.

Cada fabricante tiene su versión de un sistema operativo, que se configura y personaliza para adaptarse al hardware y las interfaces del fabricante (por ejemplo, z/OS es el sistema operativo para mainframes de IBM).

Virtualización

La virtualización es el proceso de configurar un sistema informático en un entorno que está separado del hardware real. Antes del concepto de virtualización, todos los sistemas operativos se instalaban en el hardware de la computadora real, y esa computadora solo podía ejecutar un sistema operativo. Con el concepto de virtualización, el sistema operativo de la máquina virtual (VM) se ejecuta en el hardware de la computadora y varios sistemas operativos virtualizados pueden ejecutarse bajo el control de esa máquina virtual. Los recursos informáticos comunes, como servidores, escritorios, sistemas operativos, archivos, almacenamiento o redes, se pueden virtualizar. Las máquinas virtuales se pueden usar para fines específicos y descartarse una vez que se haya cumplido con ese uso.

Este entorno virtualizado generalmente se logra mediante la instalación y el uso de software especializado (llamado hipervisor) en la máquina host que emula un entorno virtualizado. Un hipervisor es un conjunto de software específico que crea y ejecuta máquinas virtuales y también se conoce como monitor/administrador de máquina virtual o VMM. Hay dos tipos de hipervisores: el tipo 1, que se ejecuta directamente como sistema operativo en el hardware de la máquina host, también conocido como tipo "*bare metal*", y el tipo 2, que se ejecuta en un entorno de sistema operativo ya establecido y se conoce como "alojado".

Directorio de Servicios

Todas las redes de computadoras tienen recursos de TI asociados, como usuarios, impresoras, dispositivos de almacenamiento, archivos y carpetas, máquinas de fax y más. Por lo tanto, tiene sentido que cada uno de estos recursos esté asociado con una dirección de red única.

Un servicio de directorio es un servicio del sistema operativo que proporciona una lista de nombres de los recursos de TI de la red asociados (por ejemplo, usuarios, impresoras, dispositivos de almacenamiento, archivos y carpetas) y la dirección de red única de cada uno. Mantener estos directorios es importante desde el punto de vista del acceso y la seguridad.

Inicialmente se desarrolló un estándar (o protocolo) referido a servicios de directorio para administrar información en una red global de recursos. Este protocolo se denominó protocolo X.500. Basados en el estándar X.500, los proveedores de software desarrollaron soluciones patentadas para administrar dispositivos de red relacionados con sus sistemas operativos correspondientes. Una solución de servicio de directorio común es *Active Directory* (AD) de Microsoft, para su uso con el sistema operativo Windows. AD tiene una funcionalidad adicional incluida con el estándar X.500, y los administradores pueden agregar nuevos usuarios, eliminar o modificar elementos de red, especificar privilegios de uso y seguridad, administrar políticas de contraseñas y otras tareas.

Un ejemplo de un protocolo de directorio de código abierto es *light directory access protocol* (LDAP), que se deriva del estándar X.500. LDAP se utiliza para acceder a información de red almacenada de forma centralizada, pero es más simple y requiere menos recursos. Cuando se usa LDAP, la información de recursos de red para una organización se puede almacenar y administrar en una ubicación centralizada.

En un entorno Linux donde se requiere flexibilidad y personalización, se utilizan con frecuencia soluciones LDAP de código abierto como OpenLDAP. Sin embargo, el uso de soluciones de código abierto en un entorno Linux presenta algunos inconvenientes, como la necesidad de personal específicamente capacitado; autenticación ralentizada cuando se utilizan grandes repositorios LDAP, y posible incompatibilidad del sistema con algunos dispositivos, aplicaciones y aplicaciones web.

Almacenamiento de Datos

Normalmente se utilizan tres formas principales de almacenamiento de datos: bases de datos, *data warehouses* y *data lakes*. Las bases de datos son las más comunes y se analizan en detalle a continuación. La diferencia entre las tres formas de almacenamiento se puede describir por la fuente y el tipo de datos:

- *Base de datos* – repositorio de fuente única; pueden ser datos estructurados o no estructurados.
- *Data warehouse* – múltiples fuentes de datos almacenados en un solo repositorio. Normalmente, datos estructurados que se pueden recuperar fácilmente para un propósito definido.
- *Data lake* – múltiples fuentes de datos almacenados en un solo repositorio. Los datos no están estructurados y no se pueden recuperar fácilmente.

Base de Datos

Una base de datos es un conjunto de datos que permite una fácil recuperación y actualización. Hay dos tipos principales de bases de datos: bases de datos relacionales y no relacionales.

Las bases de datos relacionales presentan estas características:

- Múltiples conjuntos de datos organizados en un esquema de tablas con filas y columnas.
- Relaciones claramente definidas entre las tablas.
- Útil para administrar grandes almacenes de datos transaccionales y relacionados.
- Los modelos de seguridad de datos permiten a los usuarios ver solo lo que están autorizados a ver.
- Puede consultarse (analizarse) utilizando *structured query language* (SQL) simple y en formato tabular, por lo general con software de base de datos patentado.

Las bases de datos no relacionales o no solo SQL (NoSQL) presentan estas características:

- Conjuntos de datos organizados en grupos y en formato no tabular.
- Alojan datos no estructurados en un entorno moderno de *big data*.
- Diseño simple para diferentes tipos de datos (por ejemplo, series de tiempo, contactos, medios).

Los sistemas de administración de bases de datos relacionales (*relational database management systems,* RDBMS) son plataformas que permiten a los usuarios actualizar, crear, agregar y eliminar datos de tablas dentro de una base de datos relacional. Las plataformas RDBMS suelen ser propietarias y requieren el uso con licencia de la plataforma. Algunas plataformas RDBMS típicas son Microsoft SQL Server, IBM DB2, Oracle Database, MySQL y Microsoft Access.

SQL es un lenguaje de base de datos utilizado por las plataformas RDBMS para interactuar con (consultar) datos en tablas. Un ejemplo se muestra en la Figura 3.

Figura 3: Ejemplo de una consulta SQL

```
SELECCIONE * DE Miembros DONDE Edad> 30
```

En este ejemplo, se seleccionan todas las entradas de una tabla llamada "Miembros" en la que su edad, indicada por las entradas en la columna "Edad", es superior a 30.

Una base de datos NoSQL es una categoría de sistemas de gestión de bases de datos no relacionales. Estas bases de datos no se ajustan al modelo "relacional" de una base de datos, dado que presentan un aumento significativo en la carga de trabajo de la base de datos y un enfoque típico sería actualizar el hardware para cumplir con las expectativas de rendimiento. Hay un

impacto de tiempo y costo de este enfoque, que se conoce como "ampliación". "Escalar horizontalmente" se refiere a distribuir grandes cargas de trabajo de bases de datos a varios hosts a medida que aumentan las cargas de trabajo. Las bases de datos NoSQL son populares entre las entidades que tienen elementos de datos grandes y variados y desean "escalar" de una manera más eficiente.

En el Apéndice G se proporciona una comparación de las bases de datos SQL y NoSQL.

Mensajería

La mensajería en el contexto de esta guía se refiere a la creación, el intercambio, el uso y la gestión de la transferencia de información empresarial a través de una red de TI. Las organizaciones modernas utilizan una variedad de herramientas de mensajería con soporte interno y externo para comunicarse internamente, con socios comerciales y con los clientes.

Una de las formas más comunes de mensajería informática es el correo electrónico, que en esencia es un mensaje enviado desde una computadora y recibido por otra a través de una red. El correo electrónico y el concepto de mensajería en general han evolucionado con el tiempo para incluir elementos como texto, imágenes y archivos adjuntos, y muchas organizaciones abren sus redes a herramientas de mensajería pública, como Skype o Zoom.

Protocolos de Mensajería

Se han desarrollado varios protocolos (reglas de transferencia de mensajes) para administrar y gobernar la transferencia de mensajes entre computadoras en una red. Hay una serie de protocolos relacionados con los mensajes que determinan cómo se envían, reciben y ponen en cola los mensajes. Una forma fácil de pensar en un protocolo es considerarlo similar a un idioma. Para que dos dispositivos se comuniquen, deben establecer las reglas de idioma que seguirán.

Como se menciona en el apartado Enrutadores y conmutadores de la sección Conceptos y componentes de red, las reglas de cómo se envían y reciben los datos a través de una red son definidas por TCP/IP, el protocolo básico que da soporte a la comunicación por Internet, y que sirve de base para todos los demás protocolos.

Simple mail transfer protocol (SMTP) es el protocolo que rige cómo se envían y reciben los mensajes de correo electrónico. Los mensajes deben colocarse en cola porque los usuarios no están necesariamente disponibles inmediatamente para consumirlos.

Los mensajes se consumen mediante uno de los dos protocolos de cola: *post office protocol* (POP) e *internet message access protocol* (IMAP):

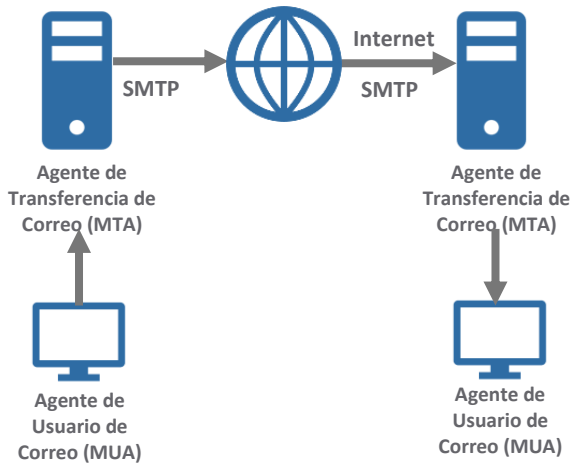
- Los mensajes POP se reciben y almacenan en un servidor de correo electrónico. Cuando estos mensajes se consumen, se descargan en el dispositivo del consumidor. Los mensajes no se conservan en el servidor una vez consumidos.

- Los mensajes IMAP se reciben y se conservan en un servidor de correo electrónico. Cuando estos mensajes se consumen, se pueden organizar en varias carpetas en lugar de descargarlos en el dispositivo del consumidor. Los mensajes se conservan en el servidor una vez consumidos, por lo que IMAP se puede considerar como un servidor de archivos para mensajes.

Dominios y Participantes de Correo Electrónico

Prácticamente todas las organizaciones tienen un dominio de correo electrónico único (el contenido que viene después del símbolo @ en una dirección de correo electrónico), que se considera un dominio local. Este dominio local se administra a través de un servidor de correo, también conocido como *mail (message) transfer agent* (MTA). Este servidor puede ser administrado por la organización o por un tercero o un servicio en la nube (Figura 4).

Figura 4: Proceso típico de entrega de correo electrónico



Fuente: Instituto de Auditores Internos.

El correo electrónico se redacta y envía mediante un cliente de correo electrónico, que puede ser una aplicación basada en la web, como Gmail, o una aplicación dedicada en la computadora de un usuario, como Microsoft Outlook. El cliente de correo electrónico también se denomina *mail user agent* (MUA).

Cuando un usuario envía un correo electrónico, lo transmite al MTA, que recopila y distribuye el correo electrónico interno (mensajes dentro del mismo dominio). También distribuye el correo electrónico saliente a usuarios externos (fuera del dominio).

A cada usuario de correo (*mail user,* MU) se le asigna una dirección de correo electrónico única, con el formato de usuario@dominio.com. Esto corresponde a un "buzón" al que el MTA entregará todos los mensajes entrantes. El MTA también etiquetará todo el correo saliente del buzón con la dirección de correo electrónico única del usuario.

Filtros de Spam

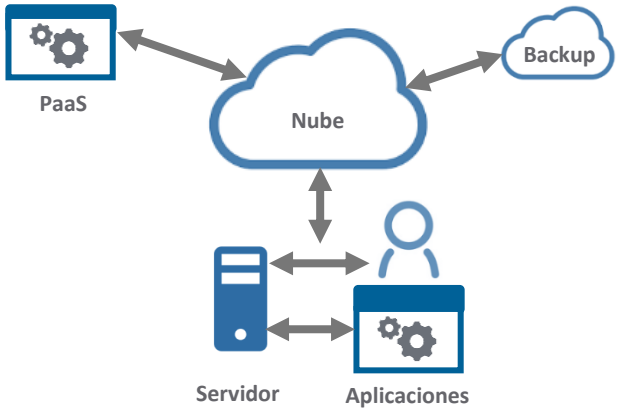
Los MTA utilizan filtros de correo no deseado (*spam)* o monitores de correo para detectar comunicaciones no deseadas. Los filtros de correo no deseado intentan identificar y redirigir el correo electrónico no deseado o no solicitado. Los filtros de spam requieren un mantenimiento casi constante debido a la naturaleza del método de filtrado. Con frecuencia, se producen falsos positivos que permiten que el correo electrónico no deseado llegue al buzón de un usuario y el correo electrónico legítimo a veces se redirija a una carpeta de correo no deseado. Los filtros de

spam reconocidos tienen capacidades antivirus sofisticadas para limitar la amenaza de virus. Los monitores de correo notifican al usuario de un nuevo correo electrónico y permiten a los usuarios identificar mensajes legítimos y sospechosos.

Archivos Compartidos

Antes de la Internet y los dispositivos en red, los usuarios compartían archivos mediante disquetes. Con la llegada de protocolos como *file transfer protocol* (FTP) y s*ecure file transfer protocol* (SFTP) (mencionado en el apartado Protocolos de la sección Red de TI), el intercambio de archivos se volvió más fácil, pero no necesariamente amigable para el usuario. El intercambio de archivos permite a los usuarios compartir fácilmente archivos como libros, música, fotos o de cualquier otro tipo en formato electrónico, ya sea de forma pública o privada, a través de Internet (Figura 5).

Figura 5: Ejemplo de Plataforma Comercial Típica para Compartir Archivos



Fuente: Instituto de Auditores Internos

Las plataformas comerciales para compartir archivos, como Dropbox, Microsoft One Drive, Google Drive, Microsoft SharePoint, Apple iCloud y otras, suelen tener parámetros o restricciones sobre el tipo de uso compartido de archivos (es decir, permisos). Los archivos compartidos se pueden crear, leer, actualizar o eliminar, según el tipo de permisos que se les asigne. Las organizaciones deben tener en cuenta que muchas de estas herramientas requieren poca o ninguna licencia, y en lo que respecta a la retención y destrucción de datos, una organización podría tener poco control de dónde residen sus datos (generalmente en la nube) o cuánto tiempo se retienen.

No obstante, las plataformas comerciales de intercambio de archivos han invertido recursos para la seguridad de archivos y usuarios en cada paso del proceso. Las funciones de seguridad pueden incluir autenticación de doble factor, permisos de usuario, cifrado de archivos y, en algunos casos, cumplimiento de regulaciones como las disposiciones, en los Estados Unidos, de la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA) para la atención médica y de la Autoridad Reguladora de la Industria Financiera (FINRA) para la industria de servicios financieros, y en Europa, de las Autoridades Europeas de Valores y Mercado (ESMA). Es importante que las organizaciones estén al tanto de cualquier problema legal, regulatorio o de seguridad sobre el uso de cualquiera de estos servicios. Se recomienda contar con una política para compartir archivos.

Dispositivos Móviles

Muchas organizaciones permiten que sus empleados conecten un dispositivo personal a la red de la empresa, lo que brinda al empleado la oportunidad de llevar menos dispositivos. También proporciona a la organización un potencial ahorro de costos al no tener que comprar dispositivos adicionales. Si bien esta práctica, conocida como "traiga su propio dispositivo" (*bring your own device,* BYOD) o "traiga su propia tecnología" (*bring your own technology,* BYOT), ofrece eficiencias, puede presentar posibles problemas de seguridad. (Para los propósitos de esta guía, nos referiremos a ambos conceptos, BYOD y BYOT, como BYOD).

Sistemas Operativos Móviles

Los sistemas operativos móviles son el software de nivel primario que permite a los dispositivos móviles administrar sus propios componentes internos e interactuar con el usuario del dispositivo. El sistema operativo móvil controla la entrada en el dispositivo móvil desde varias fuentes (por ejemplo, pantalla táctil, micrófono, cámara, GPS) y permite a los usuarios interactuar con el dispositivo a través de aplicaciones cargadas en él.

