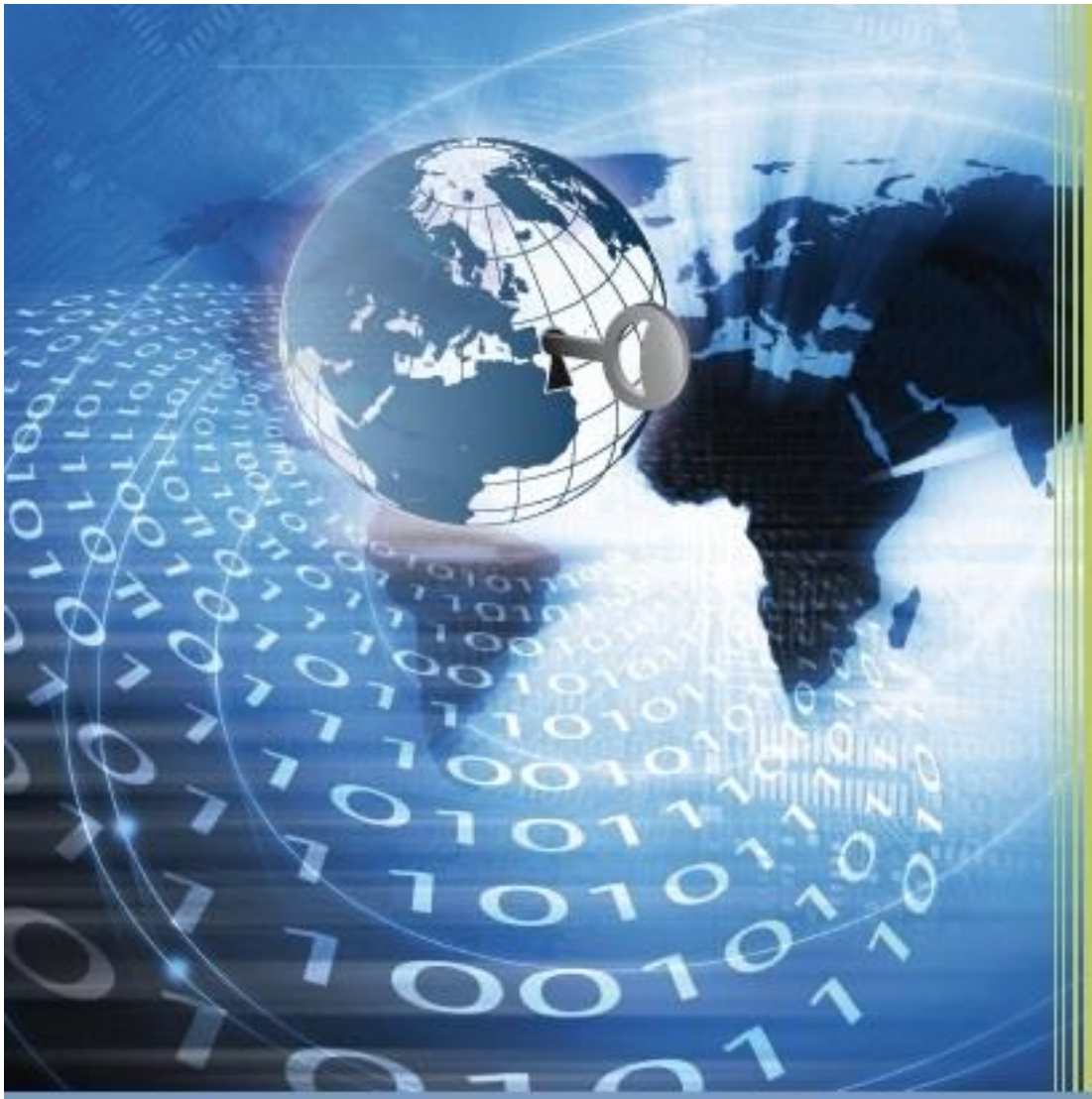


MANUAL DE LA IDI Y DEL WGITA SOBRE AUDITORÍA DE TI PARA LAS ENTIDADES FISCALIZADORAS SUPERIORES

Este Manual ha sido aprobado
por la INCOSAI XXI, llevada a cabo en
Pekín, China, en octubre de 2013.

Publicado en febrero de 2014.

Diseñado y publicado por www.printhouse.no

Traducción:
Contribución de la CTIC de la OLACEFS. Miembros de la CTIC 2017: Auditoría General de la Nación, Argentina (Presidencia), Contraloría General del Estado Plurinacional de Bolivia, Contraloría General de la República de Chile, Contraloría General de la República de Colombia, Contraloría General de la República de Cuba, Contraloría General del Estado de la República del Ecuador, Corte de Cuentas de la República de El Salvador, Auditoría Superior de la Federación de México, Contraloría General de la República de Perú, Tribunal de Cuentas de la República Oriental del Uruguay, y el Honorable Tribunal de Cuentas de la Provincia de Buenos Aires.

PREFACIO

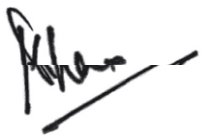
La Auditoría de Tecnologías de la Información (TI) se ha convertido en uno de los temas centrales de las auditorías realizadas por las Entidades Fiscalizadoras Superiores (EFS) en todo el mundo. Esta es una respuesta natural a las operaciones cada vez más informatizadas de los gobiernos y las organizaciones del sector público. Los sistemas utilizados deben garantizar la protección de los datos y los activos de la organización, así como contribuir con la misión, el área financiera y otras metas específicas. Si bien el uso creciente de las TI ha llevado a mejorar la eficiencia empresarial y la eficacia de la prestación de servicios, también ha traído consigo riesgos y vulnerabilidades asociadas a las bases de datos y a las aplicaciones para la gestión de las operaciones, las cuales normalmente definen un entorno laboral automatizado. El rol de la auditoría de TI para garantizar la existencia de procesos adecuados a fin de gestionar los principales riesgos y vulnerabilidades de TI es fundamental, si la intención es que las EFS informen de manera significativa la eficacia y la eficiencia de las operaciones del sector público y del gobierno. En el entorno de la auditoría de TI, los procesos, herramientas y la supervisión y otras formas de gestionar una función también se conocen como controles.

El Grupo de Trabajo de la INTOSAI sobre Auditoría de TI (WGITA) y la Iniciativa para el Desarrollo de la INTOSAI (IDI) han colaborado en la elaboración de un Manual de Auditoría de TI que proporciona a los auditores de las EFS buenas prácticas universalmente reconocidas y normas en materia de auditoría de TI. Este Manual ofrece una explicación detallada de las áreas más importantes que se puede requerir sean investigadas por los auditores de TI, mientras realizan las auditorías.

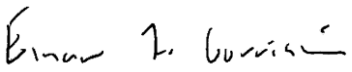
El Manual WGITA/IDI cumple con los principios generales de auditoría tal como se establece en las Normas Profesionales para las Entidades Fiscalizadoras Superiores (ISSAI)*. El Manual también se basa en los marcos de TI reconocidos internacionalmente, como el marco de referencia de buenas prácticas de TI COBIT de ISACA, las normas de la Organización Internacional de Normalización (ISO), y las guías y los manuales de TI de algunas de las EFS, con el objetivo de proporcionar a los auditores de TI un conjunto completo de sugerencias sobre auditorías de TI.

El objetivo principal de este Manual es proporcionar a los auditores de TI información esencial y preguntas clave necesarias para una planificación eficaz de las Auditorías de TI. Se espera que el manual sea de utilidad para las EFS a manera de amplia referencia y guía práctica para la realización de las auditorías de TI.

Este proyecto fue dirigido conjuntamente por el presidente del WGITA, específicamente la EFS de la India, y la IDI. Las EFS miembros del WGITA, Brasil, Estados Unidos de América, India, Indonesia y Polonia trabajaron conjuntamente en el desarrollo de esta directriz. En particular, el WGITA y la IDI desean agradecer a cada uno de los miembros del equipo que han trabajado incansablemente en el desarrollo de esta directriz. Asimismo, agradecemos a las EFS que aportaron sus valiosos comentarios sobre el Manual.



Shashi Kant Sharma
Contralor y Auditor General de India
Presidente del Grupo de Trabajo sobre
Auditorías de TI de la INTOSAI (WGITA)



Einar J. Gørrissen
Director General
Iniciativa para el Desarrollo de la INTOSAI (IDI)

* www.issai.org

MIEMBROS DEL EQUIPO DEL PROYECTO MANUAL IDI-WGITA

1. Sr. Madhav S Panwar
Tecnólogo Nivel Superior (Director, Oficina de Rendición de Cuentas del Gobierno de los Estados Unidos de América)

2. Sr. Pawel Banas
Asesor del Presidente de la Entidad Fiscalizadora Superior de Polonia (NIK)
Entidad Fiscalizadora Superior de Polonia

3. Sr. Neelesh Kumar Sah
Contador General
Oficina del Contralor y Auditor General de la India

4. Sr. Anindya Dasgupta
Director
Oficina del Contralor y Auditor General de la India

5. Sr. Marcio Rodrigo Braz
Auditor
Tribunal de Cuentas de Brasil (Tribunal de Contas União)

6. Srta. Shefali S Andaleeb
Subdirector General
Iniciativa para el Desarrollo de la INTOSAI (IDI)

7. Novis Pramantya Budi
Subdirector
Comisión de Auditoría de la República de Indonesia

8. Srta. Ria Anugriani
Subdirectora
Comisión de Auditoría de la República de Indonesia

LISTA DE ABREVIATURAS

BCP	Plan de Continuidad del Negocio
BIA	Análisis del Impacto del Negocio
CAAT	Técnicas de Auditoría Asistidas por Computadora
COBIT	Objetivos de Control para Información y Tecnología Conexa
DRP	Plan de Recuperación ante Desastres
EUROSAI	Organización Europea de Entidades Fiscalizadoras Superiores
GAO	Oficina Gubernamental de Rendición de Cuentas, Estados Unidos de América (EE.UU.)
ISACA	Asociación de Auditoría y Control de Sistemas de Información
ISSAI	Normas Profesionales para las Entidades Fiscalizadoras Superiores, eventualmente; también denominadas Normas de la INTOSAI, en especial en Documentos Antiguos
ISP	Política de Seguridad de la Información
TI	Tecnologías de la Información
ITIL	Biblioteca de Infraestructura de Tecnologías de la Información
NIST	Instituto Nacional de Normas y Tecnología, Departamento de Comercio de los Estados Unidos
RPO	Objetivo de Punto de Recuperación
RTO	Objetivo de Tiempo de Recuperación
SLA	Acuerdo de Nivel de Servicio
Wi-Fi	Wireless Fidelity (Fidelidad Inalámbrica)

TABLA DE CONTENIDOS

INTRODUCCIÓN

El advenimiento de las tecnologías de la información ha cambiado muchos aspectos de la forma en que trabajamos, y el trabajo de auditoría claramente no es una excepción. La presencia casi generalizada de la informática, sin duda una de las herramientas operativas más eficaces, también ha traído consigo vulnerabilidades relacionadas con el entorno automatizado de la organización. Cada nueva vulnerabilidad necesita ser identificada, mitigada y controlada. Evaluar la idoneidad de cada control requiere nuevos métodos de auditoría[1].

