UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

Evaluación de la efectividad de controles tecnológicos bajo el marco de las normas internacionales

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniero en Telecomunicaciones

P R E S E N T A

Rafael Amarillas Carrillo

ASESOR DE INFORME

Ing. Carlos Gabriel Girón García

Ciudad Universitaria, Cd. Mx., 2026

PROTESTA UNIVERSITARIA DE INTEGRIDAD Y HONESTIDAD ACADÉMICA Y PROFESIONAL
(Titulación con trabajo escrito)

De conformidad con lo dispuesto en los artículos 87, fracción V, del Estatuto General, 68, primer párrafo, del Reglamento General de Estudios Universitarios y 26, fracción I, y 35 del Reglamento General de Exámenes, me comprometo en todo tiempo a honrar a la institución y a cumplir con los principios establecidos en el Código de Ética de la Universidad Nacional Autónoma de México, especialmente con los de integridad y honestidad académica.

De acuerdo con lo anterior, manifiesto que el trabajo escrito titulado EVALUACION DE LA EFECTIVIDAD DE CONTROLES TECNOLOGICOS BAJO EL MARCO DE LAS NORMAS INTERNACIONALES que presenté para obtener el titulo de INGENIERO EN TELECOMUNICACIONES es original, de mi autoría y lo realicé con el rigor metodológico exigido por mi Entidad Académica, citando las fuentes de ideas, textos, imágenes, gráficos u otro tipo de obras empleadas para su desarrollo.

En consecuencia, acepto que la falta de cumplimiento de las disposiciones reglamentarias y normativas de la Universidad, en particular las ya referidas en el Código de Ética, llevará a la nulidad de los actos de carácter académico administrativo del proceso de titulación.

Rafael A

RAFAEL AMARILLAS CARRILLO
Número de cuenta: 317217515

Contenido

Introducción

En la actualidad, la operación de las organizaciones depende de sistemas de información interconectados que soportan procesos críticos y gestionan datos con alto valor para el negocio. Esta dependencia tecnológica ha incrementado la exposición a riesgos los cuales pueden impactar la continuidad del servicio, la integridad de la información y la confianza en los resultados que producen los sistemas (National Institute of Standards and Technology, 2018).

Ante este escenario, la seguridad de la información se entiende como un conjunto de prácticas técnicas y de gestión orientadas a proteger la información y los sistemas que la soportan. Dentro de estas prácticas, la evaluación de la efectividad de los controles tecnológicos resulta de suma importancia, ya que permite verificar, con base en evidencia, si los controles implementados sobre sistemas críticos operan como se espera y si contribuyen a mitigar los riesgos asociados al uso de tecnología en la operación. Asimismo, la existencia de políticas, procedimientos y estándares es requerida para asegurar que los controles se apliquen de manera consistente y alineada con los objetivos de la organización (Landoll, 2017).

En términos de referencia técnica, la norma ISO/IEC 27001 ofrece un marco reconocido para estructurar conceptos relacionados con la gestión de riesgos y la definición de controles de seguridad dentro de un Sistema de Gestión de Seguridad de la Información (SGSI). De forma complementaria, la ISO/IEC 27002 establece lineamientos para la selección e implementación de controles organizacionales, físicos y tecnológicos, partiendo de una evaluación de riesgos y de las necesidades particulares de cada organización. En este trabajo, dichas normas se utilizan como referencias para contextualizar la seguridad de la información y la lógica en sí de los controles tecnológicos; sin embargo, no representan un proceso formal de certificación ni el esquema bajo el cual se ejecutaron las actividades profesionales descritas (UNE, 2017; International Organization for Standardization, 2022; Calder & Watkins, 2022).

Por otro lado, la Ley Sarbanes–Oxley (SOX) establece requerimientos de control interno sobre la información financiera en organizaciones sujetas a sus requerimientos, las cuales son aquellas que tienen operaciones en los Estados Unidos. Su cumplimiento depende en gran medida de la confiabilidad de los sistemas de información que soportan los procesos empresariales. Por ello, los controles tecnológicos asociados a accesos, segregación de funciones, administración de cambios, monitoreo y operación de plataformas adquieren un papel central para asegurar que la información que circula sobre estos sistemas se mantenga íntegra, disponible y trazable (IBM, 2025; Microsoft, s. f.; PCAOB, 2010).

Durante mi experiencia profesional, participé en actividades enfocadas en la evaluación de la efectividad operativa de controles tecnológicos dentro de proyectos alineados con requerimientos de control interno. Esta experiencia me permitió aplicar de forma práctica los conocimientos adquiridos durante mi formación como Ingeniero en Telecomunicaciones, particularmente en redes, infraestructura tecnológica y administración de sistemas, integrando un enfoque analítico para interpretar configuraciones, comprender flujos de información y documentar resultados de manera sustentada.

Capítulo 1. Evaluación de los Controles de Seguridad de la Información

1.1 Importancia de Contar con Controles de Seguridad de la Información

Dado que los sistemas de información se han convertido en uno de los pilares principales para la operación de las organizaciones, los procesos financieros, administrativos, operativos y estratégicos dependen directamente de plataformas tecnológicas que almacenan, procesan y transmiten información crítica, la seguridad de la información deja de ser un aspecto exclusivamente técnico y da pie a convertirse un elemento fundamental para la estabilidad y continuidad del negocio.

Los controles de seguridad de la información surgen como mecanismos diseñados para reducir los riesgos asociados al uso de la tecnología en sistemas críticos. Estos controles buscan prevenir el fraude corporativo, por lo que sin su existencia, las organizaciones quedan expuestas a pérdidas económicas, interrupciones operativas y daños a su reputación.

De acuerdo con Landoll (2017), los controles son más efectivos cuando forman parte de un enfoque estructurado y alineado con las necesidades de la organización. Esto implica que los controles no deben implementarse de forma aislada, sino integrarse dentro de políticas, procedimientos y estándares que definan responsabilidades, lineamientos y mecanismos de supervisión.

Asimismo, de acuerdo con la ISO/IEC 27001, los controles de seguridad deben establecerse con base en una evaluación de riesgos, considerando el contexto de la organización y la criticidad de la información y de los sistemas involucrados. Esto significa que no existe un conjunto único de controles aplicable a todas las organizaciones, sino que estos deben seleccionarse y adaptarse de acuerdo con los riesgos identificados y con los objetivos del negocio.

En entornos empresariales complejos, donde múltiples aplicaciones, plataformas y usuarios interactúan de forma simultánea, la ausencia de controles adecuados puede generar inconsistencias, errores y vulnerabilidades difíciles de detectar. Calder y Watkins (2022) señalan que la efectividad de los controles depende de que estos se encuentren integrados dentro de un esquema de gestión de riesgos y de mejora continua, permitiendo

que la organización mantenga la integridad, disponibilidad y confiabilidad de la información.