Los sistemas operativos móviles más comunes son Apple iOS y Android, pero hay otros, como los sistemas operativos Windows Mobile, Symbian y Blackberry de Microsoft. Aunque estos pueden no ser tan frecuentes como iOS o Android, las organizaciones deben estar al tanto del uso de estos otros sistemas operativos si permiten que sus empleados traigan sus propios dispositivos, ya que cualquier dispositivo conectado a la red de una organización puede presentar riesgos de seguridad.

La naturaleza de código abierto del sistema operativo Android implica que los fabricantes de dispositivos y los proveedores de red pueden realizar cambios en el sistema operativo por muchas razones, incluida la optimización de dispositivos y redes. Este enfoque en capas puede tener un impacto significativo en la seguridad y las funciones del sistema operativo Android. Por otro lado, Apple controla estrictamente el entorno iOS. El código fuente no se comparte con los proveedores de red y Apple envía actualizaciones a sus dispositivos.

Gestión de Dispositivos Móviles y Gestión de Aplicaciones Móviles

La gestión de dispositivos móviles (*mobile device management,* MDM) es un software que permite a una organización controlar las funciones de un dispositivo (por ejemplo, teléfonos inteligentes, tabletas, lectores electrónicos, dispositivos portátiles) para proteger y hacer cumplir las políticas. Esto permite a las organizaciones gestionar una gran cantidad de sus dispositivos móviles de forma coherente y escalable. MDM también permite a la organización limpiar de forma remota cualquier dispositivo que se pierda o se vea comprometido. El inconveniente de esto es la flexibilidad de usuario limitada resultante en el dispositivo móvil corporativo.

La gestión de aplicaciones móviles (*mobile application management,* MAM) describe el software y los servicios responsables del aprovisionamiento y la gestión del acceso a las aplicaciones móviles (desarrolladas internamente o disponibles comercialmente) ya sea que se apliquen a dispositivos móviles propiedad de la organización o BYOD. MAM también tiene el beneficio adicional de poder limitar el intercambio de datos corporativos entre aplicaciones.

El enfoque principal de MDM y MAM es controlar la exposición de las aplicaciones corporativas, el correo y los documentos confidenciales, y mantener la integración con otros activos tecnológicos corporativos (por ejemplo, computadoras portátiles, impresoras). Además, las políticas de seguridad pueden integrarse y aplicarse en el nivel de la aplicación corporativa y es posible que no dependan de la seguridad a nivel del dispositivo o los parches del sistema operativo. Esto implica que se requieren pruebas constantes de las aplicaciones MAM para garantizar la compatibilidad con las actualizaciones del sistema operativo a nivel de dispositivo.

Las organizaciones deben considerar una política apropiada de administración de dispositivos móviles y una política BYOD.

Desafíos y riesgos de infraestructura

La infraestructura de una organización es la columna vertebral de sus operaciones de TI. Cuando se configura bien, puede ayudar a maximizar la eficiencia. Cuando no está optimizada, puede presentar riesgos y desafíos innecesarios. La infraestructura es un componente clave que un auditor interno debe comprender para todos los trabajos relacionados con TI. Existen numerosos desafíos/riesgos relacionados con la infraestructura de TI de una organización que pueden incluir, entre otros:

- *Configuración –* cuando los sistemas operativos y las aplicaciones asociadas (empresa y usuario final) no están configurados de forma segura, pueden existir vulnerabilidades.
- *Seguridad –*
  - El desarrollo o la gestión inadecuados de las excepciones de seguridad pueden permitir la obsolescencia del dispositivo.
  - La gestión de acceso o cifrado deficiente o fragmentado puede permitir un acceso excesivo, especialmente cuando la clave no cambia después de que la persona a la que se le asignó ya no está en posición de necesitar acceso. Además, existe el riesgo de exposición de datos cuando la clave caduca y no se asigna una nueva clave de manera oportuna.
  - Los dispositivos agregados a la red sin el refuerzo (seguridad) adecuado pueden aumentar el riesgo de compromiso debido a protocolos abiertos, contraseñas predeterminadas y falta de monitoreo.
  - Una capacitación en seguridad obsoleta o genérica aumenta el riesgo de que los usuarios sucumban a las tácticas de ingeniería social.
  - BYOD puede provocar la fuga de datos de los dispositivos en la red cuando los procesos internos no se siguen correctamente.

- Las reglas faltantes, desactualizadas o colocadas incorrectamente pueden permitir a actores maliciosos eludir controles como listas de control de acceso (ACL) y reglas de firewall.

- *Conformidad* – Es posible que no se sigan los marcos, normas o metodologías reconocidos por la industria, lo que introduce un potencial riesgo regulatorio o de cumplimiento.
- *Parches* – Si los parches no se aplican a los sistemas críticos, pueden ocurrir vulnerabilidades y problemas de seguridad en la infraestructura de TI.

Recurso

Para obtener más información sobre la administración de parches, consulte IIA GTAG, "Gestión del Cambio de TI: Crítico para el éxito de la organización, 3.° edición".

Red de TI

Definición de red

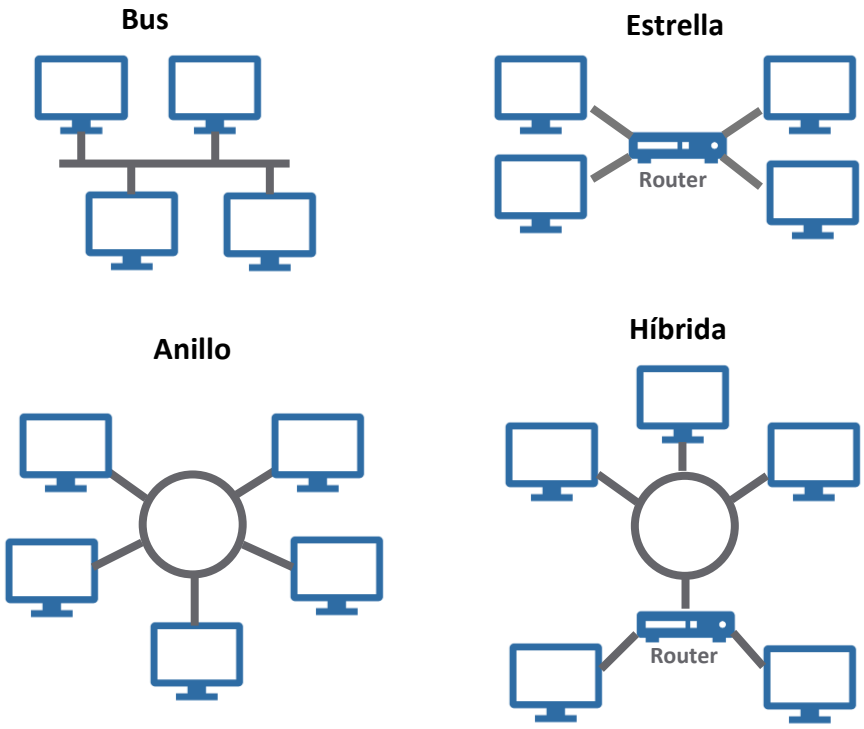
La definición más simple de una red en el contexto de TI es la siguiente: medio para conectar dos o más computadoras con el propósito de compartir información. Una red generalmente tiene tres características clave: topología, arquitectura y protocolos. Esta sección explica cada uno y ofrece ejemplos. También presenta conceptos que incluyen el modo de servicio en capas, el acceso a la red remota y la defensa de la red.

Hay tres tipos principales de redes: redes de área local (LAN), redes de área metropolitana (MAN) y redes de área amplia (WAN). El tamaño y la huella geográfica de una organización determinarán normalmente qué tipo es el más adecuado. Las LAN se utilizan para comunicarse dentro o entre los pisos de un edificio; las MAN están destinadas a comunicarse entre los edificios dentro de un campus o ciudad; y una WAN permite la comunicación dentro de múltiples ciudades, estados o incluso países. Cualquier sistema o dispositivo, como una PC, una computadora portátil o un dispositivo móvil, que se conecta a una red se denomina nodo.

Topología

La topología de una red describe cómo está organizada física y lógicamente. Las topologías de bus, estrella, anillo o híbridas, como se muestra en la Figura 6, son ejemplos comunes.

Figura 6: Ejemplos de Topología de Red



Fuente: El Instituto de Auditores Internos

Arquitectura de Red

La arquitectura de red proporciona un contexto para comprender la estructura de TI de una organización y hay varios tipos de arquitectura entre los que elegir.

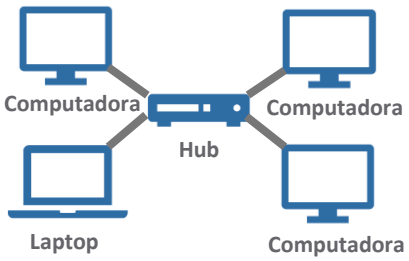
Peer-to-peer

La arquitectura *peer-to-peer*, o P2P, se utiliza normalmente para servidores de red o sistemas de usuarios finales más pequeños, y a veces se la denomina red de intercambio de archivos de aplicaciones distribuidas. La aplicación distribuida se refiere a software o aplicaciones que se ejecutan en varios nodos dentro de la red.

Una arquitectura P2P indica que no existe una jerarquía en la red. Las tareas se realizan y los datos se comparten entre los miembros de una red (nodos) a través de un concentrador o *hub*. Si bien algunos nodos pueden ser más potentes debido a diferencias de hardware o contener datos diferentes debido a su propósito, el diseño de la red P2P ofrece los mismos privilegios o niveles de autoridad entre todos los nodos.

En una red P2P, los nodos pueden comunicarse directamente entre sí, lo que le da a esta arquitectura una mayor flexibilidad en el diseño de aplicaciones distribuidas. Esta arquitectura ofrece resiliencia al cambio y a interrupciones, ya que las dependencias entre los nodos pares son bajas. Una estructura P2P simplifica las capas de servicios (consulte el modelo de siete capas OSI en la Figura 11), al simplificar los diseños de conexión entre nodos.

Figura 7: Modelo de red *peer-to-peer*



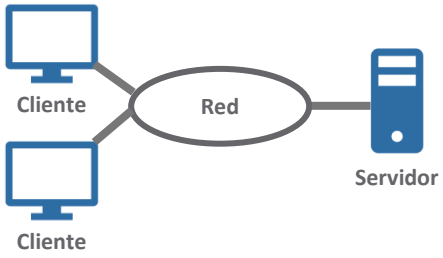
Fuente: Instituto de Auditores Internos

Una LAN, por ejemplo, podría configurarse como una arquitectura P2P, como se muestra en la Figura 7.

Cliente-servidor

La arquitectura cliente-servidor es un modelo basado en una jerarquía de servicio. Los clientes o nodos individuales (es decir, una computadora en una red) solicitan servicios de los servidores. A continuación, el/los servidor/es proporciona/n el servicio o los servicios al cliente. Este método es beneficioso por sus aspectos de seguridad. Por ejemplo, los servidores de autenticación (es decir, inicio de sesión) utilizan una jerarquía para dar acceso seguro a los recursos de la red. Un cliente proporciona credenciales a un servidor de inicio de sesión y recibe un token o clave de acceso.

Figura 8: Modelo de red cliente-servidor

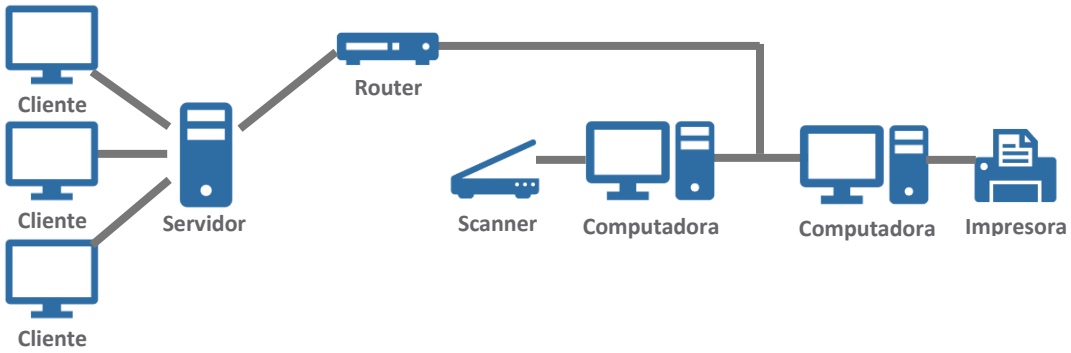


Fuente: Instituto de Auditores Internos

Por ejemplo, una LAN se puede configurar como una arquitectura cliente-servidor, como se muestra en la Figura 8.

Un solo nodo puede ser tanto cliente como servidor, lo que puede ofrecer facilidad de planificación y comprensión en implementaciones de red a pequeña escala o basadas en la ubicación.

Figura 9: Arquitectura de Red Híbrida



Fuente: Instituto de Auditores Internos

Híbrida

La arquitectura de red híbrida, como se muestra en la Figura 9, como su nombre lo indica, es una combinación de los tipos de *peer-to-peer* y cliente-servidor. A excepción de las redes más pequeñas, rara vez existe una red P2P o una red cliente-servidor pura y, funcionalmente, todas las redes ofrecen modelos de servicios híbridos, según los servicios necesarios. Un solo nodo puede usar los servicios de un servidor en la red mientras participa con un par nodo en un sistema de archivos distribuido también en la red y envía información a un cliente, todo en la misma red.

Funcionalmente, la arquitectura de red es más que un sistema de conexiones entre nodos. La demanda de computación moderna ha avanzado rápidamente y las redes requieren el control centralizado de una arquitectura de servicio de cliente en algunos casos, pero también necesitan la flexibilidad de las relaciones P2P abiertas en otros casos.

Basada en la nube

En un modelo tradicional "en las instalaciones" (*on-premise)*, la organización es responsable de todos los aspectos de la red, incluida la propiedad y el mantenimiento de todos los servidores, el almacenamiento, los sistemas operativos, el desarrollo y el mantenimiento de las aplicaciones. Los servicios basados en la nube ofrecen una alternativa a este modelo.

Según el Instituto Nacional de Estándares y Tecnología (NIST), "la computación en la nube es un modelo para permitir el acceso a la red bajo modalidad a pedido, en forma conveniente y ubicua, a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y publicar rápidamente con un mínimo esfuerzo de gestión o interacción con el proveedor de servicios" a través de Internet.[1]

1. Peter Mell, Tim Grance, "La Definición del NIST de Computación en la Nube", Laboratorio de Tecnología de la Información del NIST, Centro de Recursos de Seguridad Informática, SP 800-145, septiembre 2011. https://csrc.nist.gov/publications/detail/sp/800-145/final.

En este modelo, una organización contrata a un proveedor externo que ofrece servicios basados en la nube. Una arquitectura basada en la nube puede combinar o simplificar algunas de las relaciones de la red y ofrece flexibilidad para el destinatario del servicio en la nube.

Hay tres tipos generales de servicios en la nube en los que el tipo de servicio puede denominarse "'X' como servicio", abreviado XaaS. XaaS significa "entrega (u otra cosa) como servicio: productos, servicios y tecnologías". Los tres tipos generales de servicios en la nube incluyen Infraestructura (IaaS), Plataforma (PaaS) o Software (SaaS). Los detalles de cada uno de estos modelos, en comparación con el modelo local tradicional, incluyen:

- *On Premise o local, en las instalaciones* – la organización es responsable de todos los aspectos de la red, incluido el mantenimiento de todos los servidores, el almacenamiento, los sistemas operativos y el desarrollo y mantenimiento de las aplicaciones.
- *Infraestructura como Servicio (IaaS)* – la organización es propietaria del mantenimiento de los servidores dentro de la nube. Este es un modelo de pago por uso para redes, servidores, almacenamiento, aplicaciones, etc., donde el tamaño se puede modificar según sea necesario. La organización receptora es responsable de todas las configuraciones lógicas y el mantenimiento, aunque normalmente no tienen acceso al hardware. Las organizaciones que desean sus propias características y funcionalidades a menudo usan IaaS para desarrollar aplicaciones personalizadas sin la necesidad de albergar la infraestructura. En este caso, el proveedor de IaaS, como Amazon Web Services (AWS), Microsoft, Google o IBM, proporciona una plataforma en la que las organizaciones pueden desarrollar rápidamente sus aplicaciones.
- *Plataforma como Servicio (PaaS)* – proporciona herramientas de hardware y software (plataforma) para crear software y aplicaciones. Esta estructura es adecuada para organizaciones que desean alojar y ejecutar aplicaciones en la nube sin tener que administrar la infraestructura (es decir, almacenamiento, actualizaciones, O/S). Los proveedores de PaaS incluyen, entre otros, Microsoft Google y AWS.
- *Software como Servicio (SaaS)* – una aplicación entregada por la nube disponible a través de Internet, generalmente por una tarifa fija. Este modelo permite la mayor flexibilidad a la organización receptora. Los proveedores de SaaS incluyen Google Apps, Netsuite, Salesforce.com, ServiceNow, Workday, Dropbox y DocuSign, entre otros.