Los sistemas informáticos han pasado de ser meros sistemas para el procesamiento de datos a sistemas que recogen, almacenan y proporcionan acceso a grandes cantidades de datos. Estos datos son utilizados en la toma de decisiones y el desempeño de las principales actividades operativas de la organización. En la actualidad, los sistemas informáticos se comunican entre sí e intercambian datos a través de redes públicas y privadas.

De hecho, con la llegada y el desarrollo de los sistemas de redes informáticas, los sistemas informáticos son ahora efectivamente sistemas de información. Esta evolución se refleja en que el término "auditoría EDP", en gran medida, ha sido sustituido por términos como "Auditoría de Tecnologías de la Información" y "Auditoría de los Sistemas de Información".

Con el incremento en la inversión y la dependencia de los sistemas informáticos por parte de las entidades auditadas, se ha hecho imprescindible para el auditor de TI adoptar una metodología apropiada y un enfoque tal que la auditoría pueda definitivamente identificar los riesgos para la integridad, el abuso y la privacidad de los datos; y además garantizar la existencia de controles para la mitigación. En un típico sistema de TI, especialmente cuando se lo implementa en un entorno de controles ineficientes, la entidad auditada se enfrenta a muchos riesgos que el auditor de TI debe ser capaz de identificar. Aún cuando la entidad auditada haya implementado algunas medidas de reducción de riesgos, se requiere una auditoría independiente para garantizar que se han diseñado y puesto en operación los controles adecuados (controles informáticos generales[2] y/o controles de aplicación[3]) a fin de minimizar la exposición a diversos riesgos.

CONTENIDO Y ESTRUCTURA DEL MANUAL

Este Manual está destinado a proporcionar a los auditores de TI una guía descriptiva de las diferentes áreas de la Auditoría de TI, así como una orientación detallada sobre cómo planificar estas auditorías de manera efectiva.

---

[1] *Manual de Auditoría de TI*, Volumen I, Contralor y Auditor General de la India.
[2] Los Controles Generales de SI no son específicos de un flujo de transacciones individuales o aplicación, y son controles sobre los procesos en una implementación de TI que respaldan el desarrollo, la implementación y la operación de un Sistema de TI. Normalmente, éstos podrían involucrar la Gobernanza, Organización y Estructura, Controles Físicos y Ambientales de TI, operación de TI, Seguridad de SI, Continuidad del Negocio.
[3] Los Controles de aplicación son controles específicos de un Sistema de TI e involucran el mapeo de las reglas operativas en la aplicación proporcionando, de este modo, controles de entrada, procesamiento, salida y sobre los Datos Maestros.

En el capítulo 1 de esta guía, los usuarios encontrarán una descripción general de la definición de auditoría de TI, el mandato de la EFS, y el alcance y los objetivos de dichas auditorías. También proporciona una explicación de los controles generales y controles de aplicaciones de TI y la relación entre ambos. El alcance de estos controles se explica con más detalle en los capítulos siguientes. El Capítulo 1 también describe el proceso de auditoría de TI y la metodología de la evaluación basada en el riesgo para seleccionarlas. En el Anexo I se proporciona una "Lista de Verificación de Evaluación del Riesgo" genérica. La descripción del proceso de auditoría de TI es de carácter genérico. Este proceso se basa en los métodos de auditoría estándar que se utilizan en una auditoría típica de TI. Los usuarios del Manual deben remitirse a los manuales y a las directrices de procedimientos de auditoría de sus respectivas EFS para planificar y realizar auditorías específicas.

Los capítulos 2-8 proporcionan una descripción detallada de las diferentes áreas de TI que ayudarán a los auditores de TI a identificar potenciales áreas auditables. Los riesgos a nivel organizacional relacionados con el área de TI se han enumerado al final de cada capítulo, lo que ayudará a los auditores de TI a identificar las áreas auditables de alto riesgo. La directriz proporcionada en cada área ayudará a los auditores de TI en la planificación de sus auditorías, ya sea en un área específica o una combinación de áreas dependiendo del alcance y objetivo de la auditoría de TI que está siendo planificada (auditoría financiera o de desempeño). Por ejemplo, la directriz para la auditoría de gobernanza de TI puede ser utilizada para planificar una auditoría del mecanismo de gobernanza de TI de la entidad o para planificar la auditoría del entorno de controles generales, de la cual la gobernanza de TI es una parte importante.

Cada capítulo está respaldado por una directriz detallada para el desarrollo de una matriz de auditoría que se indica en los Anexos II-VIII. La matriz de auditoría enumera las cuestiones clave de auditoría, los criterios, la información requerida y los métodos de análisis. Los auditores deben tener en cuenta que las cuestiones de auditoría enumeradas en las matrices son indicativas y no exhaustivas y su objetivo es alentar el desarrollo de las mismas de acuerdo con los requerimientos de sus auditorías. El modelo de matriz de auditoría es de carácter genérico y podría ser utilizado como papeles de trabajo por las EFS, o ser modificado de acuerdo con las normas de la EFS.

Además, este Manual incluye una visión general de las áreas emergentes en Auditoría de TI. El capítulo 9 destaca algunas de las áreas que podrían ser de interés para los auditores de TI, tales como los sitios web y los portales, la gobernanza informatizada, la auditoría Informática Forense y la Informática Móvil. Este capítulo contiene una lista indicativa de las áreas de auditoría y proporciona referencias de lecturas adicionales para el usuario interesado.

La directriz técnica sobre el uso de Técnicas de Auditoría Asistidas por Computadoras (CAAT) excede el alcance de este Manual. Se incentiva a las EFS a organizar una capacitación independiente en CAAT para su personal. Las EFS también pueden considerar proponer a su personal para el programa de desarrollo de capacidades de la IDI en la auditoría de TI.

Agradecemos que visiten el sitio web del WGITA y de la IDI para obtener más información sobre los recursos y los próximos programas de capacitación.

WGITA: http://www.intosaiitaudit.org IDI: http://www.idi.no

Esperamos que este Manual sea una herramienta de utilidad para las EFS y su personal de auditoría de TI en cuanto al mejoramiento de sus conocimientos y comprensión de las cuestiones relacionadas con la auditoría de TI, y que los asista en la planificación y realización de auditorías de TI.

CAPITULO 1

AUDITORÍA DE TECNOLOGÍAS DE LA INFORMACIÓN (TI)

Introducción

A la luz de las oportunidades de informatización disponibles en todo el mundo, las organizaciones dependen cada vez más de la automatización de sus actividades y de la gestión de la información. Esto configura el contexto para que los auditores adquieran confianza en dichos mecanismos y utilicen la información disponible en los mismos para sacar conclusiones apropiadas de la auditoría.

Este capítulo proporciona una visión general de los procesos de auditoría de TI. Sirve tanto de introducción como de resumen de los capítulos 2-8. Por lo tanto, este capítulo difiere de todos los demás en términos de diseño y detalle. El proceso de auditoría de TI descrito en este capítulo no se documenta en una norma internacional, pero es un reflejo de la metodología de auditoría integrada en las ISSAI y otras Normas Internacionales, así como de las prácticas de auditoría generalmente aceptadas y aplicadas por las EFS.

I.QUÉ ES LA AUDITORIA DE TI

La auditoría de TI es el proceso para garantizar que el desarrollo, la implementación y el mantenimiento de los sistemas de TI cumplen con los objetivos del negocio, protegen el valor de la información y mantienen la integridad de los datos. En otras palabras, la Auditoría de TI es un examen de la implementación de los sistemas y controles de TI para asegurar que los mismos cumplen con las necesidades operativas de la organización, sin comprometer la seguridad, la privacidad, el costo y otros elementos críticos del negocio.

I.1 Mandato de las Auditorías de TI

El mandato de una EFS en cuanto a la realización de una auditoría de los sistemas de TI se describe en la ISSAI 1 - Declaración de Lima.[4] En consecuencia, el mandato de una EFS para la auditoría de TI deriva del mandato general otorgado a la EFS a fin de llevar a cabo auditorías financieras, de cumplimiento, de desempeño o la combinación de las mismas.[5] Algunas EFS pueden tener un mandato específico para la realización de auditorías de TI. Por ejemplo, si la EFS tiene el mandato de auditar la función de recaudación fiscal, ésta debe auditar la porción automatizada de la función de recaudación fiscal a través de una derivación de su mandato original.

[4] *Declaración de Lima* de la INTOSAI, Parte VII Sección 22.
[5] ISSAI *100 Principios Fundamentales de la Auditoría del Sector Público.*

I.2 Objetivos de la Auditoría De TI

El objetivo de las Auditorías de TI es garantizar que los recursos de TI permitan alcanzar las metas organizacionales con eficacia y utilizar los recursos de manera eficiente. Las auditorías de TI pueden cubrir los sistemas ERP (enterprise resource planning), la Seguridad Informática (SI), la adquisición de la solución para el negocio, el Desarrollo de Sistemas, y la Continuidad del Negocio, que son áreas específicas de la implementación de SI; o pueden analizar la propuesta de valor que los sistemas de SI puedan haber efectuado.