1.2 Controles Tecnológicos y su Relación con los Sistemas de Información

Los controles tecnológicos son medidas técnicas y procedimentales que se implementan dentro de los sistemas de información para prevenir el uso indebido de la tecnología y reducir los riesgos asociados a su operación. Estos controles pueden estar integrados directamente en las aplicaciones, configurados a nivel de infraestructura o definidos como parte de las políticas de la organización que regulan el uso de los sistemas.

Según la ISO/IEC 27002, los controles tecnológicos pueden agruparse en controles organizacionales, físicos y tecnológicos, los cuales deben implementarse de manera conjunta para proteger la confidencialidad, integridad y disponibilidad de la información. Por lo que estos no actúan de forma aislada, sino como conjunto interrelacionado de mecanismos que trabajan de manera conjunta para mitigar riesgos.

Por ejemplo, un control de acceso puede limitar quién utiliza una aplicación, mientras que un control de cambios asegura que las modificaciones realizadas no afecten su estabilidad o seguridad. Del mismo modo, los registros de actividad permiten monitorear las acciones realizadas por los usuarios y facilitan la identificación de comportamientos inusuales o no autorizados.

Calder y Watkins (2022) indican que la relación entre controles tecnológicos y sistemas de información es importante en las organizaciones donde múltiples aplicaciones intercambian datos entre sí, ya que una debilidad en un solo sistema puede afectar la confiabilidad de otros procesos o plataformas relacionadas. Por esta razón, los controles tecnológicos deben analizarse considerando la forma en que los sistemas interactúan y la dependencia existente entre ellos.

Desde una perspectiva técnica, los controles tecnológicos también permiten traducir políticas y lineamientos generales en mecanismos concretos dentro de los sistemas. Landoll (2017) señala que una política de seguridad únicamente puede ser efectiva cuando se

transforma en controles específicos dentro de aplicaciones, bases de datos, servidores o infraestructura tecnológica.

1.3 Evaluación de la Efectividad Operativa de los Controles

La existencia de controles tecnológicos no garantiza por sí sola que los riesgos estén adecuadamente mitigados. Para que un control cumpla su propósito, es necesario que funcione de manera consistente y conforme a lo esperado durante la operación normal de los sistemas. Por esta razón, es que se debe evaluar su efectividad operativa de manera constante.

La evaluación consiste en analizar si un control tecnológico realmente cumple su función en la práctica. Este análisis se basa en la revisión de evidencia generada por los sistemas y los procesos operativos, como registros, reportes, configuraciones y autorizaciones. El objetivo no es rediseñar ni implementar controles, sino verificar que aquellos que existen operen de forma adecuada. De acuerdo con Landoll (2017), uno de los problemas más frecuentes consiste en asumir que un control es efectivo únicamente porque se encuentra documentado, cuando en realidad puede no ejecutarse de manera consistente.

Este tipo de evaluaciones permite identificar situaciones en las que un control está documentado, pero no se aplica correctamente, o bien, casos en los que el control existe, pero no se ejecuta de manera continua. Detectar estas diferencias es importante para entender el nivel real de robustez tecnológica de una organización y su capacidad para gestionar riesgos.

Además, la evaluación de la efectividad operativa aporta un enfoque objetivo al análisis de la seguridad de la información, ya que se fundamenta en evidencia verificable y no únicamente en declaraciones o políticas formales. De acuerdo con la ISO/IEC 27001, la revisión y monitoreo de los controles debe realizarse de forma continua, como parte del ciclo de mejora del SGSI (UNE, 2017).

1.4 Relación entre los marcos de control de auditoría SOX y la norma ISO/IEC 27001 en la evaluación de controles tecnológicos

La Ley Sarbanes–Oxley (SOX) establece requerimientos en materia de control interno con el objetivo de asegurar la confiabilidad de la información financiera y reducir el riesgo de errores o posibles fraudes. Aunque su origen se encuentra en el ámbito financiero, la efectividad de estos controles depende directamente de los sistemas de información que procesan, almacenan y generan dicha información, así como de los responsables de la ejecución, mantenimiento y desarrollo de estos, que en la mayoría de los casos suelen ser profesionales de la Ingeniería (IBM, 2025; PCAOB, 2010).

En este sentido, los sistemas tecnológicos representan un punto neural dentro de SOX, ya que cualquier falla en su operación, configuración o control puede derivar en información incorrecta, manipulada o incompleta. Por ello, la evaluación de controles tecnológicos se vuelve fundamental para mitigar riesgos que puedan impactar la integridad de los reportes financieros.

Por su parte, la norma ISO/IEC 27001 proporciona un marco reconocido para la gestión de la seguridad de la información, enfocado en la protección de la confidencialidad, integridad y disponibilidad de los datos, permitiendo así estructurar de manera ordenada la gestión de riesgos y los controles que soportan los sistemas de información utilizados dentro de esquemas de control interno (UNE, 2017).

De acuerdo con Calder y Watkins (2022), la ISO/IEC 27001 funciona como un marco conceptual que complementa los esquemas de evaluación utilizados en auditorías asociadas a SOX, aportando una visión técnica sobre la gestión de riesgos y la protección de la información. Mientras que SOX se orienta a validar la efectividad operativa de los controles para prevenir errores o fraudes, la ISO/IEC 27001 proporciona una base estructurada para comprender cómo dichos controles contribuyen a la seguridad de la información.

Con el propósito de sintetizar esta relación, la Tabla 1 presenta una correspondencia técnica de alto nivel entre la norma ISO/IEC 27001 y los marcos utilizados en auditorías SOX y SOC, considerando su aplicación en la evaluación de controles tecnológicos.

Elemento técnico	ISO/IEC 27001	SOX / SOC
Naturaleza del marco	Norma técnica internacional	Marco de evaluación de controles
Enfoque principal	Gestión estructurada de riesgos de información	Validación de controles en operación
Alcance técnico	Políticas, procesos y controles de seguridad	Controles tecnológicos que soportan procesos críticos
Definición de controles	Proporciona controles de referencia	Evalúa controles existentes
Tipo de actividades	Análisis y referencia conceptual de controles	Revisión, verificación y documentación de controles en operación
Evidencia técnica	Políticas, matrices de riesgo, procedimientos	Registros del sistema, aprobaciones, reportes
Rol del ingeniero	Analizar y estructurar controles	Evaluar y validar su funcionamiento
Uso en este trabajo	Marco técnico de referencia	Contexto operativo de la experiencia

Tabla 1: Comparación técnica entre ISO/IEC 27001 y marcos utilizados en auditorías SOX / SOC.