Aunque los proveedores externos usan estos términos para comercializar y explicar sus servicios y enfoques, también puede usarlos el departamento de TI de una organización si provee dichos servicios.

El término "nube" describe cómo se almacenan los datos y la información y se accede a ellos a través de la Internet, pero de manera simple, es el uso de la red informática de otra persona. El uso del término nube es un reconocimiento de que la arquitectura de red es en gran medida irrelevante para la mayoría de los consumidores de servicios de TI, desde los sistemas de TI organizacionales hasta los usuarios individuales. La Figura 10 muestra los modelos *on-premise* y en la nube y las responsabilidades correspondientes típicas. Sin embargo, algunas de estas

responsabilidades pueden variar según el caso, y la organización casi siempre es responsable del aprovisionamiento, el acceso y la autenticación de los usuarios.

En general, desde el punto de vista de la responsabilidad, una organización suele ser responsable de la seguridad "en" la nube, mientras que el proveedor de la nube es responsable de la seguridad "de" la nube.

Figura 10: Arquitectura de Nube Típica por Tipo y Responsabilidad

Premisa	IaaS	PaaS	SaaS
Aplicaciones	Aplicaciones	Aplicaciones	Aplicaciones
Seguridad	Seguridad	Seguridad	Seguridad
Base de datos	Base de datos	Base de datos	Base de datos
Sistemas operativos	Sistemas operativos	Sistemas operativos	Sistemas operativos
Virtualización	Virtualización	Virtualización	Virtualización
Servidores	Servidores	Servidores	Servidores
Almacenamiento	Almacenamiento	Almacenamiento	Almacenamiento
Red	Red	Red	Red
Centros de Datos	Centros de Datos	Centros de Datos	Centros de Datos
Clave:	Gestionado por la Empresa	Gestionado por el Proveedor de Nube	

Fuente: Instituto de Auditores Internos

Modelo de Red de Servicios en Capas

> Para ver más detalles sobre el Modelo OSI de 7 Capas, ver Apéndices D y E.

En lo que a redes se refiere, ayuda a conceptualizar las diferentes "capas" de red si se usa un modelo. A veces denominado colectivamente *network stack* o pila de red, el modelo de capas de red más utilizado es el modelo de siete capas de interconexión de sistemas abiertos (*Open Systems Interconnection,* OSI), que se muestra en la Figura 11.

Figura 11. El modelo OSI de 7 capas

Como muchos conceptos de TI, este modelo no es universal, pero puede resultar útil cuando se piensa en los servicios proporcionados por una pila de red. La mayoría de los sistemas operativos proporcionan una pila de red que contiene una serie de aplicaciones que permiten conexiones

remotas y envío/recepción de datos a dispositivos remotos. Cada capa tiene una responsabilidad y opera independientemente de otras capas. Además, cada capa acepta datos del nivel superior y realiza sus funciones requeridas antes de pasarlos a un nivel inferior. Esto se conoce como pasar información por la "pila de red" y permite a los desarrolladores suponer que los servicios necesarios habrán sido proporcionados por capas inferiores. También requiere que los servicios que desarrollan proporcionen una interoperación estable "en la pila".

La información transmitida desde una capa superior suele estar intacta. Puede dividirse o combinarse según sea necesario en la nueva capa porque todos los datos del nivel superior son simplemente un campo de datos. Se agrega información de control llamada metadatos (datos sobre datos); a estos metadatos se les suele llamar encabezado o *header*.

Partes de esta guía harán referencia a las diferentes capas.

Protocolos de Red

El protocolo de una red es un formato acordado para intercambiar o transmitir datos entre sistemas (o hacia arriba y hacia abajo en la pila de la red). Los protocolos definen una serie de parámetros acordados, como el método para comprimir los datos, el tipo de verificación de errores a utilizar y los mecanismos para que los sistemas indiquen cuando han terminado de recibir o transmitir datos. Una analogía simple es una conversación telefónica en la que el destinatario de la llamada dice "hola" al contestar la llamada, y la persona que llama responde "hola", estableciendo un protocolo de voz (hablando en un idioma acordado).

Algunos protocolos de red comunes incluyen Ethernet, *Transmission Control Protocol/Internet Protocol* (TCP/IP), *File Transfer Protocol* (FTP), *Hypertext Transfer Protocol* (HTTP) y *Secure Sockets Layer* (SSL). Las descripciones simples de cada uno están disponibles en el Apéndice F.

Algunas versiones de estos protocolos tienen una seguridad o encriptación adicional, que se indica con la letra "S", como SFTP, FTP a través de una conexión *Secure Shell* (SSH) o HTTPS. Es importante que una organización comprenda los requisitos de protocolo de seguridad aplicables en relación con las regulaciones, las políticas y las normas de gobierno (por ejemplo, NIST, la Norma de Seguridad de Datos [DSS] de la Industria de Tarjetas de Pago [PCI]).

Muchos profesionales de TI a menudo hablan en términos de protocolos que implementan las funciones requeridas por la capa. También se ofrece una lista de algunos de los protocolos utilizados en cada capa como "protocolos (o medios) que implementan esta capa". Los protocolos de ejemplo no son exhaustivos, pero pueden ayudar a identificar recursos de información o equivalencias y proporcionar contexto. La Figura 12 muestra algunos de los protocolos comunes que se utilizan en cada capa.

Por ejemplo, los servicios web se realizan en la capa HTTP (capa 7). Además, cuando se analizan los componentes de la red (descritos en la siguiente sección), a menudo se los identifica como "que funcionan" en una capa específica.

Figura 12: Modelo OSI con Protocolos de Ejemplo

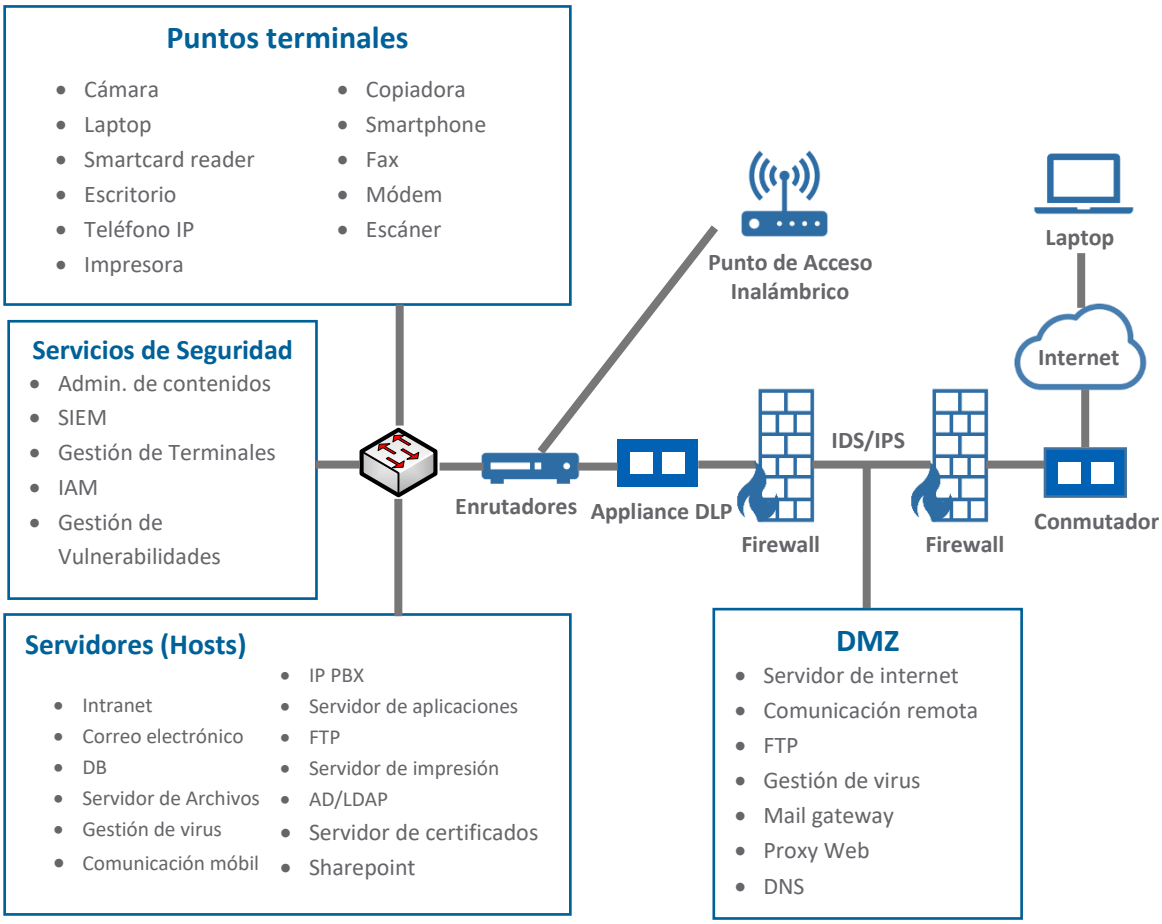
El Modelo OSI de Siete Capas

Capa	Nombre	Protocolos de Ejemplo
Capa 7	Capa de Aplicación	HTTP, SMTP, POP3, FTP, Telnet, Email
Capa 6	Capa de Presentación	SSL, TSL, JPEG, GIF
Capa 5	Capa de Sesión	NetBIOS, SAP
Capa 4	Capa de Transporte	TCP, UDP
Capa 3	Capa de Red	IPv4, IPv6, IPsec, IP
Capa 2	Capa de Enlace de Datos	Ethernet, PPP, ATM, Fiber, MAC Address, VLAN
Capa 1	Capa Física	Cables, Conectores, Hubs (T1, ISDN), USB, Bluetooth

Componentes y conceptos de la red

Una típica arquitectura de red en la mayoría de las organizaciones tendría varios de los componentes que se muestran en la Figura 13.

Figura 13: Componentes de una arquitectura de red típica



Fuente: Sajay Rai.

Nodos y Hosts de Red

Un *host* o "host de red" es una computadora u otro dispositivo conectado a la red capaz de comunicarse con otros hosts. Puede ser un cliente o servidor y puede existir como una arquitectura de pares o híbrida, pero siempre tendrá una dirección de Protocolo de Internet (IP). Como se mencionó, un nodo se define como cualquier sistema o dispositivo conectado a la red, incluidos enrutadores y conmutadores, pero un nodo no siempre necesita una dirección IP. El software de red del host implementa varios protocolos que realizan las funciones de cada capa del modelo de siete capas OSI. La "pila" completa de servicios de red está disponible en un host.

Enrutadores y Conmutadores

Un enrutador (*router)* es un dispositivo de capa 3 (capa de red) que transmite datos entre redes. Los datos se envían en forma de paquetes (datos empaquetados para ser transferidos dentro de una red). Los servicios como LAN virtual (vLAN), Firewalls de filtrado de paquetes y otros servicios de red se pueden integrar en los enrutadores.

Un conmutador (*switch)* es un dispositivo de red de capa 2 (enlace de datos) que conecta nodos dentro de una red con medios físicos como cables de cobre. Un conmutador recibe, procesa y transmite datos a dispositivos de destino específicos a través de tramas, que son grupos de datos similares a los paquetes utilizados en el protocolo TCP/IP en capas superiores. Los conmutadores solo envían mensajes a los nodos previstos. La funcionalidad del conmutador se puede incluir en los enrutadores, por lo que el dispositivo se puede llamar conmutador o enrutador según la función que se esté analizando. Aunque confuso para algunos, en realidad es útil porque los conmutadores y enrutadores independientes pueden tener funciones superpuestas.

Los conmutadores de capa 3, o "conmutadores multicapa", crean circuitos virtuales para transmitir datos entre nodos. El uso de un conmutador de capa 3 reduce la latencia de la red porque el paquete fluye a través del conmutador en lugar de tener el paso adicional de pasar por un enrutador. Normalmente, implementar un conmutador de capa 3 para la Internet corporativa o para establecer una vLAN, mientras que utilizarían un enrutador si necesitaran tráfico para atravesar la WAN. Los conmutadores de capa 7 integran capacidades de enrutamiento y conmutación, que normalmente se utilizan para equilibrar la carga entre un grupo de servidores. Los conmutadores también se conocen como conmutadores de contenido, web o aplicaciones.

Firewalls

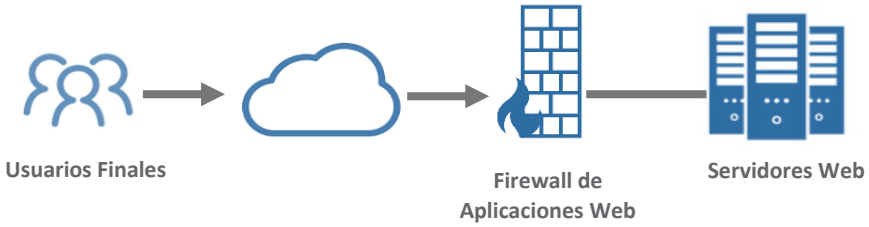
Un cortafuegos o *firewall* es un sistema de seguridad de red que monitorea y controla el tráfico entrante y saliente en base a reglas y configuración de seguridad predeterminadas, y está diseñado para evitar el acceso no autorizado hacia y desde una red privada. Las organizaciones deben asegurarse de que el acceso al firewall esté restringido, y los conjuntos de reglas y la configuración de los firewalls deberían revisarse periódicamente. Cada conjunto de reglas debe tener la documentación adecuada para su propósito y la identificación de su propietario/solicitante.

Hay muchos tipos de firewalls, cada uno con un propósito específico, y las organizaciones pueden tener varios tipos según sus necesidades únicas. Los firewalls básicos inspeccionan la información del encabezado de la capa de red (Capa 3) y la capa de transporte (Capa 4). A veces se les llama filtros de paquetes, ya que eliminan los datos provenientes de direcciones IP prohibidas (capa de red) o destinados a puertos prohibidos (capa de transporte). Si el paquete no está bloqueado, pasa a su destino dentro de la red protegida por el firewall.

Los *stateful firewalls* inspeccionan los paquetes y pueden bloquear los potencialmente maliciosos que no forman parte de una conexión establecida o que no cumplen las reglas para iniciar una conexión legítima. Los firewalls de la capa de aplicación, o los firewalls de próxima generación (NG), interceptan el tráfico de paquetes y decodifican los datos desde la pila hasta la capa de aplicación (Capa 7).

Los firewalls móviles proporcionan comunicaciones seguras cuando el acceso a la red se inicia por un dispositivo móvil. Los firewalls de aplicaciones web (WAF) analizan el tráfico que entra y sale de una aplicación, y se pueden colocar entre los servidores web y la Internet para detectar y proteger las aplicaciones web de ataques conocidos de aplicaciones web, como se muestra en la Figura 14.

Figura 14: Ejemplo de colocación de firewall de aplicaciones web



Fuente: Instituto de Auditores Internos

A través de una configuración, se puede implementar seguridad adicional para rechazar destinos con reputación cuestionable. Las herramientas de seguridad, como los firewalls, pueden interceptar paquetes, inspeccionar la información del encabezado o incluso reconstruir los datos originales de la pila para inspeccionarlos en busca de amenazas de seguridad.

IDS/IPS

Los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS) son dispositivos o aplicaciones de software que monitorean el tráfico de la red en busca de indicios de compromiso o intento de compromiso de un sistema. Los conjuntos de reglas IDS e IPS pueden ser muy grandes y cada regla puede requerir calibración y configuración de umbral para garantizar la integridad del sistema, como la prevención de falsos positivos. Las aplicaciones IDS e IPS bien calibradas y supervisadas pueden aumentar en gran medida la capacidad de una organización para detectar y detener ataques.