Algunos ejemplos de los objetivos de la auditoría son:

- Revisión de los controles de los sistemas de TI para garantizar su adecuación y eficacia;
- Evaluación de los procesos involucrados en el funcionamiento de un área determinada, como el sistema de liquidación de sueldos o sistema de contabilidad financiera;
- Evaluación del desempeño de un sistema y su seguridad, por ejemplo, un sistema de reservas ferroviario;
- Análisis del proceso de desarrollo del sistema y los procedimientos.

I.3 Alcance de la Auditoría de TI

Generalmente, las Entidades Fiscalizadoras Superiores (EFS) realizan auditorías de TI conjuntamente con una auditoría de los estados financieros, una revisión de los controles internos y/o como auditorías de desempeño de los sistemas de TI o aplicaciones de TI. En términos generales, las auditorías de TI se extienden a las auditorías financieras (para evaluar la exactitud de los estados financieros de una organización); auditorías de cumplimiento/operativas (evaluación de los controles internos), auditoría de desempeño (incluyendo temas de sistemas de información), auditorías especializadas (evaluación de los servicios prestados por un tercero, como la subcontratación, etc.), auditorías forenses y auditorías de los proyectos de desarrollo de los Sistemas de Información (SI)[6].

Independientemente del tipo de auditoría, se requiere que el auditor de TI evalúe las políticas y los procedimientos que guían el entorno global de TI de la entidad auditada, garantizando la existencia de los correspondientes controles y mecanismos de aplicación. El alcance de una auditoría de TI implica decidir la profundidad de los procedimientos de auditoría, la cobertura de los sistemas de TI y sus funcionalidades, los procesos de TI a ser auditados, la ubicación de los sistemas de TI[7] y el periodo de tiempo a ser cubiertos. Se tratará, básicamente, de establecer o definir los límites de la auditoría.

[6] Ver en la Base de Datos de la EUROSAI Informes de Auditoría de TI, los diferentes tipos de Auditorías de TI- http://egov.nik.gov.pl/.

[7] La ubicación incluye los servidores "*back-end*" (de aplicación o datos, etc.), ubicación de usuarios, redes de manera genérica y podría también determinar las ubicaciones físicas a ser cubiertas en una red distribuida en edificios, ciudades o países, si es aplicable.

Figura 1.1 Controles Generales y de Aplicación

I.4 Controles de TI

Un control es la combinación de métodos, políticas y procedimientos que garantizan la protección de los activos de la organización, la precisión y la confiabilidad de sus registros, y el cumplimiento operativo con las normas de gestión.

En un contexto de TI, los controles están divididos en dos categorías: los controles generales y los controles de aplicación. Las categorías dependen del período de influencia de un control y si está vinculado a una aplicación en particular.

Los controles generales de TI son la base de la estructura de Control de TI. Estos están relacionados con el entorno general en el que los sistemas son desarrollados, operados, gestionados y mantenidos. Los controles generales de TI establecen un marco de control general para las actividades de TI y garantizan el cumplimiento de los objetivos generales de control.

Los controles generales son implementados mediante la utilización de una serie de herramientas tales como la política, las directrices y los procedimientos, así como el establecimiento de una estructura de gestión adecuada, incluyendo la estructura para la gestión de los sistemas de TI de la organización.

Ejemplos de controles generales incluyen el desarrollo y la implementación de una Estrategia de SI y una política de Seguridad de SI, el establecimiento de un comité directivo de TI, la organización del personal de SI para dividir las responsabilidades en conflicto y la planificación de la prevención y recuperación ante desastres.

Los Controles de Aplicación son controles específicos y únicos para cada aplicación informatizada. Se aplican a los segmentos de la aplicación y se refieren a los registros y datos existentes. Los controles de aplicación incluyen la validación del ingreso de datos, encriptado de datos a transmitir, controles de procesamiento, etc. Por ejemplo, en una aplicación de pago en línea, un control de entrada podría ser que la fecha de vencimiento de la tarjeta de crédito sea posterior a la fecha de transacción y los detalles ingresados sean encriptados.

I.5 Controles Generales de TI, Controles de Aplicación y su Relación

Los controles generales de TI no son específicos para flujos de registros individuales, paquetes contables determinados o aplicaciones financieras. El objetivo de los controles generales de TI es garantizar el adecuado desarrollo e implementación de las aplicaciones, así como de los programas y archivos de datos y de operaciones informatizadas.[8]

El diseño e implementación de controles generales de TI pueden tener un impacto significativo en la eficacia de los controles de aplicación. Los controles generales proporcionan a las aplicaciones los recursos que necesitan para operar y garantizar que no se puedan realizar cambios no autorizados en ninguna de las aplicaciones (es decir, están protegidos contra la reprogramación) ni en las bases de datos subyacentes (un importante repositorio de registros).

[8] ISACA, Directrices de Auditoría de SI – Revisión de los Sistemas de Aplicación-Documento GI4, p.3.

Los controles generales de TI más comunes que mejoran los controles de aplicación son:[9]

- Control de acceso lógico a la infraestructura, las aplicaciones y los datos,
- Controles del ciclo de vida del desarrollo del sistema,
- Controles de gestión de cambio de programa,
- Controles de acceso físico al centro de procesamiento de datos,
- Controles del sistema y de copia de seguridad de los datos y recuperación,
- Controles de las operaciones informatizadas.

Los controles de las aplicaciones operan sobre registros individuales y garantizan que éstos sean ingresados, procesados y emitidos de manera correcta. La efectividad del diseño y de la operatividad de los controles generales de TI influye considerablemente en la medida en la que la administración puede confiar en los controles de aplicación para gestionar los riesgos.

I.6 ¿Por Qué los Controles de TI son Importantes para el Auditor de TI?

Generalmente, el auditor de TI es convocado para evaluar los controles relacionados con la tecnología, mientras que los auditores que no auditan las TI evalúan los controles financieros, regulatorios y de cumplimiento. A medida que cada vez más organizaciones dependen de TI para automatizar sus operaciones, la línea que divide la función de los auditores de TI y los auditores que no auditan las TI se reduce rápidamente. Como mínimo, se requiere que todos los auditores comprendan el entorno de control de la entidad auditada con el fin de brindar seguridad respecto de los controles internos que operan en la entidad. De conformidad con los Principios Fundamentales de Auditoría del Sector Público de ISSAI: "Los auditores deben comprender la naturaleza de la entidad/programa a ser auditado". [10] Esto incluye la comprensión de los controles internos, los objetivos, las operaciones, el entorno regulatorio y los sistemas y procesos del negocio involucrados. Cada área de control se basa en un conjunto de objetivos de control que una organización implementa a fin de mitigar riesgos. La función del auditor es entender los riesgos potenciales del negocio y de TI que enfrenta la entidad auditada y, a su vez, evaluar si los controles implementados son los adecuados para cumplir con los objetivos de control. En el caso de los controles generales de TI, es importante que el auditor comprenda las grandes categorías y el alcance de los controles generales en funcionamiento, evalúe la supervisión de la gestión y la concientización del personal de la organización respecto de los controles, y descubra cuán efectivos son estos para ofrecer seguridad. La ISSAI 1315 señala que, incluso en pequeñas entidades, en donde los sistemas de información y los procesos de negocio aplicables a la información financiera son menos sofisticados, su papel es importante. Si los controles generales son débiles, disminuye seriamente la confiabilidad de los controles asociados con las aplicaciones individuales de TI.

En los capítulos siguientes, se analizan en detalle algunas de las áreas clave de los Controles Generales y los Controles de Aplicación de TI. En los Anexos, se proporcionan las matrices de auditoría sugeridas para cada una de las áreas de control.

[9] Guía General de Auditoría de Tecnología (GTAG) 8- Auditoría de Controles de Aplicaciones.
[10] ISSAI 100, párrafo 49.

II. PROCESO DE AUDITORÍA DE TI

PLANIFICACIÓN DE LAS AUDITORÍAS DE TI

La planificación es una parte clave de cualquier auditoría, incluida la de TI. En la mayoría de las EFS, la planificación de las auditorías se lleva a cabo en tres niveles - planificación Estratégica, planificación Macro o Anual y planificación Micro o a Nivel de la Entidad.

II. 1. Planificación Estratégica

Un plan estratégico de la EFS es una planificación a largo plazo (3-5 años) de las metas y los objetivos de la auditoría, incluidos aquellos objetivos para los sistemas de TI y para las respectivas organizaciones bajo la competencia de una EFS.

En algunas EFS, sólo una lista de áreas nuevas y emergentes para auditar en relación a las TI puede ser incluida en su plan estratégico. Éstas podrían incluir la consideración de nuevos métodos de desarrollo de sistemas (por ejemplo, programación ágil) y la adquisición o quizás la informática en la nube (*cloud computing)* en el sector público.

En cualquier caso, el proceso de planificación estratégica o el plan estratégico de la EFS marcan la pauta y la dirección de las metas de Auditoría de TI de una EFS para el futuro.

II.2 Planificación Macro

La planificación de la auditoría a nivel macro se realiza generalmente sobre una base del ciclo anual a nivel de las EFS[11] para la selección de las áreas de auditoría. Con la rápida proliferación de los sistemas modernos de SI en los gobiernos y la limitación de los recursos disponibles para las EFS, sería apropiado utilizar **un enfoque basado en riesgos** para priorizar y seleccionar los temas adecuados. Por otra parte, las EFS, además, deberá incorporar las auditorías obligatorias, como las exigidas por la ley o aquellas solicitadas por el Parlamento, Congreso u otros organismos de control.