Fuente: Elaboración propia con base en UNE (2017), International Organization for Standardization (2022), IBM (2025), Public Company Accounting Oversight Board (2010) y Calder y Watkins (2022).

1.5 Relevancia del enfoque técnico en la evaluación de controles

La evaluación de controles tecnológicos requiere un enfoque técnico que permita comprender el funcionamiento interno de los sistemas y su interacción con los procesos del negocio. No se trata únicamente de revisar documentos, sino de interpretar configuraciones, flujos de información y evidencias generadas por los propios sistemas, lo cual permite identificar riesgos que no siempre son evidentes a nivel administrativo, así como evaluar la lógica entre los controles implementados y el entorno tecnológico en el que operan.

De acuerdo con Calder y Watkins (2022), la efectividad de un control depende en gran medida de comprender la forma en que los sistemas se relacionan entre sí, así como los puntos donde la información es transferida, modificada o procesada. Por esta razón, la evaluación de controles tecnológicos requiere analizar no solo cada sistema de manera individual, sino también las interacciones existentes entre aplicaciones, bases de datos, servicios e infraestructura.

Asimismo, Landoll (2016) señala que un enfoque técnico adecuado permite traducir políticas y lineamientos generales en mecanismos concretos dentro de los sistemas para determinar si los controles realmente mitigan los riesgos para los cuales fueron diseñados.

Capítulo 2. El Sistema de Gestión de Seguridad (SGSI)

2.1 Concepto y propósito de un Sistema de Gestión de Seguridad de la Información (SGSI)

De acuerdo con el Colegio Oficial Ingenieros en Telecomunicación (2022), un Sistema de Gestión de Seguridad de la Información (SGSI) es la parte de un sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información.

A diferencia procesos aislados, un SGSI plantea un enfoque integral y estructurado, sin limitarse a la implementación de controles tecnológicos para incorporar también elementos organizacionales que repercuten en la operación. De esta forma, la seguridad de la información deja de depender exclusivamente de soluciones técnicas y se convierte en una responsabilidad de múltiples equipos.

La ISO/IEC 27001 establece que un SGSI debe permitir identificar la información crítica, analizar los riesgos asociados y definir los controles necesarios para reducir dichos riesgos a niveles aceptables. Asimismo, los controles deben supervisarse y revisarse de forma continua para asegurar que sigan siendo adecuados frente a los cambios en el entorno y en las necesidades de la organización (UNE, 2017).

2.2 Enfoque Basado en Riesgos dentro del Sistema de Gestión de Seguridad de la Información (SGSI)

Uno de los pilares de un SGSI es el enfoque basado en riesgos, ya que este parte de la idea de que no todos los activos de información tienen el mismo nivel de criticidad ni se encuentran expuestos a las mismas amenazas. Por ello, es necesario identificar qué información es más relevante para la organización y cuáles son los riesgos que podrían afectarla. Teniendo esto en cuenta, es posible evaluar la probabilidad de ocurrencia de eventos adversos y el impacto que estos tendrían sobre la operación, teniendo como resultado el establecimiento de controles orientados a mitigar sus riesgos asociados.

En función de los riesgos identificados, para cada tipo de organización se lleva a cabo esta fase de establecimiento de dichos controles, lo cual permite evitar la aplicación de medidas innecesarias para concentrar así los esfuerzos en procesos, sistemas y activos que representan un mayor riesgo (UNE, 2017).

2.3 Relación entre el SGSI y los Controles Tecnológicos

Dentro de un SGSI, los controles tecnológicos representan la herramienta más importante para la protección de la información, sin embargo, su éxito depende de qué tan alineados con las políticas y procesos previamente definidos. El SGSI proporciona el marco necesario para que estos controles operen como se espera, más si se encuentran en entornos en donde múltiples sistemas y aplicaciones interactúan entre sí, ya que un riesgo no mitigado dentro de un sistema puede afectar el funcionamiento de otros que estén relacionados. Calder y Watkins (2022) destacan esta relación como uno de los principales retos en organizaciones con infraestructuras complejas.

Por otra parte, la ISO/IEC 27002 plantea que los controles tecnológicos no deben analizarse de forma aislada, sino integrarse con controles organizacionales y operativos, debido a que la seguridad de la información depende de la interacción entre personas, procesos y tecnología (International Organization for Standardization, 2022).

2.4 Norma ISO/IEC 27001 como Referencia para el Sistema de Gestión de Seguridad de la Información (SGSI)

La norma ISO/IEC 27001 es uno de los estándares internacionales más reconocidos para la implementación de un SGSI. Esta norma establece los requisitos para definir, implementar, mantener y mejorar un SGSI de forma ordenada y continua.

La ISO/IEC 27001 propone un marco en donde se integra la seguridad de la información dentro de los procesos operativos de la organización, lo que permite identificar los riesgos y definir los controles que resulten más adecuados.

De acuerdo con UNE (2017), uno de los elementos centrales de la norma consiste en que esta definición de controles debe justificarse con base en una evaluación de riesgos, lo cual permite que el SGSI sea adaptable a distintos tipos de organizaciones. Este enfoque se complementa con los principios de gestión de riesgos establecidos en ISO 31000, los cuales permiten priorizar amenazas y definir estrategias de tratamiento de manera consistente (ISO, 2018).

Aunado a lo anterior, Calder y Watkins (2022) consideran que una de las principales fortalezas de la ISO/IEC 27001 radica en que proporciona una estructura clara para vincular la seguridad de la información con los objetivos del negocio, permitiendo que las decisiones relacionadas con controles, riesgos y recursos se encuentren alineadas con las necesidades de cada organización.

2.5 El ciclo PDCA (Plan-Do-Check-Act) como Base del Sistema de Gestión de Seguridad de la Información (SGSI)

El funcionamiento de un SGSI puede entenderse de mejor manera haciendo uso del ciclo PDCA (Plan–Do–Check–Act). Rodríguez Garraza (2017) explica que el ciclo PDCA está compuesto por cuatro etapas que se desarrollan de forma cíclica: planificar, ejecutar, verificar y actuar, que adaptado a este trabajo y su aplicación dentro de un SGSI se puede explicar de la siguiente manera:

• Plan (Planificar): Etapa donde se asocia un riesgo a un determinado control (haciendo uso de una matriz de riesgos), los objetivos de seguridad, así como los controles necesarios para mitigarlos.

• Do (Hacer): Etapa donde se implementan los controles y procedimientos definidos dentro de una organización.