Las alertas generadas por un IDS generalmente se recopilan en un sistema de gestión de eventos e información de seguridad (SIEM). Las alertas se pueden correlacionar con la información del flujo de tráfico de la red (flujos netos) y las herramientas de seguridad perimetral, como los firewalls. Las alertas de IDS se comparan con las reglas de IPS; si hay una coincidencia, el IPS y/o el software diseñado para detectar posibles violaciones de datos y/o la prevención de fugas de datos/información (DLP/ILP), ejecutarán una regla para detener una actividad.

Puntos de Accesso Inalámbrico (AP)

Un punto de acceso inalámbrico (AP) proporciona acceso inalámbrico a una red. Los AP modernos brindan opciones para el cifrado, o para codificar y asegurar los datos transmitidos, pero debido a que el mundo tecnológico avanza tan rápidamente, los sistemas a menudo no logran mantenerse al día con los actores maliciosos que intentan anular las funciones de cifrado para sus propios - generalmente (o con frecuencia) criminales o maliciosos - propósitos.

Los entornos corporativos logran el acceso a la red inalámbrica mediante la transmisión de señales de radio entre hosts y puntos de acceso. Un AP proporciona una gama de opciones para la arquitectura de capa 1 del servicio inalámbrico. Dependiendo de la antigüedad del equipo utilizado, se pueden usar varios tipos de encriptación, o una organización puede optar por no usarla. Sin

embargo, esto puede exponer a la organización a un riesgo adicional y el costo de actualizar los componentes de la red inalámbrica para aumentar la seguridad es relativamente económico.

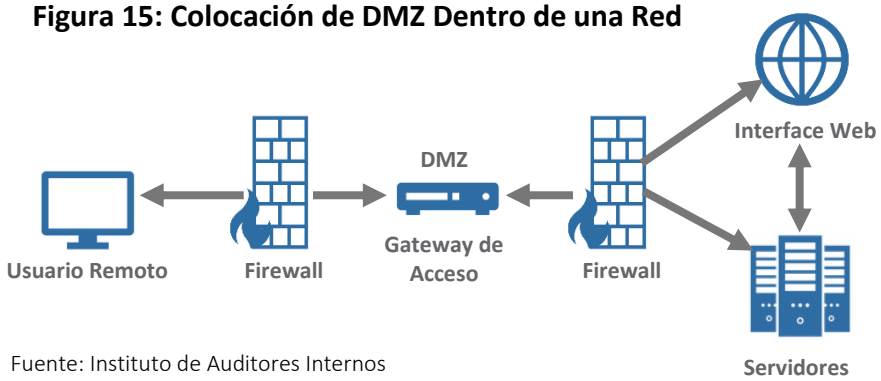
Actualizar el equipo o la configuración de toda la base de usuarios para utilizar protocolos de cifrado más nuevos puede ser una tarea muy grande. Aquí se presenta una breve lista de varios protocolos de encriptación inalámbricos, desde el menor hasta el mayor nivel de encriptación.

- *WEP (Wired Equivalent Privacy):* un protocolo de seguridad obsoleto que ofrece cifrado básico. Este protocolo se utiliza normalmente porque puede ser la única opción para infraestructuras más antiguas. Desde el punto de vista de la seguridad, dado el tráfico suficiente e incluso la potencia informática marginal en una computadora portátil o dispositivo móvil, WEP puede ser fácilmente penetrado y fue reemplazado por el protocolo WPA por la *Wi-Fi Alliance* en 2003.
- *WPA (Wi-Fi Protected Access):* reemplazó a WEP como un protocolo de seguridad más seguro para redes inalámbricas. Al igual que WEP, WPA solo debe usarse si lo requiere una infraestructura anterior porque es vulnerable y proporciona menos cifrado que sus sucesores.
- *WPA2 (Wi-Fi Protected Access 2):* protocolo de seguridad requerido actualmente en todos los dispositivos considerados Wi-Fi CERTIFICADOS por la *Wi-Fi Alliance*, que proporciona algoritmos de encriptación más fuertes que los predecesores. Ofrece un grado de seguridad contra el acceso no autorizado.
- *WPA3 (Wi-Fi Protected Access 3):* proporciona cifrado de datos individuales, protege algunos dispositivos de "Internet de las cosas" (IoT), protege contra ataques de fuerza bruta (método de prueba y error), de diccionario (uso de palabras de diccionario para adivinar contraseñas) y ofrece el más alto nivel actual de cifrado.

DMZ: Una Aplicación de Seguridad

Una zona desmilitarizada (DMZ) es una parte de la red contenida entre dos firewalls y protege a los servidores externos de la organización. El primer firewall está "orientado hacia el exterior" o está sujeto a la Internet, y protege los sistemas DMZ. El firewall que mira hacia el exterior tiene más exposición que el segundo firewall, que protege la red interior. La Figura 15 muestra un ejemplo de DMZ y su ubicación.

Figura 15: Colocación de DMZ Dentro de una Red



Fuente: Instituto de Auditores Internos

Acceso remoto a la red

Hay numerosas opciones de acceso remoto disponibles para las organizaciones, determinadas por factores como los requisitos de seguridad, las expectativas del usuario, las capacidades técnicas y las necesidades de negocio. La necesidad de acceder a las redes corporativas es el resultado de que la fuerza laboral actual se vuelve más móvil; para seguir siendo productivos, los usuarios necesitan un acceso constante a la red. Esto incluso puede requerir una conexión desde una red pública no segura, como un punto de acceso público.

La mayoría de las soluciones implementadas por organizaciones requieren algún tipo de seguridad para garantizar que las conexiones remotas sean seguras. Los controles de seguridad suelen adoptar la forma de autenticación multifactor (MFA) (a veces denominada autenticación de dos factores (2FA)) o cifrado, o ambos. MFA/2FA significa que además de ingresar una contraseña, un usuario debe ingresar un token o una clave que se actualiza periódicamente (por ejemplo, un número de varios dígitos o un "token" único se envía al teléfono móvil de un usuario remoto y debe ser utilizado para completar el acceso al sistema de una organización).

Acceso Remoto: Red Privada Virtual (VPN)

Una VPN extiende una red privada a través de una red pública y permite a los usuarios enviar y recibir datos como si estuvieran conectados a través de una red privada. Proporciona los beneficios de las características de funcionalidad, seguridad y administración de una red privada. Las organizaciones deben asegurarse de que todo el acceso a VPN esté verificado y autenticado para evitar el acceso remoto no autorizado a la red de la organización (p.ej., MFA).

El acceso remoto presupone inherentemente una conexión insegura de Capa 2 a 4. Cuando se utiliza una VPN, antes de que se envíen los datos, la capa de sesión (Capa 5) proporciona un "túnel" cifrado para transferir datos. Esta es una medida de seguridad importante para la organización, en caso de que una persona que no sea un empleado obtenga acceso a los datos, todo el contenido encapsulado y, en algunos casos, incluso la información de transmisión, se encuentran encriptados. El sistema interno que recibe estas conexiones y descifra el contenido se denomina punto de presencia (*point of presence,* PoP). Debido a su función, los servidores PoP nunca deben estar conectados a la Internet. La forma más común de lograr el servicio PoP es mediante el uso de una VPN para cifrar el tráfico entre el host y el punto de presencia de la red interna.

Acceso Remoto: Escritorio Virtual

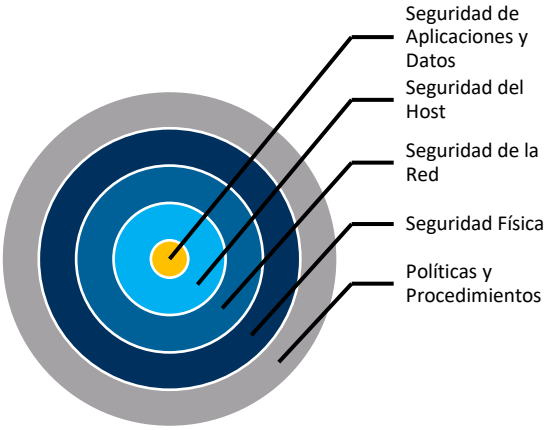
Los protocolos de escritorio virtual o *virtual desktop*, como el *Remote Desktop Protocol* (RDP) de Microsoft, brindan a los usuarios una interfaz gráfica para conectar un sistema (computadora) a otro a través de una conexión de red. El uso principal de los protocolos de escritorio virtual es proporcionar soporte técnico y administrar servidores que no tienen un teclado/monitor de video/mouse conectado, lo que permite a los administradores operar y mantener servidores en un centro de datos.

Ambas computadoras deben tener instalado el mismo software de protocolo de escritorio virtual para usar esta función. Para acceder a otra computadora, un usuario remoto debe tener tanto la dirección IP como la capacidad de autenticarse (por ejemplo, iniciar sesión, ofrecer un token de seguridad). Por motivos de seguridad, las conexiones de software de protocolo de escritorio virtual a menudo se bloquean en el firewall perimetral o en la DMZ.

Defensa de la red

Para comprender completamente la seguridad de la red en lo que respecta a los componentes y la arquitectura de una red, se debe comprender el concepto de defensa en capas o defensa en profundidad (Figura 16). Este concepto se centra en la premisa de que ningún punto único de falla debe causar el compromiso total de la seguridad.

Figura 16: Defensa en profundidad en capas



Fuente: Instituto de Auditores Internos

Defensa en Capas o Defensa en Profundidad

Este concepto garantiza que haya varias capas de controles antes de que un intruso potencial pueda acceder a información confidencial. Por lo general, estas capas de controles existen en una red, servidores, aplicaciones y bases de datos. Este concepto también asegura que existan controles físicos apropiados. El concepto general se rige por políticas y procedimientos adecuados.

El concepto de defensa en profundidad es similar a cómo se protegían los castillos durante la época medieval, cuando múltiples controles o barreras protegían tanto a las joyas de la corona como a los habitantes. Hoy en día existe una filosofía similar para definir los controles cibernéticos en varias capas del entorno cibernético.

- Internet está por fuera del portón del castillo.
- El portón del castillo es el primer firewall (que da al exterior).
- Las murallas, el foso y el patio son la DMZ.
- Las torres de vigilancia son portales de seguridad IDS/IPS, DLP, correo electrónico y web.
- La puerta interior del castillo es el segundo firewall (que da al interior).
- Las habitaciones del castillo son la red segmentada.

Desafíos y riesgos de la red

Las redes tienen muchos componentes y cada organización tendrá una estructura de red única. Tener una red eficaz puede tener un impacto significativo en las operaciones de una organización. La comprensión de un auditor interno de la arquitectura de la red es clave para comprender los riesgos y desafíos asociados con las redes.

Existen numerosos desafíos/riesgos relacionados con la red de una organización que los auditores internos deben conocer, que pueden incluir, entre otros:

- *Asegurar la identificación adecuada de todos los servicios de cara al exterior proporcionados por la organización.*
- *Garantizar una seguridad de red suficiente.*
  - Garantizar que los componentes de la red sean seguros y estén configurados de acuerdo con las políticas de la organización alineadas con las regulaciones aplicables y las mejores prácticas de la industria.
  - Monitorear la *dark web* en busca de correos electrónicos/contraseñas comprometidas y verificar que las contraseñas se cambien con frecuencia.
  - Garantizar la implementación del software *anti-malware* y *anti-phishing* adecuado.
  - Realización de capacitaciones obligatorias de sensibilización de los empleados sobre software *anti-malware* y *anti-phishing*.
- *Garantizar el acceso adecuado.*
  - Garantizar que el acceso a los conmutadores esté restringido y que los técnicos mantengan y actualicen periódicamente su funcionalidad.
  - Asegurarse de que el acceso físico a los enrutadores esté restringido. Los enrutadores casi siempre tienen capacidades de acceso remoto para los propios dispositivos. Estos deben protegerse con contraseñas seguras y supervisarse para detectar intentos fallidos de inicio de sesión.
  - Verificar que los usuarios remotos usen la autenticación de dos factores.
- *Asegurar el mantenimiento de parches.* Asegurarse de que los últimos parches de seguridad y actualizaciones de firmware estén instalados en los componentes de la red; por ejemplo, firewalls, enrutadores, impresoras y teléfonos habilitados con *Voice over Internet Protocol* (VoIP).
- *Asegurar una gestión adecuada de riesgos de la red de terceros.* Se aplica si la administración de la red se subcontrata y, de ser así, se garantiza que los programas de seguridad del proveedor sean sólidos, eficientes, efectivos y accesibles.

Aplicaciones

Arquitectura de aplicaciones

La arquitectura de aplicaciones implica el diseño y el comportamiento de las aplicaciones de una organización y se centra en su interacción con otras aplicaciones y con los datos y los usuarios en apoyo de los ciclos y funciones de negocio. La arquitectura de una organización debe diseñarse en consonancia con sus requisitos y estrategia comercial, y debe tener los controles adecuados para garantizar la integridad, precisión y autorización.

Recursos

Para obtener más información sobre los controles generales de TI, consulte IIA GTAG "Riesgos y Controles de Tecnología de la Información, 2.° edición".

Para obtener más información sobre los controles de la aplicación, consulte IIA GTAG "Auditoría de controles de aplicaciones."

Las consideraciones deben incluir la interacción entre los paquetes de aplicaciones y los usuarios, la integración de datos y cómo los sistemas están diseñados para trabajar junto con la red y la infraestructura. Dentro de la arquitectura, deben considerarse la escalabilidad y la capacidad de las aplicaciones, debido al potencial crecimiento empresarial, el cambio en las prioridades organizativas y otros factores. La consideración del alcance de la fluctuación comercial plantea posibles problemas de integración o brechas en la cobertura funcional. Para fines de planificación, se pueden desarrollar estrategias para identificar sistemas que pueden ser funcionales ahora pero corren riesgos de no mantener el ritmo del cambio así como la necesidad de integridad, confiabilidad o disponibilidad de los datos.

Comprender la arquitectura de aplicaciones de una organización permite a los auditores internos apreciar cómo las múltiples aplicaciones se encuentran estratégicamente alineadas para cumplir una operación de negocio. Por ejemplo, una plataforma basada en la nube puede combinar múltiples tecnologías y aplicaciones proporcionadas por SaaS para entregar un proceso de negocio específico. Luego, la dirección diseñaría una combinación de controles de aplicaciones, controles generales de TI y monitoreo continuo suficiente para abordar las aplicaciones administradas tanto en las instalaciones como fuera de ellas (potencialmente por proveedores de servicios externos).

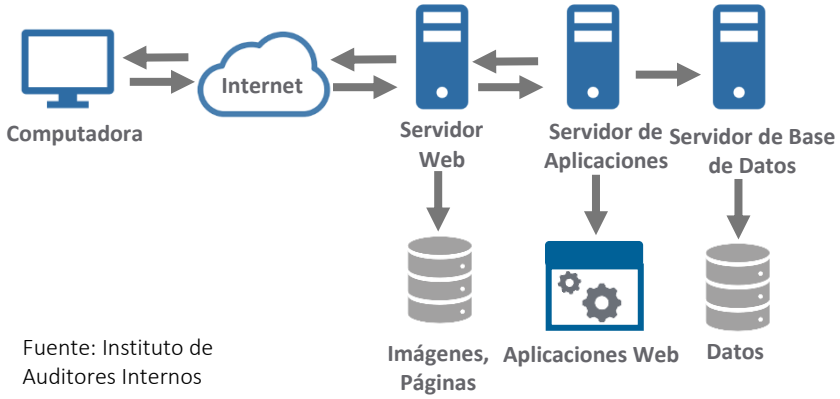
Aplicaciones Web o de Internet

La arquitectura para aplicaciones web generalmente requiere un servidor web al que se pueda acceder desde la Internet y que, por lo general, resida en la DMZ. Los lenguajes de secuencias de comandos que se utilizan para escribir código fuente de aplicaciones incluyen Java, C, Python, Ruby, PHP y otros. Ejemplos de aplicaciones web incluyen sitios como www.amazon.com o www.rakuten.co.jp. Cualquier usuario con acceso a la Internet puede acceder a estas aplicaciones. El servidor web generalmente solo maneja la interfaz con el usuario a través de la Internet.