Medidas a tomar para el enfoque basado en el riesgo

1. **Identificar el universo de auditoría que forma parte de la lista de todas las organizaciones auditables o unidades que recaen en la jurisdicción de una EFS.**
2. **Enumerar los sistemas de información en uso en la organización/unidades auditables.**
3. **Identificar los factores que afectan la criticidad del sistema de la organización para llevar a cabo sus funciones y prestar un servicio.**
4. **Otorgar importancia a los factores críticos, que se podrían realizar en colaboración con la organización auditada.**
5. **Recopilar información para todos los sistemas, en todas las organizaciones y en base a los resultados acumulados, ordenar los sistemas/organizaciones según la prioridad para ser auditados.**
6. **Preparar un plan anual de auditoría que establezca la prioridad, el enfoque y el cronograma de las auditorías de TI. Esta práctica podría realizarse a intervalos anuales y, por lo tanto, podría ser un plan periódico.**

[11] La organización de EFS alrededor del mundo tendrá diferentes estructuras. La etapa aquí se refiere a una formación en el campo de la Sede de una EFS en el que la planificación a nivel global se lleva a cabo o se aprueba en las sedes y la auditoría actual (etapa dos para planificación) se lleva a cabo en el nivel del ámbito.

i. Enfoque Basado en Riesgos

Por lo general, las EFS tienen bajo su mandato de auditoría una serie de organizaciones que utilizan diferentes sistemas de información. Puede haber diferentes aplicaciones para diferentes funciones y actividades, y puede haber un número de instalaciones informáticas en diferentes ubicaciones geográficas.

Si bien hay riesgos inherentes a los sistemas de información, estos riesgos impactan en diferentes sistemas de diferentes maneras. El riesgo de no disponibilidad, incluso durante una hora, puede ser grave para un sistema de facturación en una tienda de venta minorista muy concurrida. El riesgo de una modificación no autorizada puede ser una fuente de fraudes y potenciales pérdidas para un sistema de banca en línea. Un sistema de procesamiento por lotes o un sistema de consolidación de datos puede ser relativamente menos vulnerable a algunos de estos riesgos. Los entornos técnicos en los que los sistemas se ejecutan también pueden influir en el riesgo asociado a los sistemas.[12]

Un enfoque basado en el riesgo ayuda al auditor a seleccionar y priorizar las auditorías de TI. Para utilizar el marco de la evaluación de riesgos, una EFS necesita tener cierta información mínima en todas las agencias, por lo general obtenida a través de una encuesta.

Mientras que un proceso de evaluación de riesgos es una manera de seleccionar la entidad auditada para la auditoría de TI, las EFS también seleccionan las entidades auditables de manera cíclica, mediante auditorías por mandato o en virtud de solicitudes específicas de los órganos de control (Congreso, Parlamento, Poder Legislativo, etc.)

II.3 Planificación Micro (o a Nivel de la Entidad)

La planificación micro implica el desarrollo de un plan de auditoría detallado para entidad seleccionada, comenzando por el trazado de los objetivos de auditoría. El plan de auditoría ayudará a los auditores en la preparación de un programa de auditoría. El requisito previo para desarrollar el programa de auditoría será contar con una clara comprensión de la entidad auditada y de sus Sistemas de Información. El Manual tiene como objetivo asistir al auditor, una vez que el plan haya sido creado, para completar la matriz de auditoría con los objetivos específicos de cada área (gobernanza, seguridad de la información, etc.) a ser examinada. La planificación a nivel micro requiere una comprensión de la organización y algunas evaluaciones preliminares de los controles para facilitar una detallada planificación de auditoría.

i. Conocimiento de la Organización

El grado de conocimiento de la organización y sus procesos requeridos por el auditor de TI serán determinados en gran medida por la naturaleza de la organización y el nivel de detalle con el que se realiza el trabajo de auditoría. El conocimiento de la organización debe incluir los riesgos de negocio, financieros y riesgos inherentes que enfrenta la organización y sus sistemas de TI. Asimismo, debe incluir el grado en el que la organización depende de la subcontratación para cumplir con sus objetivos y en qué medida el proceso completo del negocio ha sido planificado en un entorno de TI.[13] El auditor debe utilizar esta información para identificar los posibles problemas, establecer los objetivos y el alcance del

[12] S Anantha Sayana-ISACA.

[13] Las organizaciones que cambian de un entorno manual a un entorno informatizado podrían normalmente realizar un ejercicio de Reingeniería del Proceso del Negocio (BPR). Es posible que algunos de los procesos de negocios se llevan a cabo manualmente conjuntamente con los Sistemas de TI. Estas situaciones especiales podrían constituir áreas específicas de interés para los Auditores de TI.

trabajo, ejecutarlo, y tener en cuenta las medidas de gestión a las que el auditor de TI debe prestar atención.

A continuación, se presenta un diagrama típico de un sistema SI en una organización:

Figura 1.2: Diagrama típico de TI en una organización

Una aplicación típica que constituye el núcleo de un sistema de TI en una organización informatizada tendrá una combinación de un sistema de gestión de base de datos y bases de datos específicas, software de aplicación que elabora las reglas de negocio en el sistema a través de módulos específicos, interfaces *front-end* de usuario con soporte de software de aplicación de la red, en caso de existir una Red. Las bases de datos y software de aplicaciones residen en los servidores que son esencialmente computadoras con una alta capacidad que pueden albergar múltiples bases de datos y aplicaciones de gran tamaño. Los servidores podrían ser específicos para diferentes necesidades de los usuarios, como servidores de datos, servidores de aplicaciones, de Internet y proxy.

En base al nivel de conocimiento alcanzado respecto del Sistema de Información y de la entidad auditada, los auditores de TI pueden decidir su enfoque. La auditoría de TI finalmente comprende la auditoría de controles generales y/o de aplicación.

ii. Materialidad

La materialidad[14] de los temas de Auditoría de TI debe ser determinada dentro del marco general para decidir la política de materialidad en una EFS, al realizar un informe de auditoría. El auditor debe considerar la importancia del tema en el contexto de los estados financieros (auditoría de regularidad), o la naturaleza de la entidad o actividad objeto de la auditoría.

El auditor de TI debe determinar si alguna deficiencia general de TI podría ser potencialmente importante. La importancia de la deficiencia de tales controles generales de TI debe ser evaluada en relación a su efecto en los controles de aplicación, es decir, si los controles de aplicación asociados también son ineficaces. Si la deficiencia de aplicación es causada por el control general de TI, entonces es importante. Por ejemplo, si un cálculo impositivo realizado mediante la aplicación es sustancialmente incorrecto y fue causado por deficientes controles de cambios en las tablas impositivas, la decisión de la administración de no corregir una deficiencia de control en TI y su impacto asociado al entorno de

[14] *ISSAI 100* párrafo 43 define "La materialidad es considerada con frecuencia en términos de valor, pero la naturaleza inherente o características de un ítem o grupo de ítems pueden también convertirse en una cuestión material".

control podría transformarse en esencial cuando se suma a otras deficiencias de control que afectan el entorno de control.[15]

iii. Asignación de Recursos

La Auditoría de TI requiere la asignación específica de recursos, especialmente de personal que requiere estar bien familiarizado con los sistemas típicos, los procesos y los mecanismos que determinan una exitosa implementación de TI. Además de los recursos humanos[16] adecuados, se debe proporcionar un presupuesto razonable, infraestructura[17] y cualquier otro requisito identificado. Los plazos para la auditoría deben ser decididos, si es posible, conjuntamente con la entidad auditada.

iv. Compromiso con la Entidad Auditada

Se debe informar a la entidad auditada el alcance y los objetivos, y los criterios de evaluación de la auditoría se deben discutir con ésta, si es necesario. La EFS puede, de ser necesario, redactar la carta compromiso a la entidad auditada, en la que también podrá establecer sus términos. La EFS debe garantizar que se procure una debida cooperación y apoyo de la entidad auditada para concluir la auditoría, incluido el acceso a los registros e información, ya sea de forma manual o electrónica.

v. Recolección de Evidencia de Auditoría

1. Evaluación Preliminar de los Controles de TI

El auditor de TI debe llevar a cabo una evaluación preliminar de los controles de TI en el sistema que se audita para garantizar que los controles existentes (Controles Generales y Controles de Aplicación) sean confiables. La evaluación de controles a este nivel incluiría:

a. Evaluar la existencia y operación de los mecanismos adecuados de gobernanza de TI.
b. Evaluar el alineamiento de los objetivos de TI con los objetivos del negocio.
c. Evaluar la existencia de los mecanismos adecuados para alcanzar una solución de TI (que abarca la aplicación de TI, hardware, software, recursos humanos, redes, soluciones de servicio, etc.)
d. Los controles a nivel de la organización incorporados en las operaciones de TI, que regulan las funciones de TI diarias, los procedimientos de seguridad de la información de la organización, procedimientos de la continuidad del negocio y de las copias de seguridad, la gestión del cambio y prestación del servicio y comentarios.

Estos puntos comprenden los controles generales, que no son para un único flujo de registros o aplicables a una única aplicación, sino que se aplican a la infraestructura global de TI de la organización, incluidas las políticas, los procedimientos y las prácticas de trabajo relativos a las TI. Las pruebas tienen

[15] *Los conceptos de materialidad para Auditoría de la Información*, Directrices ISACA (G6).
[16] Recursos Humanos adecuados implica personal con conocimiento de los Sistemas de Información y podría llevar a cabo la extracción de datos y un análisis, de corresponder, ya que las Auditorías de TI invariablemente podría requerir el uso de habilidades de TI para llevar a cabo las auditorías. La EFS debería referirse a la ISSAI 100 párrafo 52, en donde se hace referencia a las competencias necesarias para su personal antes de llevar a cabo una auditoría de TI.
[17] Podría incluir las plataformas de hardware, sistemas operativos, RDBMS (base de datos), así como dispositivos de almacenamiento, instalaciones informáticas, como PC, laptops, etcétera, para que se pueda extraer y analizar la información.

que ser diseñadas específicamente utilizando técnicas como[18] entrevistas, encuestas mediante cuestionarios, observaciones, revisiones,[19] captura y análisis de datos y referencias, etc.