• Check (Verificar): Etapa donde se revisa el funcionamiento de los controles mediante el análisis de evidencia y resultados.

• Act (Actuar): Etapa donde se realizan ajustes y mejoras a partir de las deficiencias o áreas de oportunidad identificadas.

Es por eso que, dentro de un SGSI, el ciclo PDCA permite que la seguridad de la información sea vista como un proceso permanente de revisión y mejora. La ISO/IEC 27001 incorpora este enfoque para asegurar que los controles continúen siendo adecuados frente a los cambios en los riesgos y en el entorno de una organización (UNE, 2017).

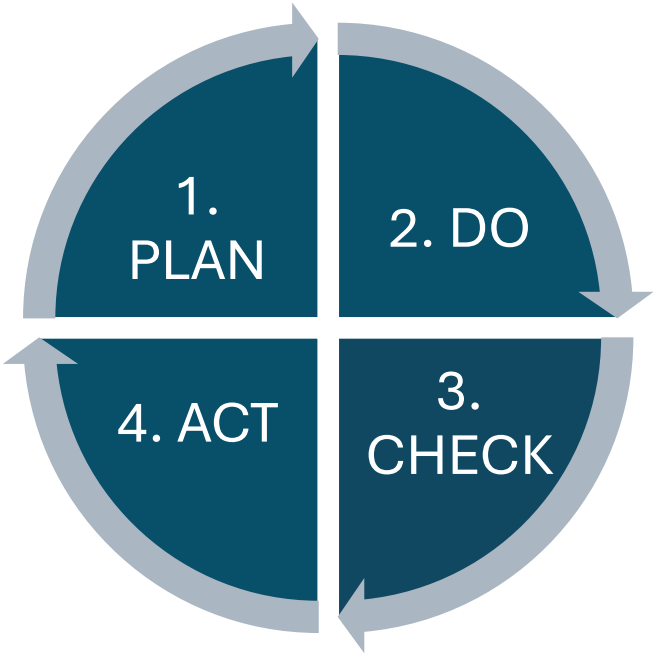

Figura 1: Diagrama del ciclo PDCA

Fuente: Elaboración propia con base en Rodríguez Garraza (2017) y Asociación Española de Normalización (UNE, 2017).

2.6 Importancia del Sistema de Gestión de Seguridad de la Información (SGSI) en Entornos Empresariales Actuales

En el contexto actual donde la transformación digital avanza de forma acelerada, el SGSI se vuelve una herramienta indispensable para garantizar la estabilidad operativa de las organizaciones. La dependencia de plataformas tecnológicas, servicios en la nube y sistemas interconectados incrementa la exposición a riesgos, por lo cual Calder y Watkins (2022) destacan que contar con un SGSI adquirió una mayor relevancia dado que las organizaciones incrementan su dependencia de estos sistemas interconectados y servicios tecnológicos distribuidos en múltiples plataformas.

Contar un SGSI bien estructurado permite responder de manera ordenada ante incidentes, reducir el impacto de fallas tecnológicas y mantener la confianza de clientes, socios, autoridades regulatorias, además de facilitar la alineación entre los objetivos del negocio y las estrategias de seguridad de la información. Este requerimiento de coordinación y supervisión continua forma parte de los principios establecidos en la ISO/IEC 27001 (UNE, 2017).

Desde una perspectiva técnica, se puede comentar que el SGSI proporciona el marco para evaluar la efectividad de los controles, tal como señala Landoll (2017), la utilidad de estos depende no solo de su existencia, sino de que se encuentren alineados con los riesgos y se revisen de forma periódica para confirmar que continúan siendo efectivos.

Capítulo 3. Seguridad de la Información en México

3.1 Contexto nacional de la seguridad de la información en México

En México, la seguridad de la información adquirió mayor relevancia creciente conforme las organizaciones han incrementado su dependencia de los sistemas tecnológicos para soportar sus operaciones. Como se ha mencionado anteriormente, la digitalización de procesos, el uso de plataformas en la nube y la interconexión entre sistemas han permitido mejorar la eficiencia operativa, pero también han incrementado la exposición a riesgos cibernéticos que pueden traer consigo consecuencias perjudiciales para las organizaciones.

A nivel nacional, la gestión de la seguridad de la información se ha desarrollado de manera heterogénea, donde por una parte algunas organizaciones han adoptado estándares internacionales y esquemas formales de gestión, otras continúan operando con enfoques reactivos, basados principalmente en controles técnicos aislados o en medidas correctivas posteriores a incidentes. Como consecuencia, existen diferencias importantes en el nivel de madurez y protección entre organizaciones.

Ante la ausencia de una regulación única en materia de seguridad de la información, las empresas mexicanas suelen apoyarse en marcos de referencia internacionales para estructurar sus operaciones; los cuales proporcionan criterios para identificar riesgos, definir controles y supervisar su funcionamiento, aun cuando su adopción no sea obligatoria.

3.2 Aplicación de la ISO/IEC 27001 en el Entorno Empresarial Mexicano

Dentro del entorno empresarial mexicano, la norma ISO/IEC 27001 se consolidó como una de las principales referencias para la gestión de la seguridad de la información. Su aplicación es más frecuente en organizaciones que manejan información sensible o que dependen de la continuidad de sus servicios, tales como instituciones financieras, empresas tecnológicas y proveedores de telecomunicaciones.

La norma propone una transición desde un enfoque reactivo hacia uno preventivo. A través de la identificación de activos de información, el análisis de riesgos y la selección de

controles, las organizaciones pueden gestionar la seguridad de manera más estructurada y alineada con sus objetivos. Es por eso por lo que más allá de la certificación formal, la ISO/IEC 27001 funciona como una guía para ordenar procesos, asignar responsabilidades y fortalecer la gobernanza tecnológica.

No obstante, su implementación enfrenta diversos retos. Entre los más comunes se encuentran la falta de personal especializado, la escasa documentación en procesos y una cultura organizacional que todavía subestima los riesgos tecnológicos.

3.3 Seguridad de la Información y Telecomunicaciones en México

La seguridad de la información mantiene una relación estrecha con el sector de telecomunicaciones, ya que gran parte de los procesos empresariales dependen de redes, enlaces de comunicación, servidores y servicios de conectividad para operar de forma continua.

En México, las empresas de telecomunicaciones administran infraestructuras críticas que soportan servicios como lo son la telefonía móvil y el acceso a internet. Debido a ello, una interrupción ocasionada por fallas técnicas o incidentes de seguridad puede generar impactos significativos tanto para las organizaciones como para los usuarios.