Desde la perspectiva de la arquitectura, el servidor web generalmente "habla" con un servidor de aplicaciones que realiza las funciones principales de la aplicación. El servidor de aplicaciones

interactúa con la base de datos donde se almacena la información, que generalmente se encuentra en un servidor de base de datos. Según la aplicación, los servidores de bases de datos pueden contener información sensible o crítica relacionada con la aplicación (por ejemplo, información de tarjetas de crédito, información médica o información personal de un usuario) y, por lo tanto, deben ser seguros y el acceso debe controlarse de manera adecuada. Esta base de datos reside en la red interna, inaccesible desde la Internet por motivos de control y seguridad. Solo el servidor de aplicaciones puede conectarse a la base de datos y solo el servidor web puede conectarse al servidor de aplicaciones a través de una conexión segura, como se muestra en la Figura 17.

Figura 17: Arquitectura típica de aplicaciones web



Fuente: Instituto de Auditores Internos

En muchas organizaciones, la arquitectura de aplicaciones web también incluirá un firewall de aplicaciones web (WAF, como se muestra en la Figura 14), para identificar, detectar y prevenir ataques de aplicaciones web como inyección SQL o scripts entre sitios (XSS). Estos ataques pueden tener éxito si una aplicación web que se ejecuta en un servidor web no está codificada de forma segura. En lugar de revisar todas las aplicaciones web, una organización puede implementar un WAF para prevenir los ataques a las aplicaciones web.

Interfaces de programa de aplicación (API) y servicios web

Las API *(application program interfaces)* y los servicios web son piezas de código diseñadas para interactuar con otras piezas de código y describen cómo se comunican dos aplicaciones. Esto permite que las aplicaciones de una organización interactúen con otras aplicaciones dentro o fuera de la organización. En consecuencia, las aplicaciones web y móviles dependen en gran medida tanto de los servicios web como de las API. Un diferenciador principal entre una API y un servicio web es que las API funcionan con una variedad de protocolos de comunicación. Debido a que estas interfaces pueden ser críticas para las funciones de negocio de una organización, la organización debe hacer un inventario de todas las API y los servicios web en uso. Los usos deben ser parte de la documentación de la API y las API deben incluirse en el proceso de administración de parches de una organización.

Aplicaciones Internas

En general, se accede a las aplicaciones internas a través de la red interna de una organización o mediante su VPN. Solo los usuarios registrados en la red interna pueden acceder a estas aplicaciones. En este caso, la arquitectura típica comprende un servidor de aplicaciones, un servidor de base de datos y una base de datos. La arquitectura suele ser menos compleja en comparación con una aplicación web.

Aplicaciones en la Nube

Debido al potencial ahorro de tiempo y costo, así como a la facilidad de implementación, muchas organizaciones están dispuestas a prescindir de algunas características de aplicaciones y adaptarse a las características proporcionadas por diferentes aplicaciones en la nube (consulte la sección Arquitectura de Red, para obtener detalles sobre los diferentes tipos de modelos de servicios en la nube). Esto permite a las organizaciones prescindir del desarrollo interno de aplicaciones o la compra de software estándar de los proveedores. En muchos casos, el costo de la aplicación en la nube es más económico que desarrollar una aplicación internamente, pero cada organización debe determinar si las aplicaciones en la nube seleccionadas pueden cumplir con los requisitos normativos y de la organización.

Debido a su enfoque en servicios específicos, las aplicaciones en la nube a menudo colocan a una organización en una mejor posición para reducir los costos de recursos de red y hardware interno en comparación con el mantenimiento de su infraestructura de TI actual. El uso de la nube también puede proporcionar a la organización una ventaja competitiva frente a la competencia cuando se trata de implementar tecnologías emergentes.

Desarrollo y mantenimiento de aplicaciones

Para algunas organizaciones, el desarrollo de aplicaciones puede ser una competencia central que les ayude a alcanzar sus objetivos estratégicos. El desarrollo de aplicaciones implica la creación e integración de programas que pueden facilitar los procesos de negocio, automatizar las actividades de control y mejorar la eficiencia. Las aplicaciones se conectan con la red y la infraestructura de la organización y llevan a cabo la lógica empresarial prevista por el proceso. Los programas de software pueden tener controles de aplicación integrados para abordar los riesgos relacionados con la precisión, la integridad y la autorización.

Las aplicaciones y el software se han desarrollado tradicionalmente utilizando el método de gestión de proyectos en cascada. Una forma sencilla de pensar en el método de la cascada es considerar la forma en que se desarrolla la vivienda. Una casa se diseña, construye e inspecciona antes de que se otorgue un certificado de ocupación. A veces, esto puede resultar ineficaz.

El desarrollo de aplicaciones y software puede adoptar un enfoque más incremental, que puede abordar la posible demora en los entregables. En lugar de entregar un producto completo a la vez, ahora se usa con frecuencia un método conocido como *Agile* (o desarrollo de software adaptativo). Con este método, todavía hay un plano y un resultado final conocido, como lo hay para una casa,

pero se puede desarrollar o construir un entregable a la vez, en lo que se conoce como *sprints*. Usando la analogía de construir una casa, el método ágil de desarrollo de software sería como seguir el plano, construir, inspeccionar y otorgar la ocupación de una casa una habitación a la vez; es decir, entregar una unidad o una sección de una aplicación o un proyecto completo.

El método *Agile* puede ser eficaz en el desarrollo de aplicaciones, dado que el enfoque en cascada requiere que se completen todos los pasos intermedios antes de entregar el producto final.

Agile, correctamente implementado, ha creado un nuevo proceso de desarrollo y prueba de software denominado *DevOps* (una combinación de las palabras desarrollo y operaciones) o *DevSecOps* (desarrollo, seguridad y operaciones). Con este método, una organización no necesita conocer el producto final porque se basa en la gestión de programas frente a la gestión de proyectos. El enfoque está más centrado en el cliente, construyendo una característica a la vez. Así, aborda las frustraciones que surgen por la espera de los entregables completos del proyecto.

Independientemente de la metodología de gestión de proyectos que se siga, se deben realizar tres actividades para desarrollar una aplicación confiable:

1. Plan estratégico y diseño.
2. Desarrollo y pruebas.
3. Implementación y mantenimiento.

La práctica de un enfoque de desarrollo de aplicaciones disciplinado fortalece la madurez de la capacidad de una organización desde una actividad manual ad hoc hasta prácticas sistemáticas optimizadas. Si se hace bien, el desarrollo de aplicaciones puede tener un impacto positivo al:

- Mejorar el compromiso continuo con las relaciones externas (p. ej., cliente y proveedor) e internas (p. ej., subordinados directos y a lo largo de la organización).
- Determinar la integridad de los datos mediante la lógica y las reglas comerciales que garantizan que los datos estén autorizados, completos y sean precisos.
- Garantizar que la información esté disponible y se comunique a tiempo para tomar medidas decisivas.

Un enfoque estructurado ayudará a acelerar el cambio transformador de forma controlada:

- Los controles de acceso protegen la transición desde el diseño estratégico hasta el desarrollo y la implementación del código.
- La protección del código fuente promueve los cambios de la aplicación aprobados por la dirección.
- Las pruebas sólidas garantizan que el diseño funcione con fiabilidad y con tecnologías interdependientes, de acuerdo con las expectativas de la dirección.
- La documentación y la formación proporcionan un uso adecuado y coherente de la aplicación.

Con mantenimiento continuo, las aplicaciones se mantienen adecuadas para su propósito y se garantiza la disponibilidad, seguridad e integridad del sistema.

Recursos

Para obtener más información sobre la gestión de cambios en relación con las aplicaciones, consulte la Guía GTAG del IIA "Gestión de cambios de TI: Crítico para el éxito de la organización, 3.° edición".

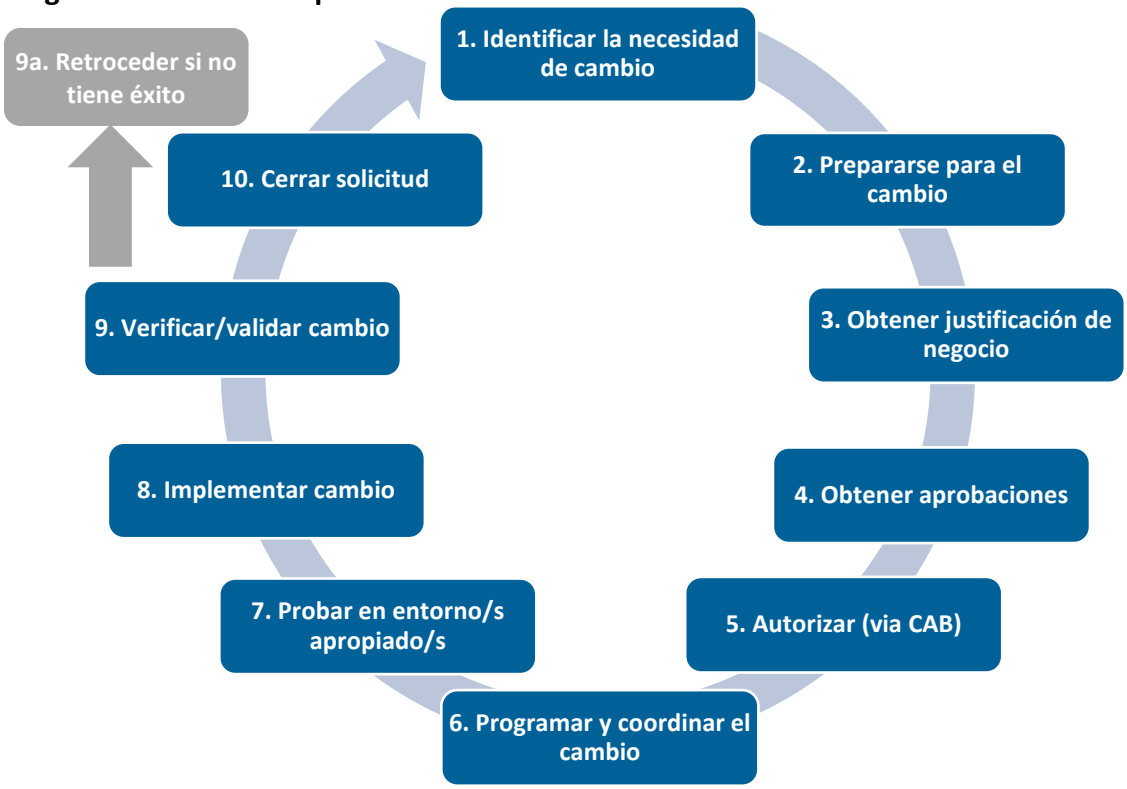
Cambios en Aplicaciones y Controles

Ya sea que los programas de computadora se desarrollen internamente o sean desarrollados por otros según las especificaciones de la organización, los controles son necesarios para garantizar que los cambios en las aplicaciones se diseñen de manera adecuada y se implementen en forma efectiva. Esto protege el entorno de producción (en vivo) de una aplicación.

Los cambios deben seguir los protocolos de cambios de la dirección. Cada uno debe ser solicitado, delimitado y aprobado por la función de negocios correspondiente. Las iniciativas de cambio deben evaluarse en función de los beneficios y la prioridad, y debe realizarse un seguimiento con una orden de servicio o un número de ticket. El impacto y el riesgo que plantea el cambio deben tenerse en cuenta al determinar el alcance del esfuerzo y el calendario del proyecto, y deben asignarse los recursos adecuados con experiencia para llevar a cabo el cambio.

Las solicitudes de cambio deben diseñarse en base a los requisitos documentados dirigidos por la unidad de negocios apropiada, y debe existir una separación adecuada de controles de funciones durante todo el proceso. Deben seguirse pasos secuenciales en la evolución de un cambio necesario, como se muestra en el ejemplo de la Figura 18.

Figura 18: Pasos en el proceso de cambio



Contar con pruebas sólidas garantiza la calidad de la información afectada por el cambio. Los cambios deben ser desarrollados y probados en entornos que no son de producción, como un entorno de desarrollo o prueba (DEV y TEST), primero por TI y luego proporcionados a la unidad de negocios para la prueba de aceptación. Los usuarios finales que tienen experiencia con el proceso que se está probando desarrollan un plan de prueba de aceptación del usuario y deben identificar las actividades o funciones de negocio clave afectadas por el cambio. Estos factores pueden contribuir a desarrollar un plan de prueba de aceptación de usuario eficaz:

- Participación de los representantes de la aplicación y de la unidad de negocio con conocimiento directo de la aplicación y los datos a probar.
- Objetivos claramente establecidos y escenarios de prueba basados en eventos del ciclo de actividad de negocio, incluso actividades de alto riesgo (por ejemplo, posibles pérdidas/interrupciones de ingresos o problemas legales).
- Un conjunto de condiciones de prueba requeridas para el escenario empresarial, en lugar de condiciones basadas en variaciones de un programa de software.
- Un conjunto de resultados de prueba predeterminados para el plan de prueba.
- Seguimiento y resolución de defectos.
- Técnicas de seguimiento de la diligencia a seguir con posterioridad al movimiento de producción (PROD).
- Interrelaciones e impactos con otras aplicaciones.

En última instancia, la dirección de la organización garantiza el nivel adecuado de documentación y autoriza el cambio que afecta el entorno de producción de la aplicación sobre la base de los resultados de las pruebas. El código fuente aprobado luego pasa a producción mediante una función independiente dentro de un entorno de prueba que emula la actividad de producción. El cambio debe ser aceptado formalmente por el solicitante de la unidad de negocios y sujeto a debida diligencia (es decir, el monitoreo de la diligencia podría incluir la validación de una serie de ciclos de procesamiento consecutivos sin errores).

En la Figura 19 se muestra una descripción simple de la migración de un cambio propuesto a través de los entornos apropiados.

FIGURA 19: Ejemplo de una migración de cambio de TI

Entornos de producción segregados

Nota: La migración a través de cada uno de estos entornos debe estar debidamente segregada.
Fuente: Instituto de Auditores Internos

Los usuarios del negocio suelen estar restringidos a su entorno de producción en línea; los programadores y desarrolladores están restringidos a su entorno de prueba. El pasaje a entornos de producción debe realizarse de forma independiente para garantizar el control de versiones.

Los cambios de emergencia deben ser pocos y aún requerir el mismo nivel de documentación y pruebas. En algunos casos, la aprobación para ejecutar un cambio de emergencia en la producción puede obtenerse después del hecho, pero dentro de un plazo razonable y formalmente establecido (por ejemplo, dos días hábiles).

Desafíos y riesgos de aplicaciones

Las aplicaciones funcionales y eficientes son clave para el éxito de toda organización. El diseño y mantenimiento de la arquitectura de aplicaciones, el desarrollo de aplicaciones nuevas y la modificación de las existentes deben ser procesos eficientes y efectivos como responsabilidad de la dirección, y deben ser bien comprendidos por los auditores internos. Operar adecuadamente los controles en todas estas funciones puede marcar la diferencia entre un proceso eficaz o ineficaz.

Con respecto a la arquitectura de aplicaciones, los auditores internos deben tener una visión de toda la empresa de proveedores de servicios externos, el riesgo de la tecnología en la nube y los controles adecuados significativos para las operaciones y la entrega de los procesos de negocio.

Existen numerosos desafíos/riesgos relacionados con las aplicaciones de una organización que los auditores internos deben conocer, que pueden incluir, entre otros:

- *Planificación poco clara/plazos acelerados.* Cuando los esfuerzos de desarrollo de aplicaciones fallan, a menudo se debe a una planificación poco clara y/o plazos acelerados que conducen a un diseño insuficiente. Si los cambios se introducen con mayor frecuencia, los equipos de desarrollo podrían acelerar la implementación fuera de los protocolos documentados, sin priorizar la arquitectura y planificación estratégica.
- *Múltiples proveedores de servicios.* Trabajar con diversos proveedores de servicios de software puede complicar aún más la gestión de datos cuando la información debe transmitirse entre distintas aplicaciones.