2. Pruebas Sustantivas

Las pruebas sustantivas están diseñadas para avalar las afirmaciones conforme a los objetivos de la auditoría. Las pruebas sustantivas incluyen pruebas detalladas de los Controles de TI, que utilizan varias técnicas y herramientas para la búsqueda, la extracción y el análisis de datos.

El análisis de datos incluye los puntos detallados a continuación:[20]

- Identificar el propósito del análisis o proyecto;
- Comprender la(s) muestra(s) que se analiza(n);
- Conocer la configuración y los formatos de datos;[21]
- Establecer un identificador único en caso que la fusión o correspondencia sean necesarias;
- Presentación de preguntas de investigación/objetivos de auditoría;
- Métodos utilizados para responder las preguntas de investigación;
  - ❖ Criterios para la evaluación
  - ❖ Evidencia
  - ❖ Análisis
  - ❖ Conclusión
- Procedimientos de reestructuración de archivos (creación de sintaxis, incorporación de nuevas variables, según sea necesario);
- Procedimientos de depuración de datos (por ejemplo, eliminación de los valores atípicos).

La mayoría de los análisis se pueden ejecutar directamente desde un archivo de datos de trabajo. Algunos análisis pueden requerir transformaciones de los datos sin procesar, subconjuntos, o datos de entrada específicos para cumplir con el software estadístico. Los sistemas de TI utilizan muchos y diferentes tipos de datos y representaciones (numéricos, cadena de caracteres, alfabéticos, etc.). El auditor de TI debe ser consciente de esto y utilizar las herramientas adecuadas para el análisis. El auditor puede utilizar el Software de Auditoría Generalizado o Software de Auditoría Especializado para llevar a cabo el análisis de la información. Herramientas tales como Microsoft Excel, Microsoft Access, IDEA, ACL, etc., son ejemplos de software de auditoría generalizado que proporcionan facilidad para importar y analizar los datos.

A partir de allí, cualquiera de las siguientes técnicas, según la necesidad, pueden ser adoptadas por los auditores de TI, tales como:

---

[18] Las técnicas pueden ser utilizadas para pruebas preliminares o sustantivas. El Auditor de TI puede escoger una o más técnicas al realizar cualquiera de estas dos evaluaciones.

[19] Las pruebas de revisión se llevan a cabo para comprender y verificar la confiabilidad del Sistema de TI de un cliente y los procedimientos de control interno. Esta prueba es más adecuada para comprender el sistema de TI o para verificar los hallazgos de las pruebas preliminares o resultados de otras pruebas de confirmación. Por lo tanto, no sería estrictamente una prueba de controles.

[20] *Una Visión General del Análisis de Datos*, de Jonathan Steinberg; *Investigación sobre Análisis de Datos*, de Bruce A. Kaplan; *Introducción al Análisis de Datos*, de Muhamad Jantan.

[21] Este podría ser uno de los pasos más importantes antes de realizar el análisis de datos. La configuración podría significar la comprensión de diferentes bases de datos, tablas insertas, codificación de patrones utilizados y relaciones entre la tabla y las bases de datos. La comprensión de los diferentes modelos de bases de datos podría ser útil en este sentido.

a) Llevar a cabo la extracción de datos mediante la **obtención de una copia** proveniente de la entidad auditada. Los auditores de TI tendrán que crear entornos similares (sistema operativo, sistema de gestión de bases de datos, hardware, etc.), al igual que en la entidad auditada para analizar/extraer datos de la copia obtenida. También se puede requerir que el auditor de TI convierta los datos de un formato a otro para facilitar una mejor lectura y análisis.

b) Utilizar el software de auditoría para extraer los datos de variadas combinaciones del sistema operativo, los sistemas de gestión de base de datos, el sistema de aplicación, etc. Los auditores de TI pueden utilizar el **Software de Auditoría General** o **Software de Auditoría Específico**. El Software de Auditoría General podría ser utilizado para industrias específicas o también podría ser de utilidad para evaluar el funcionamiento de diversas funcionalidades de los sistemas informáticos. La utilización de cualquiera de ellos o su combinación dependerá de los objetivos y el alcance que cubrirán las auditorías de TI.

c) Ejecutar **pruebas de datos** en situaciones en las que se intente evaluar la calidad del programa. La premisa es que es posible hacer una generalización de la confiabilidad general de un programa si éste es confiable para un conjunto de pruebas específicas. La utilización de pruebas de datos involucra el ***Diseño*** y ***Creación*** de las pruebas antes de ejecutar el programa.

El auditor de TI debe seleccionar una evaluación de riesgo adecuada y utilizar técnicas de muestreo para obtener conclusiones adecuadas basadas en controles estadísticos suficientes sobre datos limitados. Generalmente, es una buena práctica contratar la ayuda de un experto o un especialista en estadística dentro de la organización para seleccionar y determinar el método de muestreo.

III. DOCUMENTACIÓN DE AUDITORÍA

La documentación de auditoría de TI es el registro del trabajo realizado y de la evidencia de auditoría que respalda los hallazgos y las conclusiones. Los auditores de TI deben garantizar el resguardo de los hallazgos de auditoría y las evidencias obtenidas de forma tal que se ajusten a los requisitos de confiabilidad, integridad, suficiencia y exactitud. También es importante para los auditores de TI garantizar que el proceso de auditoría sea preservado para permitir la posterior verificación de los procedimientos ejecutados. Esto implica técnicas adecuadas de documentación.

La documentación incluye un registro de:

- La planificación y la preparación de los alcances y objetivos de la auditoría;
- Los programas de auditoría;
- La evidencia recolectada en base a la cual se arriba a las conclusiones;
- Todos los papeles de trabajo, incluido el archivo general perteneciente a la organización y al sistema;
- Los puntos tratados en las entrevistas que indiquen claramente el tema de discusión, la persona entrevistada, el cargo y designación, hora y lugar;
- Las observaciones realizadas por el auditor durante el desarrollo del trabajo. Las observaciones pueden incluir el lugar y la hora, el motivo de la observación y las personas involucradas;
- Los informes y los datos obtenidos del sistema directamente por el auditor o proporcionados por el personal auditado. El auditor de TI debe asegurar que estos informes comuniquen la fuente del informe, la fecha y la hora, y las condiciones cubiertas;

- En varios puntos de la documentación, el auditor puede añadir sus comentarios y aclaraciones sobre las inquietudes, las dudas y la necesidad de información adicional. El auditor debe remitirse nuevamente a estos comentarios con posterioridad, incorporar observaciones y referencias sobre cómo y dónde se resolvieron;
- Para proteger los datos electrónicos, las EFS deben realizar una copia de seguridad de los datos recibidos de la entidad auditada y de los resultados de la investigación y el análisis. La documentación de auditoría debe ser confidencial y debe conservarse durante un período conforme a lo decidido por la EFS o según lo exigido por la ley.
- Cuando el trabajo de auditoría es revisado por un par o un superior, las observaciones que surjan de la revisión también deben registrarse en la documentación.
- Los informes preliminares y el informe final de la auditoría deben formar parte de la documentación de auditoría.

IV. SUPERVISIÓN Y REVISIÓN

El trabajo del personal de auditoría debe ser supervisado apropiadamente durante la auditoría[22] y la documentación del trabajo debe ser revisada por un miembro senior del personal de auditoría.[23] Éste también debe proporcionar la función de orientación, capacitación y asesoramiento necesarios durante el desarrollo de la auditoría, que será esencial en esta nueva área - Auditoría de TI.

V. ELABORACIÓN DE INFORMES

Un informe de auditoría de TI debe cumplir con el diseño general de informes utilizado por la EFS. Los informes de auditoría de TI deben cuantificar las cuestiones técnicas informadas conforme al nivel de detalle que requieren los usuarios del informe. El auditor de TI debe informar sobre sus hallazgos de una manera oportuna y éstos deben ser constructivos y útiles para la entidad auditada, así como significativos para otras partes interesadas. El informe podría ser presentado a las autoridades pertinentes de acuerdo con el mandato de la EFS y la auditoría de TI.

VI. ETAPAS EN LA ELABORACIÓN DE INFORMES

Hay varias alternativas para cumplir con los requerimientos de ISSAI relacionados con la etapa final del proceso de auditoría. Éstas dependen de las prácticas de las EFS y de su marco legal. Una de ellas consta de tres etapas para la elaboración de los informes en el proceso de auditoría, a saber:

VI.1. Documento para Discusión

El proceso de elaboración de informes comienza con la discusión del primer borrador (documento para discusión). Este borrador se envía a la gerencia de nivel intermedio del auditado antes de la reunión de cierre. Luego, el borrador se incluye como un tema de discusión en la reunión de cierre. Esto permite que cualquier redacción polémica, errores de hecho y/o inconsistencias sean identificadas, corregidas o

[22] ISSAI 100 párrafos 39, 41.
[23] ISSAI 100 párrafo 54.

eliminadas en una etapa temprana. Una vez que el auditado y el auditor han discutido el contenido del borrador para discusión, el auditor hace las modificaciones necesarias y envía al auditado el primer Borrador Formal.

VI.2. Carta a la Gerencia

La carta a la Gerencia es el borrador formal entregado al auditado para que pueda responder a las observaciones planteadas. Esto permite a la Gerencia concentrarse en los hallazgos, las conclusiones y las recomendaciones del borrador formal que recibe. En este punto, es obligación de la Gerencia realizar comentarios por escrito/respuestas formales al auditor y abordar todos los hallazgos.

VI.3. Informe Final de Auditoría

Cuando se reciben los comentarios del auditado, el auditor prepara entonces una respuesta indicando el punto de vista de auditoría. Esto se logra aunando los comentarios del auditor y la respuesta de la entidad en un informe, que es el Informe de Auditoría (Informe Final de Auditoría).

Al informar irregularidades o situaciones de incumplimiento de leyes o reglamentaciones, los auditores deben ser cuidadosos de ubicar sus hallazgos en la perspectiva correcta. Los informes sobre las irregularidades se pueden preparar independientemente de la opinión del auditor.