Desde la perspectiva técnica de las telecomunicaciones, la protección de la información depende de elementos como la segmentación de redes, la administración de firewalls, la redundancia de enlaces, el monitoreo del tráfico y el control de accesos sobre la infraestructura.

Por otra parte, la aplicación de marcos como la ISO/IEC 27001 permite establecer responsabilidades, definir procedimientos y evaluar de manera ordenada si los controles tecnológicos operan conforme a lo esperado, de tal manera que la seguridad de la información y las telecomunicaciones se integran dentro de una misma estrategia de gestión (ISO, 2022; Landoll, 2017).

3.4 Relación entre la Ley Sarbanes–Oxley (SOX) y la Seguridad de la Información en México

Aunque la Ley Sarbanes–Oxley (SOX) es una regulación estadounidense, sus principios son útiles para organizaciones mexicanas que forman parte de grupos internacionales, cotizan en mercados extranjeros o prestan servicios a empresas sujetas a esta regulación.

Dicha ley enfatiza la necesidad de contar con controles confiables sobre los sistemas que procesan información crítica, puntualmente en esa que impacta la elaboración de reportes, la toma de decisiones y la rendición de cuentas. En consecuencia, situaciones como el control de accesos, la segregación de funciones, la administración de cambios, la generación de respaldos y la conservación de evidencia se vuelven un factor a importante a tomar en cuenta.

Diversos proveedores tecnológicos han señalado que el cumplimiento de SOX depende en gran medida de la existencia de controles tecnológicos bien definidos. IBM (2025) destaca que los riesgos relacionados con accesos indebidos, modificaciones no autorizadas o falta de trazabilidad pueden afectar la confiabilidad de la información. Por su parte, Microsoft (2024) señala que, en entornos donde se utilizan servicios en la nube, la responsabilidad sobre los controles debe compartirse entre la organización y el proveedor.

En México, la adopción voluntaria de principios similares a los utilizados en proyectos alineados con SOX puede representar una oportunidad para fortalecer la supervisión de los sistemas y mejorar la confiabilidad de la información, incluso en organizaciones que no se encuentran obligadas a cumplir formalmente con esta Ley.

3.5 Aportación de los Esquemas de Evaluación de Controles al Contexto Mexicano

La combinación de marcos de gestión, como la ISO/IEC 27001, con esquemas de evaluación de controles inspirados en enfoques como SOX, ofrecen una base para fortalecer la seguridad de la información en el entorno empresarial de nuestro país.

Mientras la ISO/IEC 27001 permite identificar riesgos, definir controles y organizar la gestión de la seguridad, la evaluación de controles aporta un elemento adicional: la

verificación de que dichos controles realmente operan de manera consistente y cumplen con el propósito para el que fueron establecidos.

En muchas organizaciones mexicanas existen políticas, procedimientos y configuraciones formalmente definidos; sin embargo, no siempre se cuenta con mecanismos suficientes para comprobar si estos operan de manera adecuada en la práctica. La revisión de evidencia, registros, configuraciones y actividades realizadas dentro de los sistemas permite identificar diferencias entre lo establecido y la operación real para llegar a una conclusión: los controles se están ejecutando de manera correcta o se deben hacer cambios para que lo hagan.

Capítulo 4. Validación y Desarrollo del Proyecto

4.1 Contexto Tecnológico y Desarrollo de Actividades

La experiencia profesional descrita en este trabajo tuvo lugar dentro de una organización dedicada a la prestación de servicios profesionales, más puntualmente relacionados con consultoría y auditoría. Durante el periodo comprendido entre febrero de 2025 y finales de diciembre del mismo año, el cual fue el momento en el desarrollé el escrito; participé bajo el rol de becario en proyectos vinculados con la evaluación de controles tecnológicos para así determinar la confiabilidad de la información utilizada por distintas organizaciones con énfasis en procesos relacionados con sus estados financieros.

Identifiqué distintos entornos empresariales con arquitecturas tecnológicas complejas, integradas por múltiples plataformas, aplicaciones y componentes de infraestructura que soportaban procesos críticos de negocio. En dichos entornos, los sistemas de información constituían un elemento principal con impacto en la operación diaria.

Participé en la evaluación de la efectividad de controles embebidos dentro de sistemas Enterprise Resource Planning (ERP), que son utilizados para integrar y gestionar procesos financieros, operativos y administrativos, así como en sistemas Customer Relationship Management (CRM), que están orientados a la administración de relaciones con clientes y manejo de información comercial. Estos controles se encontraban integrados en la configuración funcional del sistema y regulaban aspectos como, por mencionar algunos ejemplos: la gestión de usuarios, la asignación de roles, la segregación de funciones, la autorización de transacciones.

En el caso de los controles automatizados de aplicación (ITACs), principalmente establecidos con relación a asuntos financieros, em donde se debe tener la menor intervención humana posible, evalué fórmulas y configuraciones que permitían validar de forma automática la integridad y consistencia de la información procesada por los sistemas. Estas evaluaciones incluyeron el análisis de parámetros de configuración, dependencias entre módulos, flujos de información y controles de validación que se ejecutaban sin intervención manual.

Como segundo punto, participé en actividades relacionadas con el ciclo de vida del desarrollo de software (Software Development Life Cycle, SDLC), el cual comprende las etapas de análisis, diseño, desarrollo, pruebas, implementación y mantenimiento de sistemas, en donde al igual que para un ITAC, evalué la documentación proporcionada para cada etapa del mismo, de tal forma que quedara sustentado que la migración de desarrollos a ambientes productivos estuviera acordemente probada, documentada y autorizada antes de su implementación reduciendo el riesgo de fallas operativas o impactos no controlados en los sistemas productivos.

Por otra parte, también participé en evaluaciones en torno a Controles Generales de IT (ITGC) los cuales se refieren a controles semi automáticos, es decir, que se tiene intervención humana e intervención por parte de un sistema. Están diseñados para operar sobre sistemas (CRM y ERP) y es importante evaluarlos debido a los riesgos asociados que conlleva la intervención humana en procesos críticos. Este tipo de control constituyó el más numeroso del número total de los que evalué durante mi experiencia profesional.

También formé parte de la revisión de Reportes Clave (Key Reports) utilizados como fuente de verdad, dada su naturaleza en cuanto a que no puede ser modificados debido a que provienen de un tercero, dejando a la organización al margen en cuanto a las modificaciones que pudiera hacer a la lógica de dichos reportes. Sin embargo, me encontré con casos donde determinadas organizaciones tenían la capacidad de modificar parámetros preestablecidos por el desarrollador (por ejemplo, el periodo de tiempo para el cual se está generando un determinado reporte) dejando por sentado la importancia de validar la integridad, exactitud y consistencia, así como entender los controles asociados a su generación, extracción y uso.