Los siguientes factores de riesgo, relacionados con los cambios de aplicaciones, se clasifican según tres causas fundamentales: metodología informal, lógica incorrecta y volatilidad creciente. Abordar la causa raíz puede contribuir a corregir las excepciones sintomáticas y promover la remediación:

Metodología Informal/ Cambios Ad Hoc

- Las expectativas de ROI poco realistas inhiben la presentación de ideas emergentes.
- Requisitos ambiguos del sistema.
- Cambios aplicados a la versión incorrecta del código fuente.
- Cambios recurrentes en el mismo programa/aplicación.
- Retrasos en la entrega de la solución.
- Interrelaciones no consideradas durante un cambio de emergencia.
- Falta de participación del usuario durante las pruebas.
- Falta de revisión y diligencia por parte del usuario posterior a la aplicación del cambio.

Lógica Incorrecta/Deficiente incorporada en el Diseño de Programas

- Aplicaciones críticas para el negocio se cambian *in-house* como solución provisional.
- Errores introducidos al entregar un cambio basado en una comprensión incompleta de la solución.
- Acceso sin restricciones al código fuente.
- Falta de herramientas de control y seguimiento de cambios.
- Prueba insuficiente.

Aumento de la Volatilidad de la Aplicación

- Frecuencia creciente de cambios e interrupciones en el servicio por mantenimiento (aplicaciones que cambian cada semana).
- Volumen creciente de cambios (aplicaciones que requieren más mantenimiento).
- Aumento de la cantidad de informes clave y los cambios realizados en los informes clave.
- Ocurrencia de una cantidad de cambios de emergencia.

Temas adicionales y emergentes de TI

En esta sección se analizan algunos temas de TI emergentes y fundamentales adicionales, a nivel general. Es importante comprender que estos temas adicionales son dinámicos, no estáticos, y la lista no es exhaustiva. Los temas cubiertos en las secciones anteriores alguna vez se consideraron como temas emergentes/novedosos en el área de TI y con el tiempo se han vuelto omnipresentes y esenciales para las organizaciones. Lo mismo se aplica a los diversos temas de esta sección; es posible que algún día se conviertan en procesos comunes para todas las organizaciones.

A medida que surgen nuevos temas de TI y evolucionan los existentes, continuar informado y aplicar el escepticismo profesional sigue siendo crucial para los auditores internos que se esfuerzan por mantenerse relevantes y de conformidad con las *Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna* del IIA.

Gestión de Datos

En muchas organizaciones, las aplicaciones se desarrollan u obtienen/utilizan en silos, y puede resultar difícil verificar la integridad de los datos utilizados y producidos por las aplicaciones. La integridad de los datos se basa en muchas variables, como la(s) fuente(s) de entrada de datos en la aplicación, la lógica utilizada por la aplicación para producir los datos y la precisión de los datos producidos por la aplicación.

Una de las razones por las que la calidad de los datos puede ser insuficiente es que las organizaciones a menudo recopilan o adquieren datos de diversas fuentes. A medida que estos datos se ingresan en las diversas aplicaciones de una organización a lo largo del tiempo, debido al gran volumen, la calidad puede deteriorarse. Además, si el formato de los datos recopilados es diferente para cada método de recopilación, los datos resultantes podrían verse comprometidos. Es importante tener controles de *front-end* para garantizar un formato uniforme.

Algunos ejemplos de problemas de entrada de datos:

- Errores de entrada de datos.
- Datos almacenados de forma incorrecta dentro de las aplicaciones.
- Formateo incorrecto de datos.

Una vez que las aplicaciones (que pueden haber sido desarrolladas en silos) se incorporan en los procesos de negocio clave, los usuarios se vuelven dependientes de estas aplicaciones y datos, aunque en algunos casos, estos datos pueden no ser confiables.

La posible mala calidad, la falta de integridad y la incapacidad de las organizaciones para confiar en sus datos pueden costar millones de dólares. Estimaciones recientes indican que una organización

promedio puede sufrir pérdidas de US$ 15 millones al año debido a la mala calidad de los datos, y la economía de los EE. UU. podría sufrir pérdidas que superen los US$ 3 billones anuales.[2]

Los desafíos y riesgos asociados con la gestión de datos empresariales también pueden depender de la cultura de la organización y su estructura (factores como si está descentralizada o centralizada). Cuanto más operan en silos las divisiones individuales de la organización, más difícil es tener una estrategia de gestión de datos empresarial eficaz.

Otros factores que podrían afectar potencialmente la gestión de datos incluyen:

- Inventario de activos de información y datos inexactos o incompletos.
- Falta de políticas de gestión de datos empresariales.
- No hay una persona responsable o capaz de gestionar la arquitectura de datos empresariales de la organización.
- Fuentes de datos de mala calidad.
- Falta de procedimientos para identificar aplicaciones y sistemas con problemas de calidad de datos y falta de procedimientos para iniciar proyectos que aborden problemas.

Los posibles resultados adversos de una mala gestión de datos incluyen:

- El descontento del cliente cuando sus datos se reflejan de manera inexacta en los sistemas y aplicaciones de la organización.
- Multas y/o sanciones reglamentarias.
- Violaciones de datos.
- Impacto potencial en la rentabilidad de una organización.

Análisis de Datos

El análisis de datos se puede utilizar para identificar indicadores clave de tendencias para ayudar a la dirección a ver qué tan bien están funcionando los procesos y controles. Más importante aún, los análisis pueden mostrar una degradación continua de los procesos y controles, lo cual podría desencadenar una acción correctiva acelerada. A medida que las organizaciones maduran, el análisis de datos tiene un gran impacto en la forma en que pueden evaluar y recopilar información relevante para la toma de decisiones y el seguimiento de riesgos clave.

Asimismo, la analítica de datos también ha ganado terreno como técnica que la actividad de auditoría interna puede aplicar al ejecutar auditorías. Un programa formal de análisis de datos puede ser útil para respaldar una función de auditoría para que sea más eficaz, más eficiente, fácilmente escalable y reduzca significativamente los errores de auditoría y también brinde una mayor cobertura de auditoría y riesgo de fraude. Los programas de análisis de datos pueden ofrecer auditoría o monitoreo continuo a largo plazo en cuanto a problemas legales y de cumplimiento, y la capacidad de hacer pruebas de auditoría ad hoc y revisión del negocio, y ayudar con posibles investigaciones de fraude.

[2] Kaerrie Hall, "Customer Data Quality: The Good, the Bad and the Ugly," Validity, 5 de septiembre de 2019. https://www.validity.com/blog/customer-data-quality/.

Tanto para la auditoría interna como para el negocio, la calidad de los datos puede seguir siendo un desafío. Si bien la aplicación de análisis a conjuntos de datos estructurados (por ejemplo, tablas SQL) puede ser avanzada en algunas organizaciones, la aplicación de análisis de datos a conjuntos de datos no estructurados (por ejemplo, hojas de cálculo o correos electrónicos) puede ser de especial interés para las organizaciones, ya que podría proporcionar información clave adicional.

Redes Sociales

Las redes sociales comprenden un conjunto de tecnologías y canales destinados a formar y permitir que una comunidad potencialmente masiva de participantes colabore de manera productiva. Ejemplos de plataformas y canales de redes sociales en todo el mundo incluyen Facebook, LinkedIn, YouTube, Twitter, Instagram, QQ, Wechat, WhatsApp y muchos más.

Los riesgos que enfrentan las organizaciones en este ámbito van desde no adoptar las redes sociales (por ejemplo, marca/imagen, perder la interacción con el cliente), daño a la reputación por publicaciones de información engañosas o incorrectas, riesgo de seguridad, violación de las regulaciones de privacidad/confidencialidad, pérdida/robo de propiedad intelectual y exposición de secreto comercial. Por ejemplo, una declaración despectiva hecha por un empleado sobre un competidor podría resultar en una demanda potencial contra la organización, o un comentario publicado por un empleado sobre otro empleado podría interpretarse como acoso que daría lugar a una demanda. En consecuencia, las organizaciones deben comprender su presencia social y supervisar cada canal en el que tengan presencia.

Las organizaciones deben tener una política y procedimientos de presencia social (digital) con respecto a la forma en que se administran los sitios de redes sociales. Las políticas también deben abordar el comportamiento de los empleados con respecto a las redes sociales. Las organizaciones deben asegurarse de que los empleados conozcan estas políticas, ya que el uso indebido de las redes sociales podría tener un efecto drástico en la reputación de la entidad.

Automatización de Procesos Robóticos

La automatización de procesos robóticos (*robotic process automation,* RPA) se refiere al software que se puede programar para realizar tareas en todas las aplicaciones, de manera similar a como lo harían los humanos. A un robot de software (bot) se le puede enseñar un flujo de trabajo con múltiples pasos y aplicaciones, como evaluar los formularios recibidos, enviar un mensaje de recibo, verificar que los formularios estén completos, llenar formularios en carpetas y actualizar hojas de cálculo con el nombre del formulario, la fecha de archivado, y así sucesivamente. El software RPA está diseñado para reducir o automatizar tareas simples y repetitivas.

El uso de RPA difiere mucho según los resultados deseados. Puede variar el uso estratégico (automatización en el núcleo versus automatización usando RPA), el número de plataformas en uso (una plataforma versus múltiples plataformas), los tipos de bots en uso (los bots atendidos son

iniciados por un usuario de diálogo, mientras que los bots desatendidos son programados para ejecutarse automáticamente) y más.

Como cualquier innovación tecnológica, existen beneficios y riesgos en RPA. Las organizaciones deben sopesar cada uno individualmente antes de embarcarse en una estrategia de RPA. Los beneficios pueden incluir, entre otros:

- *Mejora de la moral de los empleados* – los empleados pueden verse libres de realizar tareas repetitivas.
- *Productividad* – la automatización de tareas simples permite a los empleados aumentar la productividad en otras áreas.
- *Fiabilidad* – con una programación adecuada, RPA puede producir resultados más fiables.
- *Coherencia* – los bots se pueden programar para que funcionen sin parar y realicen procesos repetibles, lo que garantiza resultados uniformes a lo largo del tiempo.
- *Tecnología no invasiva* – la disrupción de los sistemas existentes no es un problema.
- *Cumplimiento* – las pistas de auditoría se pueden documentar para satisfacer los requisitos regulatorios.
- *Barrera técnica baja* – la configuración es relativamente simple.
- *Precisión* – los bots son menos propensos a errores humanos.

Los riesgos pueden incluir, entre otros:

- *Problemas de segregación de funciones* – los bots pueden tener una autoridad excesiva.
- *Procesos mal escritos* – como con cualquier programa de computadora, se debe prestar atención a lo que se solicita al bot que haga.
- *El proceso existente no se mejoró antes de ser automatizado* – si un proceso tenía fallas antes de la automatización, simplemente transferir el mismo conjunto de reglas a un programa automatizado seguirá produciendo resultados defectuosos.
- *Monitoreo deficiente de bots y administradores* – aunque automatizados, los bots necesitan mantenimiento ocasional, y los administradores deben estar informados de nuevos procesos, resultados comprometidos, etc.
- *Ciberataques* – cualquier elemento del entorno de TI está sujeto a problemas cibernéticos. Los bots no son una excepción.

Aprendizaje Automático e Inteligencia Artificial

La automatización cognitiva combina tecnologías avanzadas como el procesamiento del lenguaje natural (*natural language processing,* LNP), la inteligencia artificial (IA), el aprendizaje automático (*machine learning,* ML) y el análisis de datos para imitar actividades humanas como inferir, leer señales emocionales, razonar, formular hipótesis y comunicarse con los humanos.

El valor va más allá de la capacidad de automatizar los procesos de negocio; la automatización cognitiva también puede servir para aumentar lo que hacen los humanos, haciendo que los empleados estén más informados y sean más productivos. Dentro de la automatización cognitiva, existe una diferencia importante entre el aprendizaje y el razonamiento. El aprendizaje consiste en reconocer patrones a partir de datos no estructurados y la automatización correlacionada se basa en calificaciones de precisión. Por el contrario, el razonamiento basado en hipótesis se sustenta en calificaciones de confianza.

Los riesgos relacionados con la automatización cognitiva incluyen, entre otros:

- La IA puede interpretar las malas prácticas como aceptables.
- La mala comprensión por parte de los diseñadores se refleja en los sistemas.
- Sistemas comprometidos y controlados por malos actores.
- Posibilidad de que el malware se incruste en los motores de aprendizaje, lo que podría sesgar los resultados del aprendizaje automático y potencialmente afectar los procesos.

Internet de las Cosas (IoT)

La creciente presión para aumentar la eficiencia y la calidad del procesamiento operativo continúa impulsando los esfuerzos para avanzar en la digitalización y la automatización. A partir de estos esfuerzos, ha surgido la Internet de las Cosas (*Internet of Things,* IoT, Figura 20, o "dispositivos conectados"), que extiende la conectividad de la Internet a dispositivos físicos y objetos cotidianos, como televisores, relojes de pulsera, refrigeradores, timbres, termostatos, automóviles y tantos más.

Figura 20: Internet de las Cosas

Fuente: Instituto de Auditores Internos

Si bien los dispositivos se comunican e interactúan entre sí a través de la Internet, se pueden monitorear y controlar de forma remota. La capacidad de las máquinas y los sistemas para interactuar e intercambiar información sin intervención humana acelera los esfuerzos en torno a la digitalización y la automatización.

Junto a los importantes beneficios percibidos, surgirán desafíos inherentes debido al rápido ritmo del cambio. Desde una perspectiva de riesgo, debido a la gran prevalencia de los dispositivos y su conectividad, el componente de seguridad subyacente es imperativo. Las organizaciones deben comprender todos los dispositivos conectados, tanto de propiedad de la empresa como de los empleados, y comprender los riesgos únicos asociados con cada uno.

Desafíos para temas emergentes y adicionales de TI

Las tecnologías surgen y evolucionan más rápido que nunca. Independientemente del nivel de madurez de una organización que utilice las tecnologías analizadas en esta sección, es imperativo que la auditoría interna las conozca y participe en las etapas iniciales de su implementación. Así, puede estar en condiciones de identificar los riesgos potenciales que pueden ocurrir y equipar mejor a la organización para abordarlos. Los numerosos riesgos a tener en cuenta incluyen los riesgos operativos, de cumplimiento e informes. Otros desafíos y riesgos pueden incluir:

- Falta de comprensión de la tecnología/concepto/herramienta.
- Falta de comprensión de los cambios en el proceso asociados con la tecnología/concepto/herramienta.
- Planificación insuficiente para la implementación, el mantenimiento o los cambios en la tecnología/concepto/herramienta.
- Falta de inclusión de la nueva tecnología/concepto/herramienta en la evaluación de riesgos.

Lo que se audita normalmente no cambia con las nuevas tecnologías, herramientas, automatización, etc.; más bien, se debe considerar cómo se realiza la auditoría en función del cambio en el riesgo inherente y residual. Por ejemplo, los controles generales de TI (como acceso, cambio, copias de seguridad) continúan siendo válidos, por lo que los marcos de control existentes siguen siendo aplicables (como Center of Internet Security [CIS], Cloud Security Alliance [CSA] o NIST 800-53). Las auditorías de áreas emergentes también enfrentan riesgos operativos, riesgos de informes y riesgos de cumplimiento. Es fundamental contar con una visión holística de los riesgos.

Además de comprender las tecnologías que utiliza una organización, la auditoría interna puede aprovechar algunas tecnologías emergentes para sus propios usos (por ejemplo, usar análisis de datos o RPA para agilizar su proceso de muestreo o para implementar auditorías continuas).

Conclusión

En el mundo actual, todas las organizaciones son impulsadas por la tecnología. Los auditores internos necesitarán más herramientas, talentos y habilidades que nunca para seguir siendo relevantes y continuar brindando aseguramiento a sus organizaciones de que los sistemas están

funcionando como deberían y los controles están en su lugar. Los fundamentos de la auditoría interna (evaluaciones basadas en riesgos, planificación, comunicación y aprendizaje continuo) son tan importantes como siempre.

Los auditores internos deben permanecer ágiles y listos para los cambios en los modelos de negocio conforme las organizaciones adoptan avances en la tecnología. Deben ser lo suficientemente ágiles para crecer junto con la organización y fomentar buenas relaciones de trabajo con sus compañeros de unidades de negocio y departamentos para colaborar progresivamente con miras a enfrentar los desafíos que se avecinan. Para seguir siendo relevante, agregar valor y ofrecer protección a sus organizaciones, será crucial que la auditoría interna se mantenga al día con los cambios.