Por su propia naturaleza, los informes de auditoría tienden a contener críticas importantes, pero para que sean constructivas también deben abordar medidas correctivas futuras mediante la incorporación de las manifestaciones de la entidad auditada o del auditor, incluidas las conclusiones y las recomendaciones.[24]

VI.4 Formulación de Conclusiones y Recomendaciones

Los hallazgos, conclusiones y recomendaciones de la auditoría deben basarse en la evidencia. Al formular la conclusión o el informe de auditoría, el auditor de TI debe tener en cuenta la importancia del tema en el contexto de la naturaleza de la auditoría o la entidad auditada.[25]

Los auditores de TI deben formular conclusiones a partir de los hallazgos de auditorías basados en los objetivos. Las conclusiones deben ser relevantes, lógicas e imparciales. Las conclusiones generales respecto de la ausencia de controles y riesgos conexos se deben evitar cuando no están respaldadas por pruebas sustantivas.

Los auditores de TI deben elaborar recomendaciones cuando la posibilidad de una mejora significativa en las operaciones y el rendimiento se fundamenta en los hallazgos informados. Los auditores también deben informar el estado de los hallazgos y recomendaciones significativas no corregidas de auditorías previas, que afectan los objetivos de la auditoría actual. Las recomendaciones constructivas pueden promover la mejora. Las recomendaciones son más constructivas cuando van dirigidas a solucionar la causa de los problemas identificados, están orientadas a la acción y son específicas, se dirigen a las partes que tienen autoridad para actuar, son viables y, en la medida de lo posible, rentables.

[24] *ISSAI 100* párrafo 55.
[25] *ISSAI 100* párrafo 54.

En una redacción de informes equilibrada se deben informar los logros relevantes, si éstos están contemplados dentro del mandato de las EFS para la elaboración de informes.

VI. 5 Limitaciones a la Auditoría de TI

Las limitaciones a la Auditoría de TI deben señalarse en el informe. Las limitaciones típicas podrían ser el acceso inadecuado a datos e información, la falta de documentación adecuada del proceso informático, que llevan al Auditor de TI a diseñar sus propios métodos de investigación y análisis para sacar conclusiones. Cualquier otra limitación que enfrenta el auditor de TI debe señalarse adecuadamente en el informe.

VI.6 Respuesta de la Entidad

En el caso de los informes de auditoría de TI, es muy importante obtener una respuesta a las observaciones de la auditoría. Los auditores de TI deben reunirse con la gerencia superior de la entidad y documentar su respuesta. Si estos esfuerzos fallan, la evidencia adecuada sobre los esfuerzos realizados debe registrarse en el expediente e incluirse en el informe correspondiente.

Referencias:

1. *COBIT 4.1 Marco, 2007*, Instituto de Gobernanza de TI.
2. IDI AFROSAI/E-IT Curso virtual de Auditoría.
3. *ISSAI 100 Principios Fundamentales de Auditoría del Sector Público.*
4. *ISSAI 200 Principios Fundamentales de Auditoría Financiera.*
5. *ISSAI 300 Principios Fundamentales de Auditoría de Desempeño.*
6. *ISSAI 400 Principios Fundamentales de Auditoría de Cumplimiento.*

PLANTILLA DE MATRIZ DE AUDITORIA

Uso de la Matriz de Auditoría

Durante la etapa de planificación es útil desarrollar una matriz de auditoría que abarque todos los aspectos importantes relativos a la auditoría, conforme a su objetivo y alcance.

Si bien las diferentes EFS utilizan diferentes formatos de matrices para planificar sus auditorías, existe uniformidad general en cuanto a la información que contienen.

Un formato sugerido para una matriz de auditoría[26], también utilizado en este manual, es el siguiente:

<table>
<tr><th colspan="2">AREA DE AUDITORIA</th></tr>
<tr><td colspan="2">Objetivo de Auditoría:</td></tr>
<tr><td colspan="2">Tema de auditoría:</td></tr>
<tr><td colspan="2">Criterios:</td></tr>
<tr><td>Información Requerida</td><td>Método(s) de Análisis</td></tr>
<tr><td colspan="2">Conclusión de la Auditoría
A ser completado por el Auditor:</td></tr>
</table>

1. Área de Auditoría

Los auditores de TI deben ser capaces de identificar los temas auditables durante la etapa de evaluación preliminar de la entidad y su entorno, particularmente el entorno de TI.

Los temas auditables también surgirán del alcance de la auditoría de TI. Por ejemplo, en muchas EFS una auditoría de TI se realiza conjuntamente con la auditoría financiera y de cumplimiento e involucra una evaluación de los controles generales y de aplicación de TI. En otros casos, el alcance de la auditoría de TI podría ser una evaluación de las acciones llevadas a cabo por la entidad para adquirir o desarrollar nuevos sistemas de TI. Cada vez más EFS están llevando a cabo una auditoría de desempeño integral de los sistemas críticos de TI. Algunos ejemplos son el sistema de recaudación y evaluación de ingresos/impuestos, el sistema de reservas ferroviario, la informatización de los servicios ciudadanos, como el registro de la propiedad, las estadísticas de población y números de identificación nacional, etc.

[26] La matriz de auditoría destaca temas importantes, criterios, etc., en diferentes áreas de auditoría de TI. Es importante para un auditor de TI entender que esta matriz se debe preparar en la etapa de planificación, si bien el contenido puede ser actualizado durante el proceso de auditoría, si corresponde. Asimismo, las EFS pueden realizar las modificaciones necesarias al formato de la matriz de auditoría, si lo consideran necesario.

Los temas auditables pueden surgir tanto de los temas relacionados con TI como de otros temas de gobernanza que tienen un impacto en el SI de la entidad auditada.

2. Los Auditores de TI también deben identificar Criterios de Evaluación Cuantificables, Confiables y Coherentes con los Objetivos/Temas de Auditoría que están siendo investigados en esta etapa.

Para cumplir con los criterios, la información o las evidencias adecuadas deben ser identificadas y recolectadas de manera que puedan ser preservadas para referencia futura, a fin de respaldar las conclusiones de la auditoría. La recopilación de la información puede requerir herramientas y técnicas específicas. Las diferentes herramientas y técnicas deben ser identificadas y utilizadas especialmente durante la fase de pruebas sustantivas. Los métodos de análisis también son típicos del entorno de SI y deben ser adecuadamente utilizados para obtener conclusiones pertinentes y significativas. Este tema se trata en el siguiente tópico sobre pruebas sustantivas en la ejecución de la auditoría.

Identificación de las Fuentes de Información

Las fuentes habituales de información en una organización que cuenta con Sistemas de TI pueden ser:

a) Diagramas de flujo, incluidos los diagramas de flujo de sistemas, diagrama de flujo de datos, diagrama de flujo de procesos, etc.
b) Documentos de desarrollo del sistema tales como el documento de Especificación de Requerimientos del Usuario (ERU) [27]o Especificación de Requerimientos del Sistema (ERS).
c) Datos electrónicos.[28]
d) Cualquier otra información disponible en la organización en relación con sus funciones, sistema de control y monitoreo, etc., como formularios, información presupuestaria, diferentes informes, incluidos los de auditorías previas, auditorías externas, revisiones internas, etc.
e) Políticas, procedimientos y otras directrices.
f) Usuarios del sistema.

Identificación de las Técnicas y Herramientas para la Recolección de Información

Las entidades auditadas tendrán su propia combinación de hardware, sistema operativo, sistemas de gestión de bases de datos, software de aplicaciones y software de redes, etc. Los auditores de TI deben ser capaces de reunir información de estas fuentes para llevar a cabo el análisis. Comprender el sistema de TI y la base de datos de la organización es claramente un paso esencial para la extracción de datos.

Los auditores de TI deben decidir sobre la conveniencia del uso de una o más de las técnicas antes mencionadas y garantizar que están satisfechos con la integridad y la utilidad de la técnica. El uso de

[27] El ERU – Documento de Especificación de Requerimientos del Usuario contiene requerimientos que muestran las funciones de la organización que se espera que el sistema de TI lleve a cabo y la operabilidad del usuario final deseada. Esta es la etapa en la que los usuarios deben especificar una clara y completa descripción de los requerimientos del usuario. Una especificación insuficiente de los requerimientos del usuario podría finalmente conducir al desarrollo de un sistema deficiente. Este es un buen punto de partida para el Auditor de TI.
[28] Los datos electrónicos incluyen datos estructurados. Los más comunes son los Sistemas de Gestión de Base de Datos Relacionales (RDBMS), que son capaces de manejar grandes volúmenes de datos tales como Oracle, IBM DB2, Microsoft SQL Server, Sybase y Teradata.

cualquiera de las técnicas anteriores no debe impactar en la integridad del sistema de aplicación y en los datos de la entidad auditada.

Las técnicas de recolección de datos deben basarse en la evaluación de riesgo llevada a cabo por el equipo de auditoría, así como en el tiempo y los recursos disponibles.

Las matrices de auditoría sugeridas para diferentes áreas auditables de TI se incluyen en los Anexos II -VIII de este Manual.

CAPÍTULO 2
GOBERNANZA DE TI

I. QUÉ ES LA GOBERNANZA DE TI

La Gobernanza de TI se puede considerar como el marco general que guía las operaciones de TI en una organización para garantizar que ésta cumple en la actualidad con las necesidades del negocio e incorpora planes para las necesidades y el crecimiento futuro. Es una parte integral de la gobernanza de la empresa y comprende el liderazgo organizacional, estructuras y procesos institucionales y otros mecanismos (información y comentarios, implementación, recursos, etc.) que aseguran que los sistemas sustentan los objetivos y la estrategia de la organización, al tiempo que equilibran los riesgos y gestionan la eficiencia de los recursos.

La Gobernanza de TI juega un papel clave en la determinación del entorno de control y fija las bases para el establecimiento de prácticas de control interno y la presentación de informes a niveles funcionales para la revisión y supervisión de la gestión.