El proceso de evaluación de los controles tecnológicos que seguí tuvo una secuencia estructurada y repetible (con matices) para cualquier organización, acorde al flujo mostrado en la Figura 2.

1. En primer lugar, solicité y recibí la evidencia correspondiente a cada control o reporte evaluado, considerando el periodo definido y el sistema involucrado.
2. Como segundo punto, realicé el análisis técnico de dicha evidencia, evaluando y documentando de manera simultánea su integridad y correspondencia con el objetivo del control.
3. Finalmente, con base en la evidencia analizada y documentada, determiné la conclusión sobre la efectividad operativa de cada control tecnológico revisado.

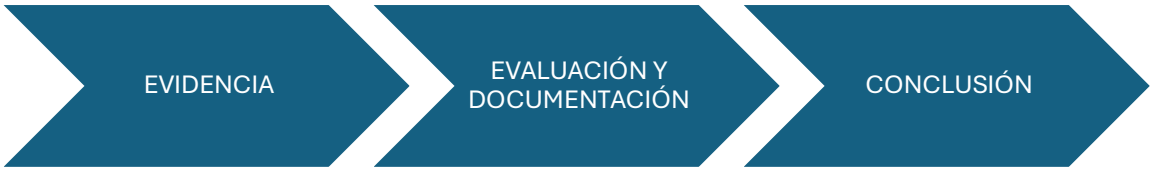

Figura 2: Proceso general de evaluación de controles tecnológicos

Fuente: Elaboración propia con base en metodología interna de evaluación de controles tecnológicos.

4.2 Problemática y Relevancia del Trabajo

Como mencioné anteriormente, lo primero que hice fue recopilar de la evidencia solicitada a los clientes para verificar su autenticidad y posterior documentación de los resultados conforme a los procedimientos establecidos. No formaba parte de mis responsabilidades diseñar, modificar o implementar controles tecnológicos, ya que dichas actividades correspondían a los equipos internos de las organizaciones evaluadas.

Para mantener la trazabilidad de la información, utilicé formatos y plantillas estandarizadas que permitieron registrar mis conclusiones de manera estructurada. Una de las cuestiones más importantes es el que mantuve independencia profesional de la organización evaluada a través del apego a los lineamientos de calidad y confidencialidad respecto a la información revisada.

Uno de los retos con los que me encontré fue que muchos clientes tenían políticas y procedimientos formalmente definidos, pero no contaban con evidencia suficiente que demostrara su aplicación. Esta situación generaba diferencias entre lo que estaba establecido en las políticas y lo que ocurría en la práctica. Identificar esas brechas requería un análisis técnico detallado, comunicación constante con los equipos del cliente y criterio profesional para validar si la evidencia recibida era suficiente y coherente.

Observé que las causas más comunes detrás de estas deficiencias estaban relacionadas con factores humanos, técnicos y metodológicos. Algunos equipos carecían de procedimientos estandarizados o dependían de herramientas limitadas que no registraban correctamente las actividades realizadas. En otros casos, la carga de trabajo o los cambios organizacionales dificultaban mantener la documentación actualizada.

Con el propósito de identificar las causas que originaban las deficiencias usé como herramienta el diagrama causa-efecto de Ishikawa, el cual me permitió agrupar las causas identificadas en factores relacionados con las personas (hombre), los sistemas (máquina), los procedimientos (método), las herramientas y recursos utilizados (material), el entorno de operación (entorno) y finalmente, los mecanismos utilizados para verificar y documentar la ejecución de los controles (medida).

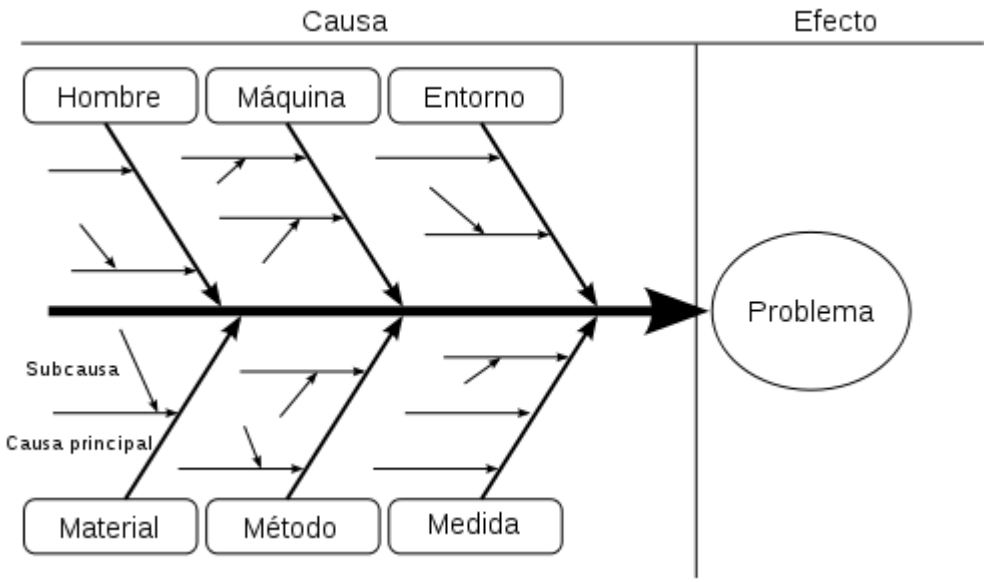

Figura 3. Diagrama causa–efecto de las deficiencias en la trazabilidad de controles tecnológicos. (Basado en la metodología de Ishikawa)

Fuente: Tomado de Production Tools, "¿Cómo implementar el Diagrama de Ishikawa para una gestión Lean?" (2026).

4.3 Planeación y Evaluación del Proyecto

La metodología que apliqué se basó en un enfoque técnico y bien estructurado dentro de proyectos con un alcance definido. Para organizar las actividades utilicé como marco de referencia el ciclo PDCA (Plan–Do–Check–Act), adaptándolo a la dinámica real de ejecución de proyectos.

La fase de planeación a nivel proyecto, con el objetivo de definir el alcance general de las evaluaciones correspondió a la etapa “Plan” del ciclo PDCA. Posteriormente, la solicitud y análisis de la información se desarrollaron durante la etapa “Do”, mientras que la validación de la evidencia y la determinación de la efectividad operativa de los controles correspondieron a la etapa “Check”. Finalmente, la documentación de resultados, la comunicación de observaciones y la definición de acciones requeridas para atender las deficiencias identificadas representaron la etapa “Act”, permitiendo dar seguimiento y al proceso de evaluación.