Apéndice A. *Normas* y directrices pertinentes del IIA

Se hizo referencia a los siguientes recursos a lo largo de esta guía práctica. Para obtener más información sobre la aplicación de las *Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna del IIA*, consulte las Guías de Implementación del IIA.

Código de Ética
Principio 4 – Competencia
Normas
Norma 1100 – Independencia y Objetividad
Norma 1200 – Aptitud y Cuidado Profesional
Norma 1210 – Aptitud
Norma 2230 – Asignación de Recursos para el Trabajo
Norma 2340 – Supervisión del Trabajo
Guia
GTAG "Auditoría de Controles de Aplicaciones," 2009.
GTAG "Auditoría del Gobierno de TI," 2018.
GTAG "Tecnologías de Análisis de Datos," 2011.
GTAG "Gestión del Cambio de TI: Crítico para el Éxito Organizacional, 3.° edición," 2020.
GTAG "Riesgos y Controles de Tecnología de la Información, 2.° edición," 2012.

Apéndice B. Glosario

Todos los términos identificados aquí están tomados del "Glosario" del Marco Internacional de Prácticas Profesionales del IIA, edición de 2017.

actividad de auditoría interna: un departamento, división, equipo de consultores, u otro/s profesional/es que proporciona/n servicios independientes y objetivos de aseguramiento y consulta, concebidos para agregar valor y mejorar las operaciones de una organización. La actividad de auditoría interna ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.

consejo: el órgano de gobierno de más alto nivel de una organización (p. ej.: junta directiva, consejo supervisor o de administradores, directorio) que tiene la responsabilidad de dirigir y/o supervisar las actividades y al que la alta dirección rinde cuentas. Aunque el funcionamiento del Consejo varía entre jurisdicciones y sectores, generalmente el consejo incluye a miembros que no son parte de la dirección. Si no existe consejo, la palabra "consejo" se refiere a un grupo o persona encargada del gobierno de la organización. Además, el "consejo" en las *Normas* puede referirse a un comité u otro cuerpo en el que el órgano de gobierno haya delegado ciertas funciones (p. ej., comité de auditoría).

director ejecutivo de auditoría: se refiere a la función de una persona en un puesto de alta jerarquía responsable de la gestión efectiva de la actividad de auditoría interna de acuerdo con el estatuto de auditoría interna y los elementos obligatorios del Marco Internacional para la Práctica Profesional. El director ejecutivo de auditoría y las personas a su cargo tendrán las certificaciones y cualificación apropiadas. El nombre del puesto específico y/o las responsabilidades del director ejecutivo de auditoría pueden variar según la organización.

fraude: cualquier acto ilegal caracterizado por engaño, ocultación o violación de confianza. Estos actos no implican una amenaza de violencia o de fuerza física. Los fraudes son perpetrados por individuos y por organizaciones para obtener dinero, bienes o servicios, para evitar pagos o pérdidas de servicios, o para asegurarse ventajas personales o de negocio.

gestión de riesgos: un proceso para identificar, evaluar, gestionar y controlar eventos o situaciones potenciales para proporcionar una seguridad razonable con respecto al logro de los objetivos de la organización.

gobierno de la tecnología de la información: consiste en el liderazgo, las estructuras organizativas y los procesos que garantizan que la tecnología de la información de la empresa respalde las estrategias y los objetivos de la organización.

gobierno corporativo: la combinación de estructuras y procesos implementados por el consejo para informar, dirigir, gestionar y supervisar las actividades de la organización en pos del logro de sus objetivos.

riesgo: es la posibilidad de que ocurra un acontecimiento que tenga un impacto en el alcance de los objetivos. El riesgo se mide en términos de impacto y probabilidad.

trabajo: una asignación, tarea o actividad de revisión de auditoría interna específica, como una auditoría interna, revisión de autoevaluación de control, examen de fraude o consultoría. Un trabajo puede incluir múltiples tareas o actividades diseñadas para lograr un conjunto específico de objetivos relacionados.

valor añadido o agregado: La actividad de auditoría interna agrega valores a la organización (y sus partes interesadas) cuando proporciona una garantía objetiva y relevante, y contribuye a la eficacia y eficiencia de los procesos de gobierno, gestión de riesgos y control.

Apéndice C. Guía de acrónimos

Estos son acrónimos de uso común en la industria de TI que aparecen en esta guía.

Acrónimos de IT Comunes	
Acrónimo	**Significado**
2FA	Autenticación de Dos Factores
ACL	Lista de control de acceso
AD	(Microsoft) Active Directory
AI	Inteligencia artificial
AP	Punto de acceso
API	Interfaz de programa de aplicación
ARP	*Address Resolution Protocol*
ATM	Modo de Transferencia Asíncrona
AWS	Servicios web de Amazon
B2B	Empresa a empresa
B2C	Empresa a consumidor
BYOD	Traiga su propio dispositivo
BYOT	Traiga su propia tecnología
CDO	Director Ejecutivo de Datos
CIO	Director Ejecutivo de Información
CIS	Centro de Seguridad de Internet
CISO	Director Ejecutivo de Seguridad de Información
CPO	Director Ejecutivo de Privacidad
CTO	Director Ejecutivo de Tecnología
DB	Base de datos
DLP	Prevención de fuga de datos
DMZ	Zona desmilitarizada
DPO	Director Ejecutivo de Protección de Datos
DNS	Sistema de nombres de dominio
ERP	Planificación de recursos empresariales
FTP	*File Transfer Protocol*
GUI	Interfaz gráfica de usuario
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
IaaS	Infraestructura como servicio
IAM	Gestión de identidades y accesos

ICMP	*Internet Control Message Protocol*
IDS	Sistema de detección de intrusos
(The) IIA	Instituto de Auditores Internos
ILP	Prevención de fugas de información
IMAP	*Internet Message Access Protocol*
IoT	Internet de las Cosas
IP	*Internet Protocol*
IP PBX	*Internet Protocol private branch Exchange*
IPS	Sistema de prevención de intrusiones
IPSec	*Internet Protocol Security*
IS	Seguridad de información
IT	Tecnologías de la información
KPI	Indicador clave de rendimiento
KRI	Indicador clave de riesgo
LAN	Red de área local
LDAP	*Lightweight Direct Access Protocol*
MAM	Gestión de aplicaciones móviles
MAN	Red de área metropolitana
MDM	Gestión de dispositivos móviles
MFA	Autenticación multifactor
ML	Aprendizaje automático
MTA	Agente de transferencia de correo (o mensaje)
MU	Usuario de correo
MUA	Agente de usuario de correo
NG	Próxima generación
NIST	Instituto Nacional de Estándares y Tecnología
NLP	Procesamiento de lenguaje natural
NoSQL	*Not only SQL*
OLTP	Procesamiento de transacciones en línea
OS	Sistema operativo
OSI	Interconexión de Sistemas Abiertos
OSS	Software de sistemas operativos
P2P	*Peer-to-Peer*
PaaS	Plataforma como servicio
PHP	Página de inicio personal (procesador de hipertexto)
PoP	Punto de presencia
POP	*Post Office Protocol*

PPP	*Point-to-Point Protocol*
PPTP	*Point-to-Point Tunneling Protocol*
RDBMS	Sistemas de gestión de bases de datos relacionales
RDP	*Remote Desktop Protocol*
RFP	Solicitud de propuesta
ROI	Retorno de la inversión
RPA	Automatización de procesos robóticos
SaaS	Software como servicio
SFTP	*Secure File Transfer Protocol*
SIEM	Gestión de eventos e información de seguridad
SLA	Acuerdo de nivel de servicio
SMTP	*Simple Network Management Protocol*
SNMP	*Simple Network Management Protocol*
SQL	*Structured Query Language*
SSH	*Secure Shell*
SSL	*Secure Socket Layer*
TCP	*Transmission Control Protocol*
TLS	*Transport Layer Security*
TUI	Interfaces de usuario de texto
UDP	*User Datagram Protocol*
USB	*Universal Service Bus*
vLAN	Red de área local virtual
VM	Máquina virtual
VMM	Monitor/administrador de máquina virtual
VoIP	*Voice over Internet Protocol*
VPN	Red privada virtual
WAF	Firewall de aplicaciones web
WAN	Red de área amplia
WEP	Privacidad equivalente por cable
WPA	Acceso protegido Wi-Fi
WPA2	Acceso protegido Wi-Fi 2
WPA3	Acceso protegido Wi-Fi 3
XaaS	"X" como servicio
XSS	Secuencias de comandos entre sitios

Apéndice D. Red de siete capas OSI

El apéndice proporciona los detalles de cada una de las siete capas del modelo de red de siete capas OSI, como se muestra en la Figura 11 de esta guía.

Descripción de la Red de Siete Capas OSI

Capa 1 — Física

Función: El trabajo de la capa física es proporcionar una ruta para la transmisión de datos.

Medios que implementan esta capa: alambre de cobre, cable de fibra óptica, ondas de radio o cualquier otro método capaz de transmitir datos.

Profesional que trabaja en este nivel: Ingeniero de Telecomunicaciones o Técnico de Telecomunicaciones.

La capa física puede ser muy costosa de actualizar. Se mantienen muchos métodos de red heredados para evitar el reemplazo de la infraestructura de Capa 1. La capa física existe en todos los tramos de la red y en los propios nodos. Los enrutadores y equipos de conmutación más antiguos pueden proporcionar una función limitada incluso con actualizaciones de software debido a sus limitaciones de Capa 1. Las tarjetas de interfaz de red (NIC) más antiguas pueden tener limitaciones similares. Los equipos más nuevos mantienen la compatibilidad con versiones anteriores para permitir el funcionamiento de la red en una infraestructura más antigua.

Capa 2 — Enlace de Datos

Función: La capa de enlace de datos controla la transmisión de datos a través de una ruta determinada. En términos de red, se trata de una transmisión de nodo a nodo.

Protocolos que implementan esta capa: Ethernet, Wi-Fi, *Address Resolution Protocol* (ARP) y otros**.**

Profesional que trabaja en este nivel: Ingeniero de redes o Técnico de redes.

La capa de enlace de datos se ocupa de organizar las transmisiones de la Capa 1 en datos utilizables. Los diferentes protocolos de Capa 2 utilizan diferentes métodos para hacerlo. Ethernet (definido por la Norma 802.3 del Instituto de Ingenieros Eléctricos y Electrónicos, por ejemplo, IEEE 802.3) divide los pulsos eléctricos en "tramas" que se pueden enviar y recibir a través de un enlace de Capa 1. Si las tramas no se reciben intactas, los protocolos de Capa 2 pueden corregirlo solicitando una retransmisión o aceptando fallas. La Capa 2 también controla la velocidad de transmisión para garantizar un servicio confiable; esto a menudo se denomina control de flujo.

Capa 3 — Red

Función: La capa de red se ocupa de direccionar computadoras individuales (también llamadas *hosts*) y enrutar conexiones en diferentes redes locales. En el uso común, un nodo es un punto en una red, pero un host es un sistema completamente funcional (no un dispositivo de red como un enrutador o una impresora) con una dirección de capa de red.

Protocolos que implementan esta capa: *Internet Protocol* (IP), *Internet Control Message Protocol* (ICMP), *Internet Protocol Security* (IPsec), *Internetwork Packet Exchange* (IPX) y otros.

Profesional que trabaja en este nivel: Ingeniero de red, administrador de red, criptógrafo o equipo de infraestructura de red.

La capa de red a menudo se asocia con direcciones IP, pero se entiende correctamente por la forma en que permite el enrutamiento a través de redes (es decir, *internetworking*). Se han propuesto y revisado numerosos métodos para lograr un enrutamiento más eficiente. Varias arquitecturas locales dependen de las características de enrutamiento de los protocolos utilizados en Layer3. Las redes troncales de conmutación de etiquetas multiprotocolo (MPLS) conectan oficinas y recursos de datos divididos geográficamente. La segregación de VLAN ayuda a dividir de manera virtual y flexible diferentes sistemas en una red para proteger los datos y equilibrar el uso de la infraestructura.

Riesgos de calidad, gestión y generación de informes de datos: "Si entra basura, sale basura" se refiere a la introducción de datos incorrectos en un sistema, lo cual dará como resultado una salida de datos incorrectos del sistema. Tener datos deficientes o problemas de calidad de datos puede generar informes de gestión inexactos y una toma de decisiones defectuosa. Las bases de datos que no están diseñadas para garantizar la integridad de los datos pueden resultar en datos incompletos o no válidos. Los análisis que se basan en datos no válidos probablemente producirán resultados defectuosos. Por lo tanto, el análisis de *big data* debe tener en cuenta estos riesgos de calidad de datos.

Además, los datos que no se obtienen y analizan de manera oportuna también pueden traducirse en resultados analíticos incorrectos, incorrectas decisiones de gestión y lucro cesante. Los datos obtenidos de terceros deben ser oportunos, precisos, completos y de fuente confiable. Los datos de terceros con formato inadecuado pueden no ser aptos para el análisis y retrasar la toma de decisiones de gestión.

Una vez que se han recibido y analizado los datos, puede resultar complicado garantizar que los usuarios finales gestionen y protejan los datos. La falta de controles informáticos para el usuario final puede generar informes inexactos y filtraciones de datos. Los informes de producción del usuario final, los informes ad hoc y los resultados analíticos predictivos deben revisarse y aprobarse para limitar las decisiones de gestión erróneas. Los informes de macrodatos también deben adherirse a las políticas de clasificación de datos de una organización para garantizar que solo se compartan los datos adecuados, tanto interna como externamente. Las opciones de informes y los canales de distribución podrían ser apropiados solo para datos de tamaños y formatos específicos. Las organizaciones podrían enfrentar obstáculos al determinar las opciones de informe y los canales adecuados para cada resultado analítico.

Capa 4 — Transporte

Función: La capa de transporte se ocupa de transmitir datos de un host a otro en una red o a través de redes con una calidad de servicio específica.

Protocolos que implementan esta capa: Protocolo de control de transmisión (TCP), Protocolo de datagramas de usuario (UDP) y otros.

Profesional que trabaja en este nivel: ingeniero de red, administrador de red, criptógrafo o equipo de infraestructura de red.

La capa de transporte se conoce principalmente por permitir que los hosts de la red utilicen y/o proporcionen múltiples servicios. Usando un ejemplo de TCP, un cliente realiza una solicitud a un servidor. El servidor está escuchando con una conexión abierta en un número de puerto conocido. Especificar el número de puerto en la solicitud permite al servidor identificar qué servicio se solicita. A continuación, el servidor responde al puerto de cliente apropiado, que puede asignarse de varias formas según el protocolo. La capa 4 especifica otros servicios como control de flujo para garantizar la velocidad sin abrumar al host, corrección de errores para identificar y reenviar paquetes defectuosos y otros.

Capa 5 — Sesión

Función: La capa de sesión proporciona servicios para la gestión de conexiones remotas en niveles de interacción muy básicos. La capa 5 es responsable de permitir la interacción de procesos locales y remotos.

Protocolos que implementan esta capa: *Remote Procedure Calls (*RPC), *AppleTalk Session Talk* (ASP), partes de TCP y otros.

Profesional que trabaja en este nivel: administrador de red, desarrollador de aplicaciones, criptógrafo o equipo de aplicaciones de red.

La capa de sesión incluye algunas de las funciones de TCP que proporcionan conexiones. En contraste, UDP proporciona un servicio "sin conexión" al tratar cada "datagrama" UDP (equivalente a un paquete TCP) como independiente de otros datagramas. Los flujos de paquetes TCP pueden ordenarse y retransmitirse si alguno se daña o se pierde. Los servicios de Capa 5 también establecen y rastrean múltiples conexiones entre hosts usando la misma aplicación (por ejemplo, descargando múltiples archivos simultáneamente usando el Protocolo de transferencia de archivos [FTP]). Algunas conexiones son sensibles para iniciar y detener o combinar múltiples flujos

de datos; la capa de sesión controla el inicio y la detención de los servicios para las aplicaciones que necesitan un flujo de datos controlado. Esta característica también permite la recuperación de sesiones interrumpidas.