Hay varias normas y marcos que definen los principios y los conceptos de la gobernanza de TI y de qué manera una organización puede optar por ponerlas en práctica.

Un marco genérico de gobernanza de TI se representa en la Figura 2.1

Figura 2.1: Marco Genérico de Gobernanza de TI.

I.1 Identificación de Necesidades, Dirección y Monitoreo

La gobernanza de TI es un componente clave de la gobernanza corporativa en general. La gobernanza de TI debe ser considerada como la forma en la que las TI crean valor para adaptarse a la Estrategia de Gobernanza Corporativa de la organización y nunca ser considerada como una disciplina por sí sola. Al adoptar este enfoque, se requerirá que todas las partes interesadas participen en el proceso de toma de decisiones. Esto crea una aceptación compartida de la responsabilidad para los sistemas críticos y garantiza que las decisiones relacionadas con TI sean tomadas y conducidas por la organización y no a la inversa.[29]

Para que la Gobernanza de TI garantice que las inversiones en TI generen valor en la organización y que los riesgos asociados con las TI sean mitigados, es esencial que una estructura organizacional con funciones bien definidas en cuanto a responsabilidad sobre la información, procesos de negocio, aplicaciones e infraestructura se ponga en marcha.

Además, es esencial que la gobernanza de TI se involucre con la identificación de necesidades nuevas o actualizadas de la organización y luego proporcione soluciones adecuadas de TI (y otras) al usuario de la organización. Durante el desarrollo o la adquisición de la solución a las necesidades de la organización, la Gobernanza de TI garantiza que las soluciones seleccionadas respondan a la organización y que la capacitación y los recursos necesarios (hardware, herramientas, capacidad de la Red, etc.) estén disponibles para implementar la solución. Las actividades de control pueden ser realizadas por la auditoría interna o por un grupo de aseguramiento de la calidad, que informarán periódicamente sus resultados a la gerencia.

Los elementos clave que definen la gobernanza de TI de una organización se describen a continuación.

I.2. Elementos Clave de la Gobernanza de TI[30]

a. Estrategia y Planificación de TI

La estrategia de TI representa la correspondencia mutua entre la estrategia de TI y los objetivos estratégicos de la organización. Los objetivos estratégicos de TI deben considerar las necesidades actuales y futuras de la organización, la capacidad actual de TI para prestar servicios y la necesidad de recursos.[31] La estrategia debe tener en cuenta la infraestructura tecnológica existente, la arquitectura, las inversiones, el modelo de prestación, los recursos, incluidos los recursos humanos y diseñar una estrategia que los integre en un enfoque común para apoyar los objetivos de la organización.

Es importante que el auditor de TI revise la estrategia de TI de la entidad con el fin de evaluar el grado en el que la gobernanza de TI ha sido parte de la toma de decisiones corporativas al decidir la estrategia de TI.

[29] *Qué es Gobernanza de TI y por qué es importante para el Auditor de SI* : WGITA IntoIT Ejemplar 25, agosto de 2007.
[30] Los elementos clave presentes en este capítulo de Gobernanza de TI están respaldados por el marco de referencia de buenas prácticas de TI COBIT y por la ISO 38.500 y un uso integral de sus definiciones y ejemplos.
[31] ISO 38.500.

b. Estructuras Organizacionales, Normas, Políticas y Procesos

Las estructuras organizacionales son un elemento clave de la gobernanza de TI en cuanto a la articulación de los roles de los diversos órganos de gobernanza y gestión en toda la organización y en la toma de decisiones. Éstas deben asignar una delegación claramente definida para la toma de decisiones y el control del desempeño. Las estructuras organizacionales deben ser respaldadas por las normas, las políticas y los procedimientos apropiados que deben fortalecer la capacidad para la toma de decisiones.

Las estructuras organizacionales en una entidad del sector público están influenciadas por las **Partes Interesadas** o *stakeholders* -es decir, los grupos, organizaciones, miembros o sistemas que afectan o pueden ser afectados por las acciones de una organización. Ejemplos de importantes grupos de interés externos incluyen el Parlamento, el Congreso y/u otras entidades gubernamentales y los ciudadanos. Las estructuras organizacionales también están influenciadas por los **Usuarios** - internos y externos. Los usuarios internos son los ejecutivos de la organización, los departamentos operativos que son responsables de los procesos y los individuos dentro de la organización que interactúan con los procesos de ésta última. Los usuarios externos son las entidades, individuos, y el público que utilizan los productos o servicios proporcionados por una organización (por ejemplo, otros departamentos, ciudadanos, etc.). Otra influencia en las estructuras organizacionales son los **Proveedores**, una empresa, unidad o personas - tanto externos como internos – que prestan un servicio.

La necesidad de funcionalidades de TI surge de los usuarios e interesados. En todos los casos, se requiere que las responsabilidades, roles y estructuras organizacionales de gobernanza adecuadas sean encomendadas al organismo regulador que aporte una clara responsabilidad y rendición de cuentas en cuanto a tareas y decisiones importantes. Esto debe incluir las relaciones con proveedores externos clave de servicios de TI.[32]

c. La estructura organizacional de TI generalmente incluye las siguientes funciones:

Comité Directivo de TI – esta es la pieza central de la estructura organizacional. Está compuesta por miembros de la alta dirección y gerencia senior que tienen la responsabilidad de revisar, aprobar y comprometer fondos para inversiones en TI. El Comité Directivo debe ser determinante en la elaboración de las decisiones organizacionales para las que se debe proporcionar tecnología a fin de respaldar las inversiones, así como en la aprobación de la forma para adquirir esta tecnología. Las decisiones de inversión que involucran las soluciones de construcción vs. compra son responsabilidad del Comité Directivo de TI, y generalmente se toman después de efectuadas las recomendaciones pertinentes por parte de los grupos o comités designados.

Por último, el comité directivo juega un papel fundamental tendiente a promover el compromiso necesario y proporcionar el respaldo a la gestión para programas que implican cambios en la organización. En muchas organizaciones del sector público, las funciones del Comité Directivo de TI forman parte de la función de gestión.

Gerente de Sistemas o Informática (CIO) - es el personal superior encargado de la gestión y explotación de las capacidades de TI de la organización. En muchas organizaciones del sector público, las funciones llevadas a cabo por el CIO pueden estar a cargo de un grupo o departamento que tiene las responsabilidades y facultades y los recursos necesarios.

[32] *COBIT 5* – Anexo E Mapeo de COBIT 5.

d. Normas, Políticas y Procesos

Las normas y las políticas son adoptadas por la organización y aprobadas por la gerencia encargada de esa función. Las políticas establecen el marco para las operaciones diarias con el fin de cumplir los objetivos fijados por la alta dirección. Las políticas son respaldadas por los procedimientos y/o los procesos que definen de qué manera se debe realizar y controlar el trabajo. Estos objetivos son establecidos por la gerencia respectiva a fin de cumplir con la misión de la organización y al mismo tiempo, con los requisitos reglamentarios y legales. Las políticas y procedimientos correspondientes deben ser comunicados a todos los usuarios y áreas pertinentes de la organización, de forma periódica.

Algunas de las políticas fundamentales que guían la gobernanza de TI incluyen:

- **Política de Recursos Humanos**

La política de recursos humanos se ocupa de la contratación, capacitación, terminación del contrato laboral y otras funciones. Tiene que ver con los roles y responsabilidades de los distintos miembros del personal dentro de la organización, así como con la habilidad o capacitación necesarias que deben poseer para llevar a cabo sus funciones. La política de recursos humanos también asigna funciones, responsabilidades y división de tareas.

- **Políticas de conservación de documentos y documentación**

La documentación de los sistemas de información, aplicaciones, roles de trabajo, sistemas de información y periodicidad es un importante punto de referencia para coordinar las operaciones de TI con los objetivos de la organización. Las políticas apropiadas de conservación de documentos permiten el seguimiento y la gestión de cambios reiterados en la arquitectura de la información de una entidad.

- **Política de subcontratación**

La subcontratación de TI muy a menudo está dirigida a permitir que la dirección de la entidad concentre sus esfuerzos en las principales actividades de la organización. La necesidad de subcontratación también puede ser impulsada por la necesidad de reducir los costos operativos. Una política de subcontratación garantiza que las propuestas para las operaciones de subcontratación y/o funciones y bases de datos, etc., se elaboren e implementen de manera beneficiosa para la organización.

- **Política de seguridad de TI**

Esta política establece los requisitos para la protección de los activos de información y puede referirse a otros procedimientos o herramientas sobre cómo éstos se van a proteger. La política debe estar disponible para todos los empleados responsables de la seguridad de la información, incluidos los usuarios de los sistemas de la organización que intervienen en la protección de la información (registros del personal, datos de ingresos financieros, etc.)

I. 3. Control Interno

El control interno es el proceso de introducción e implementación de un sistema de medidas y procedimientos para determinar si las actividades de la organización son y continúan siendo coherentes con los planes aprobados. Si es necesario, se toman medidas correctivas a fin de alcanzar los objetivos de la política. El control interno mantiene el sistema de TI operativo. Los controles internos incluyen la

gestión de riesgos, el cumplimiento de los procedimientos e instrucciones internas y de la legislación y la reglamentación externa, los informes periódicos y *ad hoc* de gestión, las verificaciones de progreso y revisión de los planes y auditorías, evaluaciones y monitoreo.[33]

a. Gestión de Riesgo[34]

La gestión de riesgos de TI debe ser una parte integral de las políticas y la estrategia de gestión de riesgos de la organización. La gestión del riesgo implica la identificación de los riesgos relativos a las aplicaciones existentes y a la infraestructura de TI, y la gestión permanente, incluida una revisión y actualización anual/periódica de la gestión de riesgos y un seguimiento de las estrategias de mitigación.

b. Mecanismo de Cumplimiento

Las organizaciones necesitan contar con un mecanismo que garantice que se está cumpliendo con todas las políticas y procedimientos conexos. Básicamente, es la cultura de la organización la que hace que todos los empleados se sensibilicen con todas las cuestiones relacionadas con el incumplimiento. El mecanismo de soporte del cumplimiento también puede incluir el grupo de aseguramiento de la calidad, personal de seguridad, herramientas automatizadas, etc. Un informe de incumplimiento debe ser revisado por la gerencia apropiada y debe tratar las cuestiones de incumplimiento grave o repetido. La gerencia puede optar por tratar el incumplimiento mediante una capacitación actualizada, procedimientos modificados, o incluso con un procedimiento de retribución creciente, dependiendo de la naturaleza del incumplimiento (violaciones a la seguridad, falta de capacitación obligatoria, etc.).