4.4 Documentación Técnica y Cierre del Análisis

Realicé la documentación en los formatos y plantillas estandarizadas descritos en el apartado 4.2, los cuales fueron utilizados durante todo el proceso de evaluación. Para cada control evaluado documenté los aspectos más importantes del mismo y, además, describí el procedimiento de evaluación aplicado y la evidencia analizada, asegurando en todo momento la correspondencia entre el control, la evidencia y el periodo definido.

Validé la evidencia recibida considerando su integridad, autenticidad y suficiencia para sustentar el análisis técnico. En los casos en que la evidencia resultó incompleta o no permitió llegar a una conclusión clara, solicité al cliente información adicional o aclaraciones para completar la evaluación.

Finalmente, con base en el análisis técnico y la evidencia revisada, documenté la conclusión sobre la efectividad operativa de cada control tecnológico. Es importante aclarar que el análisis se consideró concluido únicamente cuando la documentación reflejaba de forma clara el riesgo evaluado, los atributos revisados, la evidencia analizada y la conclusión correspondiente.

4.5 Resultados

Derivado de mi análisis, fui capaz de identificar el nivel de confiabilidad de los mecanismos implementados por las organizaciones y con base en ello llevar a cabo mi evaluación de los controles revisados, dándome cuenta de que, en la mayoría de los casos, los controles demostraron operar de manera adecuada durante los periodos revisados. En estos escenarios, la evidencia proporcionada fue suficiente y consistente, permitiendo reducir los riesgos tecnológicos. Estos controles se documentaron como efectivos, ya que existía correspondencia entre el diseño del control, su ejecución y la evidencia generada por los sistemas.

Sin embargo, en otros casos, identifiqué controles que, si bien estaban formalmente definidos, presentaban deficiencias en su operación. Estas situaciones se reflejaron en evidencias incompletas, ejecuciones inconsistentes o desviaciones respecto a los procedimientos establecidos. En dichos escenarios, los controles fueron evaluados como ineficientes, ya que no mitigaban de manera adecuada el riesgo que buscaban cubrir. Como parte del proceso de evaluación, fue necesario solicitar al cliente un plan de acción orientado a corregir las deficiencias identificadas y a establecer medidas que permitieran mitigar el riesgo en periodos posteriores.

Finalmente, se presentaron casos en los que los controles tecnológicos no fueron ejecutados durante el periodo evaluado, ya sea por la ausencia de mecanismos operativos o por la falta de aplicación de los procedimientos definidos. En estos escenarios, no fue posible obtener evidencia que demostrara la ejecución del control, por lo que se documentó su incumplimiento.

Este tipo de hallazgos representó un riesgo relevante para la organización, ya que la ausencia del control implicaba una exposición directa a fallos operativos, errores en la información o posibles impactos financieros. Al igual que en los casos de controles ineficientes, fue necesario requerir al cliente la definición de acciones correctivas y medidas de mitigación para atender el riesgo identificado.

Entre las principales recomendaciones derivadas de los hallazgos identificados, fue importante mencionarles la necesidad de formalizar procedimientos, fortalecer la

documentación de la evidencia, implementar mecanismos de seguimiento periódico, mejorar la segregación de funciones y reforzar los procesos de autorización y revisión dentro de los sistemas. Asimismo, en los casos relacionados con cambios a sistemas o administración de accesos, se recomendó establecer evidencias obligatorias de aprobación, bitácoras de seguimiento y revisiones periódicas de usuarios y privilegios.

En conjunto, los resultados obtenidos reflejaron la importancia de evaluar los controles tecnológicos no solo desde su diseño formal, sino desde su ejecución en el diaria dentro de los sistemas. La identificación de controles efectivos, ineficientes o no ejecutados me permitió dimensionar el nivel de riesgo tecnológico existente y evidenció la necesidad de contar con mecanismos de seguimiento y mejora continua para asegurar la confiabilidad de la información y la estabilidad operativa de las organizaciones evaluadas.

Conclusiones

Realizar este trabajo me permitió hacer un análisis de la importancia que tienen los controles tecnológicos que se encargan de soportar la operación de las aplicaciones más críticas dentro de una organización y que no solamente podemos medir su efectividad con base en que estos operen de una manera adecuada, sino que también intervienen otros factores como el contar con una documentación correcta que sustente su funcionamiento dado que estos están en constante evolución.

En consecuencia, consideré recomendable comentar que es de vital importancia que las organizaciones se apeguen de manera estricta a los procedimientos definidos para cada control. Si un procedimiento establecía, por ejemplo, una revisión cada determinado periodo, ésta debía ejecutarse y documentarse conforme a lo definido. De igual forma, consideré importante fortalecer la documentación de la evidencia y mantener trazabilidad sobre las actividades realizadas. La evidencia debía permitir identificar con claridad quién ejecutó el control, cuándo lo realizó, qué información revisó y cuál fue el resultado obtenido. Lo anterior no sólo contribuía a mitigar riesgos de errores o uso indebido de los sistemas, sino que también permitía que la revisión de años fiscales posteriores pudiera comprender y validar adecuadamente la ejecución del control.

En cuanto al análisis y posterior documentación de los aspectos técnicos de los controles quedaron plasmadas las conclusiones para cada uno de ellos dentro de las plantillas y herramientas internas. En estas documenté los aspectos más importantes de cada control, tales como el riesgo asociado, el objetivo del control, la evidencia obtenida para revisarlo y los atributos que se ejecutaron para llegar a una conclusión adecuada.

Por otra parte, la experiencia que obtuve durante este trabajo me permitió aplicar de manera directa diversos conocimientos adquiridos a lo largo de mis estudios como Ingeniero en Telecomunicaciones. Particularmente, las asignaturas relacionadas con redes, sistemas operativos, regulación y análisis económico me proporcionaron las bases necesarias para comprender el funcionamiento de los sistemas evaluados, interpretar la evidencia técnica y analizar el impacto que una deficiencia de control puede generar dentro de una organización.

La Tabla 2 presenta las principales asignaturas que cursé durante la carrera y la manera en que sus contenidos fueron aplicados durante el desarrollo de este trabajo profesional.