Capa 6 — Presentación

Función: La capa de presentación se ocupa de tomar datos de una amplia variedad de fuentes de la capa de aplicación y hacer que los datos estén disponibles para otras aplicaciones y protocolos estándares de red. La capa de presentación representa una desviación de las capas asociadas con los datos en movimiento. La presentación se aplica tanto a los datos en reposo como a los datos en movimiento. La capa de presentación también coordina la encapsulación de los datos en reposo en archivos comprimidos, archivos cifrados y archivos compuestos (es decir, archivos que contienen otros archivos como archivos adjuntos de correo electrónico).

Protocolos que implementan esta capa: MIME, ASCII, Zip.

Profesional que trabaja en este nivel: Desarrollador de aplicaciones, Equipo de aplicaciones de red, Criptógrafo, Arquitecto de telecomunicaciones, Arquitecto de redes, Analista forense, Ingeniero de redes.

La capa de presentación se ocupa principalmente de la conversión de datos. Se utilizan numerosos protocolos de estandarización para garantizar la interoperabilidad entre sistemas y aplicaciones como ASCII y UNICODE. Si la conversión es posible entre dos de estos estándares, la capa de presentación realiza esta función, pero también se encarga de la compresión, descompresión, cifrado y descifrado, aunque todas estas tareas no son exclusivamente parte de esta capa.

Capa 7 — Aplicación

Función: Varias otras aplicaciones generan y consumen datos en este nivel. Esta capa es la más diversa, pero también la más familiar para los usuarios. Las aplicaciones que generan y modifican los datos del usuario implementan la capa de aplicación de la pila. Es una diferencia sutil, pero esta capa no son las aplicaciones en sí mismas; más bien, es el producto de datos formateados de esas aplicaciones.

Protocolos que implementan esta capa: *File Transfer Protocol* (FTP), *Hypertext Transfer Protocol* (HTTP), *Simple Mail Transfer Protocol* (SMTP) y muchos otros.

Profesional que trabaja en este nivel: Desarrollador de aplicaciones, Equipo de aplicaciones de red, Criptógrafo, Arquitecto de telecomunicaciones, Arquitecto de redes, Analista forense, Ingeniero de redes.

La capa de aplicaciones y la capa de presentación funcionan juntas en la mayoría de los casos. Las aplicaciones que organizan datos en formatos estándares para la interoperación utilizan formatos de archivo de capa de presentación. Estos formatos se abren al usuario mediante aplicaciones que conocen ese tipo de archivo. Por ejemplo, la mayoría de los usuarios asocian automáticamente la aplicación, MS Word, con el tipo de archivo ".docx". Estas dos capas tienen funciones distintas, pero difieren de las capas estrictamente de datos en movimiento: 2, 3, 4 y 5.

Apéndice E. El modelo de siete capas en acción

Este ejemplo representa dos hosts que se comunican a través de dos LAN. (Nota: este ejemplo ignora las complejidades del enrutamiento de Internet).

Ejemplo de dos hosts que se comunican a través de dos redes de área local (LAN)

Capa 7 — Aplicación

Datos del usuario (un gráfico).

Capa 6 — Presentación

El gráfico tiene formato JPG. No se produce ningún encapsulado; se trata de una transformación de un mapa de bits mostrado a un formato de almacenamiento. Puede almacenarse en un sistema de archivos o transferirse a través de una conexión de red.

Capa 5 — Sesión

Se aplica el cifrado *Secure Socket Layer* (SSL). No se produce ningún encapsulado; esta es una transformación dentro de una sesión. El otro extremo sabe cómo descifrarlo. Esta capa comienza las capas de datos en movimiento. Visualmente, el contenido se puede presentar como <DATA>. Para refuerzo visual, los corchetes rodean el contenido en este nivel. El siguiente nivel muestra cómo los metadatos de niveles superiores se tratan como contenido.

Capa 4 — Transporte

La información del encabezado TCP se agrega para identificar el puerto conectado del host receptor para recibir los datos cifrados. Los datos de la capa de sesión cifrados se convierten en los datos de carga útil de la encapsulación de la capa 4.
Visualmente, esto se puede abreviar como 4+ <DATA>, donde los corchetes definen los DATOS en este nivel.

Capa 3 — La Red

La información del encabezado IP se agrega a los datos recibidos en la pila desde la capa 4. Los datos de la capa de sesión combinados y los metadatos de la capa de transporte se convierten en los datos de carga útil de la encapsulación de la capa 3.
Visualmente, esto se puede abreviar como 3+ <4 DATA>. Los metadatos de la capa 4 ahora están entre corchetes, lo que significa que la capa 3 los trata como DATOS.

Capa 2 — Enlace de Datos

Los paquetes IP se dividen en tramas para su transmisión a través de la red de área local al conmutador que también sirve como enrutador. De manera similar a las capas de transporte y de red, tanto los datos originales como los metadatos de las capas superiores se tratan de la misma manera cuando se forman tramas de la capa de enlace de datos.
Visualmente, esto se puede abreviar como 2+ <3 4 DATA>. Todos los datos y metadatos anteriores están encapsulados por encabezados de capa 2.

Capa 1 — Física

Los marcos están codificados como forma de onda en los cables de cobre. No se lleva a cabo ningún encapsulado porque la capa uno simplemente transforma los datos en una señal portadora. Dado que todos los datos de los niveles superiores se tratan de la misma manera, los metadatos de los niveles superiores se consideran parte de los datos que vienen de la pila.
Una vez que se eliminan los metadatos relevantes para la capa actual, los datos restantes se elevan en la pila donde los metadatos de nivel superior se reconocen nuevamente como metadatos. Los dispositivos de red a menudo solo vuelven a subir por la pila a través de la capa 4; los datos de la capa de sesión rara vez se modifican en paradas intermedias entre los hosts.

Apéndice F. Descripciones de protocolos de red comunes

Estas definiciones se extrajeron del *Diccionario de Términos Informáticos e Internet* de Barron's Business Guide, Duodécima Edición, 2017.

servidor de nombres de dominio – un servidor responsable de traducir direcciones de dominio, como www.example.com, a números de IP (protocolo de Internet), como 127.192.92.95.

Ethernet – un tipo de red de área local desarrollada originalmente por Xerox Corporation. La comunicación se realiza mediante señales de radiofrecuencia transmitidas por un cable.

***File Transfer Protocol* (FTP)** – una forma estándar de transferir archivos de una computadora a otra en Internet y en otras redes TCP/IP.

***Hypertext Transfer Protocol* (HTTP)** – un método estándar para publicar información como hipertexto en formato HTML en Internet. HTTPS es una variación de HTTP que utiliza encriptación SSL por seguridad.

***Internet Mail Access Protocol* (IMAP)** – un protocolo para ver el correo electrónico en una computadora personal mientras se lo deja en su lugar en el sistema host.

***Post Office Protocol* (POP)** – un protocolo estándar para enviar correo electrónico a computadoras personales.

Secure Sockets Layer* (SSL) *Protocol – diseñado para proteger las conexiones entre clientes web y servidores web que se producen a través de una red insegura, como Internet.

***Simple Mail Transfer Protocol* (SMTP)** – protocolo que se utiliza para transferir correo electrónico entre computadoras en la Internet y otras redes TCP/IP.

***Transmission Control Protocol/Internet Protocol* (TCP/IP)** – un formato estándar para transmitir paquetes de datos de una computadora a otra. Las dos partes de TCP/IP son TCP, que se ocupa de la construcción de paquetes de datos, e IP, que los encamina de una máquina a otra.

Apéndice G. Comparación de bases de datos SQL y NoSQL

	Base de Datos SQL	Base de Datos NoSQL
Tipos	Un tipo (base de datos SQL) con variaciones menores.	Muchos tipos diferentes, incluidos almacenes de valores clave, bases de datos de documentos, almacenes de columnas anchas y bases de datos de gráficos.
Historia de Desarrollo	Desarrollado en la década de 1970 para hacer frente a la primera ola de aplicaciones de almacenamiento de datos.	Desarrollado en la década de 2000 para hacer frente a limitaciones de bases de datos SQL, especialmente en escala, replicación y almacen. de datos no estructurados.
Ejemplos	MySQL, Postgres, base de datos Oracle.	MongoDB, Cassandra, HBase, Neo4j.
Modelo de Almacenamiento de Datos	Los registros individuales (p. ej., "empleados") se almacenan como filas en tablas, y cada columna almacena un dato específico sobre ese registro (p. ej., "gerente", "fecha de contratación"), al igual que una hoja de cálculo. Los tipos de datos separados se almacenan en tablas separadas y luego se unen cuando se ejecutan consultas más complejas. Por ejemplo, las "oficinas" pueden almacenarse en una tabla y los "empleados" en otra. Cuando un usuario desea encontrar la dirección de trabajo de un empleado, el motor de la base de datos une las tablas "empleado" y "oficina" para obtener toda la información necesaria.	Varía según el tipo de base de datos NoSQL. Por ejemplo, los almacenes de clave-valor funcionan de manera similar a las bases de datos SQL, pero tienen solo dos columnas ("clave" y "valor"), con información más compleja a veces almacenada dentro de las columnas de "valor". Las bases de datos de documentos eliminan por completo el modelo de tabla y fila, almacenando todos los datos relevantes juntos en un solo "documento" en JSON, XML u otro formato, que puede anidar valores jerárquicamente.
Esquemas	La estructura y los tipos de datos se fijan de antemano. Para almacenar información sobre un nuevo elemento de datos, se debe modificar toda la base de datos, tiempo durante el cual la base de datos debe ponerse fuera de línea.	Suele ser dinámico. Los registros pueden agregar nueva información sobre la marcha y, a diferencia de las filas de la tabla SQL, los datos diferentes se pueden almacenar juntos según sea necesario. Para algunas bases de datos (por ejemplo, almacenes de columnas anchas), es algo más desafiante agregar nuevos campos de forma dinámica.
Escala	Verticalmente, lo que significa que un solo servidor debe ser cada vez más poderoso para hacer frente a la mayor demanda. Es posible distribuir bases de datos SQL en muchos servidores, pero generalmente se requiere una ingeniería adicional significativa.	Horizontalmente, lo que significa que, para agregar capacidad, un administrador de base de datos puede simplemente agregar más servidores básicos o instancias en la nube. La base de datos NoSQL distribuye datos automáticamente entre servidores según sea necesario.

Modelo de desarrollo	Mezcla de código abierto (Postgres, MySQL) y código cerrado (base de datos Oracle).	Fuente abierta.
Admite transacciones	Sí, las actualizaciones se pueden configurar para que se completen totalmente o para que no se completen.	En determinadas circunstancias y en determinados niveles (p. ej., nivel de documento frente a nivel de base de datos).
Manipulación de datos	Lenguaje específico que usa sentencias Seleccionar, Insertar y Actualizar, p. Ej. SELECCIONE campos DE la tabla DONDE [ingrese criterios específicos]	A través de API orientadas a objetos.
Consistencia	Puede configurarse para una gran consistencia.	Depende del producto.

Fuente: página web Mongo DB, https://www.mongodb.com/nosql-explained/nosql-vs-sql.

Apéndice H. Referencias y recursos adicionales

Referencias

Hall, Kaerrie. "*Customer Data Quality: The Good, the Bad, and the Ugly*." Validity. 5 de septiembre, 2019. https://www.validity.com/blog/customer-data-quality/.

Mell, Peter y Tim Grance, "La Definición de NIST de Cloud Computing," Laboratorio de Tecnología de la Información del NIST, Centro de Recursos de Seguridad Informática, SP 800-145, septiembre 2011. https://csrc.nist.gov/publications/detail/sp/800-145/final.

Recursos adicionales

Centro de Seguridad de Internet, https://www.cisecurity.org.

Alianza de Seguridad en la Nube, https://cloudsecurityalliance.org.

Downing, Douglas, Michael Covington, Ph.D., Melody Covington, Catherine Anne Barrett, y Sharon Covington. *Diccionario de Términos Informáticos e Internet,* Duodécima Edición. Hauppauge, NY: B.E.S. Publicación, 2017. https://www.simonandschuster.com/books/Dictionary-of-Computer-and-Internet-Terms/Douglas-Downing/Barrons-Business-Dictionaries/9781438008783.

Gibbs, Nelson, Divakar Jain, Amitesh Joshi, Surekha Muddamsetti, y Sarabjot Singh. *Una Nueva Guía del Auditor para Planificar, Realizar y Presentar Auditorías de TI*. Altamonte Springs, FL: La Fundación de Auditoría Interna, 2010. https://bookstore.theiia.org/a-new-auditors-guide-to-planning-performing-and-presenting-it-audits-8-3.

ISACA, https://www.isaca.org.

Instituto Nacional de Estándares y Tecnología (NIST), https://www.nist.gov.

Rai, Sajay, Philip Chukwuma, y Richard Cozart. *Seguridad y Auditoría de Dispositivos Inteligentes: Gestión de la Proliferación de Datos Confidenciales en Dispositivos Corporativos y BYOD*. Boca Raton, FL: CRC Prensa, 2016. https://bookstore.theiia.org/security-and-auditing-of-smart-devices-managing-proliferation-of-confidential-data-on-corporate-and-byod-devices.

Sigler, Ken y Dr. James L. Rainey III. *Asegurar una Organización de TI a través del Gobierno, la Gestión de Riesgos y la Auditoría*. Boca Raton, FL: CRC Prensa, 2015. https://bookstore.theiia.org/securing-an-it-organization-through-governance-risk-management-and-audit.

Agradecimientos

Equipo de desarrollo de las guías

Susan Haseley, CIA, EE. UU. (Presidente)
Sajay Rai, CISM, CISSP, EE. UU. (Líder de Proyecto)
Brad Ames, EE. UU.
Michael Lynn, CIA, CRMA, EE. UU.
Avin Mansookram, Sudáfrica
Gerard Morisseau, EE. UU.
Justin Pawlowski, CIA, CRMA, Alemania

Colaboradores

Lee Keng "Joyce" Chua, CIA, Singapur
James Enstrom, CIA, EE. UU.
Scott Moore, CIA, EE. UU.
Shawna Flanders, Directora de Currículo de TI, Colaboradora del Plantel IIA

Normas y guías globales del IIA

P. Michael Padilla, CIA, Director (Líder de Proyecto)
Jim Pelletier, Vicepresidente
Anne Mercer, CIA, CFSA, Directora
Chris Polke, CGAP, PS Director
Jeanette York, CCSA, FS Directora
Shelli Browning, Editora Técnica
Lauressa Nelson, Editora Técnica
Geoffrey Nordhoff, Desarrollador de Contenido y Escritor Técnico
Christine, Janesko, Desarrolladora de Contenido y Escritora
Vanessa Van Natta, Especialista en Normas y Guías

El IIA desea agradecer a los siguientes organismos de supervisión por el apoyo brindado: Comité de Desarrollo de Guías de Tecnología de la Información, Consejo Asesor de Orientación Profesional, Consejo de Normas Internacionales de Auditoría Interna, Comité de Responsabilidad y Ética Profesional, y Consejo de Supervisión del Marco Internacional de Prácticas Profesionales.

Sobre el IIA

El Instituto de Auditores Internos (IIA) es la organización más ampliamente reconocida en la defensa, educación y emisión de normas, orientación y certificaciones de la profesión de auditoría interna. Fundado en 1941, el IIA hoy brinda servicio a más de 190.000 miembros de 170 países y territorios. Tiene su sede mundial en Lake Mary, Florida, Estados Unidos. Más información: www.globaliia.org.

Limitación de responsabilidad

El IIA publica este documento con fines informativos y educativos. Este material no está destinado a proporcionar respuestas definitivas a circunstancias individuales específicas y, como tal, solo debe usarse como una guía. El IIA recomienda buscar el asesoramiento de expertos independientes que se relacionen directamente con cualquier situación específica. El IIA no acepta responsabilidad alguna en casos que esta guía sea tomada como única referencia.

Copyright

Junio 2020

Traducción al Español Auspiciada por:
FLAI
FUNDACIÓN LATINOAMERICANA DE AUDITORES INTERNOS

The Institute of Internal Auditors | Global

Sede Mundial
Instituto de Auditores Internos
1035 Greenwood Blvd., Suite 149
Lake Mary, FL 32746, USA
Tel.: +1-407-937-1111
Fax: +1-407-937-1101
www.globaliia.org