Asignatura	Temas aplicados	Aplicación en el trabajo profesional
Interconexión de Redes I	Programación orientada a redes con Python, análisis del tráfico de la red a través de herramientas como Wireshark y protocolos de comunicación	Comprensión del flujo de información entre sistemas, análisis de la comunicación entre aplicaciones y capacidad para interpretar evidencia técnica relacionada con conexiones y comportamiento de la red
Interconexión de Redes II	Administración de servidores en distribuciones Linux como Debian y Ubuntu, servicios de red y funcionamiento de entornos tecnológicos modernos	Comprensión de la infraestructura tecnológica sobre la que operaban los sistemas evaluados, así como capacidad para analizar evidencia proveniente de servidores, como configuraciones vistas desde la terminal dentro de plataformas basadas en Linux

Regulación de las Telecomunicaciones	Marcos normativos y la importancia de su cumplimiento, así como la relación estrecha que existe entre tecnología y regulación	Comprensión de la relevancia de las implicaciones normativas derivadas de una deficiencia en los sistemas de información visto desde el punto de vista de Telecomunicaciones
Introducción a la Economía	Impactos económicos de los riesgos, así como la relación entre información y toma de decisiones dentro de una compañía	Comprensión de las consecuencias económicas derivadas de poseer información incorrecta
Introducción al Análisis Económico Empresarial	Estados financieros, operación de las organizaciones y relación entre procesos y resultados financieros	Comprensión de cómo la información generada por los sistemas evaluados impacta procesos financieros, reportes y estados financieros utilizados por las organizaciones

Tabla 2: Relación entre las asignaturas cursadas durante la licenciatura y su aplicación en el desarrollo del trabajo profesional.

Fuente: Elaboración propia con base en Universidad Nacional Autónoma de México (2016), Plan de Estudios de la Licenciatura en Ingeniería en Telecomunicaciones, Facultad de Ingeniería.

A partir de la experiencia adquirida, considero conveniente reforzar dentro del plan de estudios temas relacionados con auditoría de tecnologías de la información, gestión de riesgos, marcos internacionales de control y normativas aplicables a organizaciones globales. En particular, resultaría útil incorporar contenidos relacionados con marcos como ISO/IEC 27001, ISO/IEC 27002, NIST y la Ley Sarbanes–Oxley, debido a que una parte importante de los profesionistas en telecomunicaciones termina trabajando para organizaciones internacionales sujetas a este tipo de normativas, por lo cual les permitiría vincular de forma directa la formación técnica con las necesidades actuales del ámbito profesional.

Este tipo de revisiones son fundamentales porque los sistemas tecnológicos terminan respaldando información financiera, operativa y regulatoria cuya integridad es indispensable para la toma de decisiones, además de permitir identificar oportunamente deficiencias en los controles, reducir riesgos de errores o en el peor de los casos fraude corporativo

Para finalizar, me parece importante mencionar que en este trabajo se refleja la formación integral que recibí por parte de la Facultad de Ingeniería la cual me brindó la posibilidad de aprender dos pilares fundamentales para mi carrera profesional, como lo son el apartado técnico y el apartado económico, los cuales me permitieron desarrollar un criterio profesional sólido que a su vez me permitió lograr una buena adaptación a un entorno en constante evolución.

Bibliografía

1. Asociación Española de Normalización (UNE). (2017). UNE-ISO/IEC 27001:2017 Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información — Recuperado de: https://www.une.org/encuentra-tu-norma/busca-tu-norma/norma?c=N0058428
2. Calder, A., & Watkins, S. (2022). IT Governance: An International Guide to Data Security and ISO27001/ISO27002. Recuperado de: http://repo.darmajaya.ac.id/4031/1/IT%20Governance%20An%20International%20Guide%20to%20Data%20Security%20and%20ISO27001ISO27002%20by%20Alan%20Calder%2C%20Steve%20Watkins%20%28z-lib.org%29.pdf
3. Rodríguez Garraza, Tomás (2017) PDCA. Recuperado de: https://gobiernoygestionpublica.edu.pe/iggp/wp-content/uploads/2020/03/6.-PDCA.pdf
4. International Organization for Standardization. (2022). ISO/IEC 27002:2022 – Information Security, Cybersecurity and Privacy Protection — Information Security Controls. ISO. Recuperado de: https://www.iso.org/standard/75652.html
5. National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). Recuperado de: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

6. Organización Internacional de Normalización (ISO). (2015). ISO 22301:2015 – Security and Resilience – Business Continuity Management Systems – Requirements. ISO. Recuperado de: https://www.iso.org/es/contents/data/standard/07/51/75106.html
7. Universidad Nacional Autónoma de México. (2016). Plan de Estudios de la Licenciatura en Ingeniería en Telecomunicaciones, Facultad de Ingeniería. UNAM. Recuperado de: https://www.ingenieria.unam.mx/programas_academicos/licenciatura/telecomunicaciones_plan2016.php
8. Organización Internacional de Normalización (ISO). (2008). Gestión de la calidad – Principios esenciales y vocabulario (ISO 9000:2008). ISO. Recuperado de: https://www.iso.org/obp/ui/#iso:std:iso:9001:ed-4:v2:es
9. International Organization for Standardization. (2018). ISO 31000:2018 – Risk Management — Guidelines. ISO. Recuperado de: https://www.iso.org/standard/65694.html
10. U.S. Department of the Treasury. (2025). Financial Services Sector Risk Management Plan. Recuperado de: https://home.treasury.gov/system/files/216/Financial-Services-Sector-Risk-Management-Plan.pdf
11. Landoll, D. J. (2017). Information security policies, procedures, and standards: A practitioner's reference. Recuperado de: https://api.pageplace.de/preview/DT0400.9781482245912_A27136062/preview-9781482245912_A27136062.pdf

12. IBM. (2025). ¿Qué es el cumplimiento de la ley SOX (Ley Sarbanes- Oxley? Recuperado de: https://www.ibm.com/mx-es/think/topics/sox-compliance

13. THE SARBANES-OXLEY ACT. (2025). Is Sarbanes-Oxley Compliance Still Necessary 23 Years After Its Enactment? Recuperado de: https://www.sarbanes-oxley-act.com/

14. Microsoft. (2024). Sarbanes-Oxley Act of 2002 (SOX) (Ley Sarbanes-Oxley de 2002, SOX). Recuperado de: https://learn.microsoft.com/es-es/compliance/regulatory/offering-sox

15. PCAOB. (2010). PUBLIC LAW 107–204—JULY 30, 2002. Recuperado de: https://pcaobus.org/About/History/Documents/PDFs/Sarbanes_Oxley_Act_of_2002.pdf

16. Production Tools. (2026). ¿Cómo implementar el Diagrama de Ishikawa para una gestión Lean?. Recuperado de: https://productiontools.es/lean/diagrama-de-ishikawa/

17. Colegio oficial ingenieros en telecomunicación. (2021). Guía de Iniciación a Actividad Profesional Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001. Recuperado de: https://www.coit.es/sites/default/files/informes/pdf/implantacion_de_sistemas_de_gestion_de_la_seguridad_de_la_informacion_sgsi_segun_la_norma_iso_27001.pdf