El control independiente, en forma de auditorías internas o externas (o revisiones), puede proporcionar información oportuna sobre el cumplimiento de las TI con las políticas de la organización, normas, procedimientos y objetivos generales. Estas auditorías deben llevarse a cabo de una manera imparcial y objetiva, de forma que los directivos reciban una evaluación justa del proyecto de TI que está siendo auditado.

I. 4. Decisiones de Inversión (Desarrollo y Adquisición de Soluciones)

La gobernanza de TI debe proporcionar a los usuarios de la organización soluciones a sus nuevos requerimientos o requerimientos modificados. Esto lo puede llevar a cabo la gerencia de TI, ya sea mediante el desarrollo (creación) de un nuevo software o sistemas, o bien adquiriéndolos a los proveedores a un costo razonable. A fin de lograr lo antedicho de manera exitosa, las buenas prácticas generalmente requieren un enfoque disciplinado donde se identifican, analizan, priorizan y aprueban los requerimientos, un análisis de costo – beneficio considerando soluciones dispares y la solución óptima seleccionada (por ejemplo, aquella que equilibre el costo y el riesgo).

I. 5. Operaciones de TI

Las operaciones de TI se refieren, normalmente, al funcionamiento diario de la infraestructura tecnológica para dar soporte a las necesidades de la organización. Una gestión adecuada de las operaciones de TI hace posible identificar impedimentos y planificar modificaciones anticipadas en la capacidad (hardware adicional o recursos de la red), evalúa el desempeño para garantizar que éste cumple

[33] *Gobernanza de TI en el Sector Público: Una prioridad esencial* - WGITA IntoIT Ejemplar 25, agosto de 2007.
[34] Ver el capítulo 8 sobre Seguridad de TI para una descripción más detallada.

con las necesidades acordadas con la alta dirección de la organización, y proporciona soporte a la gestión de incidentes y al servicio de atención para usuarios de los recursos de TI.

I.6 Personal y Recursos

Se recomienda que la gerencia garantice la asignación de suficientes recursos a TI a través de evaluaciones periódicas para satisfacer las necesidades de la organización, de acuerdo con las prioridades acordadas y las limitaciones presupuestarias. Asimismo, el aspecto humano debe ser respetado por las políticas, prácticas y decisiones de TI, que deben considerar las necesidades actuales y futuras de los participantes en el proceso. La gestión de gobernanza debe evaluar periódicamente si se utilizan o no los recursos y si se priorizan, tal como lo demandan los objetivos de la organización.

II. RIESGOS PARA LA ENTIDAD AUDITADA

Los auditores necesitan comprender y evaluar los diferentes componentes de la estructura de gobernanza de TI para determinar si las decisiones de TI, direcciones, recursos, gestión y monitoreo contribuyen con las estrategias y los objetivos de la organización. Para llevar a cabo la evaluación, el auditor debe conocer los componentes clave de la Gobernanza y la Gestión de TI. El auditor deber ser consciente de los riesgos asociados con las limitaciones de cada componente en una entidad.

Cada organización enfrenta sus propios y únicos desafíos ya que sus cuestiones individuales, ambientales, políticas, geográficas, económicas y sociales difieren. Aunque esta no es una lista exhaustiva, las consecuencias que se presentan a continuación representan los riesgos y consecuencias típicos que pueden derivar de la falta de una adecuada Gobernanza de TI.

a. Sistemas de TI ineficaces, ineficientes o incompatibles con el usuario:

Los sistemas de administración pública que tienen por objeto servir a la sociedad, empresa o mejorar la funcionalidad de los organismos gubernamentales, a menudo son soluciones muy amplias y complejas. Estos deben entonces ser diseñados adecuadamente, adaptados a las necesidades reales, coordinados completamente y ejecutados eficientemente. Una gobernanza deficiente de TI tanto a nivel de gobierno como a nivel de las organizaciones individuales puede ser un primer obstáculo para contar con una buena calidad en las TI.

b. Carencia de dirección de TI no permiten cumplir con las necesidades de la organización:

Escaso o nulo valor agregado puede resultar de grandes inversiones de TI que no estén estratégicamente alineados con los objetivos y recursos de la organización. Esta deficiente concordancia estratégica significa que incluso las TI de buena calidad pueden no contribuir eficaz y efectivamente a la consecución de los objetivos generales de la organización. Una forma de asegurar la concordancia es hacer que los usuarios y otras partes interesadas que estén en conocimiento del tema, participen en la toma de decisiones de TI.

c. Restricciones al crecimiento de la organización:

Una planificación inadecuada o deficiente de TI puede conducir a una limitación en el crecimiento del negocio por la falta de recursos de TI o el uso ineficiente de los existentes. Una forma de mitigar este riesgo es contar con la Estrategia de TI y actualizarla periódicamente, lo que permitirá identificar los recursos y los planes para satisfacer las necesidades futuras de la organización.

d. Gestión ineficaz de recursos:

Para obtener resultados óptimos a un costo mínimo, una organización debe gestionar de forma eficaz y eficiente sus recursos de TI. Garantizar la existencia de suficientes recursos técnicos, hardware, software y, sobre todo, recursos humanos disponibles para prestar los servicios de TI, es el factor clave para generar valor a partir de las inversiones en TI. Definir y monitorear el uso de los recursos de TI, por ejemplo, en un contrato de nivel de servicio, permite a la organización saber objetivamente si los requerimientos de recursos son adecuados para satisfacer las necesidades de la organización.

e. Toma de decisiones inadecuadas:

Deficiencias en la generación de información y reportes pueden conducir a una inadecuada toma de decisiones. Esto puede afectar la capacidad de la organización para prestar sus servicios y puede impedir que cumpla con su mandato. Los comités directivos y otros grupos organizacionales con adecuada representación, ayudan en la toma de decisiones que influyen en la organización.

f. Fallas en el proyecto:

Muchas organizaciones no tienen en cuenta la importancia de la gobernanza de TI. Asumen los proyectos de TI sin entender completamente cuáles son los requerimientos de la organización para y de qué manera este proyecto se vincula con sus objetivos. Si esta premisa no se comprende, los proyectos de TI son más propensos a presentar errores. Es también una falla común que las aplicaciones no cumplan con las normas mínimas de seguridad y arquitectura. Estos proyectos pueden incurrir en costos adicionales para mantener y administrar sistemas y aplicaciones no estándar. Un *ciclo de vida y desarrollo del sistema* (SDLC) definido y su uso en el desarrollo y/o la adquisición, es una forma de reducir el riesgo de fallas en los proyectos.

g. Dependencia de terceros (proveedores):

Mientras no existan procesos adecuados para controlar la adquisición o subcontratación, la organización podría enfrentar una situación en la que dependa completamente de un solo proveedor o contratista. En primer lugar, se trata de un entorno de alto riesgo, ya que si el proveedor abandona el mercado o si no presta los servicios contratados, la organización se encontrará en una situación difícil. Existen además otros problemas, por ejemplo, las disputas sobre la propiedad intelectual, los sistemas y las bases de datos. Las organizaciones que subcontratan o contratan regularmente soluciones con los proveedores pueden necesitar contar con una política de subcontratación o adquisición que defina lo que puede o no ser subcontratado.

h. Falta de transparencia y rendición de cuentas:

La rendición de cuentas y la transparencia son dos elementos importantes de una buena gobernanza. La transparencia es una fuerza poderosa que, cuando se aplica sistemáticamente, puede ayudar a combatir la corrupción, mejorar la gobernanza y promover la rendición de cuentas.[35] Por lo tanto, en ausencia de estructuras organizacionales adecuadas, estrategias, procedimientos y monitoreo, la institución puede comprometer la rendición de cuentas y su transparencia.

i. Incumplimiento de las declaraciones legales y reglamentarias:

Las partes interesadas requieren una mayor garantía de que las organizaciones cumplan con las leyes y los reglamentos y que se ajusten a las buenas prácticas de gobernanza corporativa en su entorno operativo. Además, debido a que las TI han permitido procesos fluidos entre las organizaciones, también hay una creciente necesidad de ayudar a garantizar que los contratos incluyan requisitos importantes relacionados con TI en áreas tales como privacidad, confidencialidad, propiedad intelectual y la seguridad (Marco COBIT 5, Principio 5, y Conformidad). Las diversas políticas con las que cuenta una organización, tales como Seguridad de TI, Subcontratación, Recursos Humanos, etc., deben incorporar los marcos legales y regulatorios pertinentes.

j. Exposición a los riesgos de seguridad de la información:

Una gran cantidad de riesgos de seguridad de la información puede surgir de la ausencia de estructuras adecuadas, procesos y políticas, tales como: la apropiación indebida de activos, la divulgación no autorizada de la información, el acceso no autorizado, la vulnerabilidad a los ataques físicos y lógicos, la interrupción y falta de disponibilidad de información, el uso indebido de la información, el incumplimiento de las leyes y reglamentaciones sobre datos personales, o la imposibilidad para la recuperación ante los desastres. La política de seguridad de TI debe definir los activos organizacionales (datos, equipos, procesos de negocio) que necesitan protección y vincularse a los procedimientos, herramientas y control de acceso físico que protejan tales activos.

La Gobernanza de TI continúa siendo un área de preocupación para la mayoría de las organizaciones del sector público. Al mismo tiempo, muchas EFS están enfocándose cada vez más en la Gobernanza de TI como parte de sus auditorías de TI. Los auditores de TI pueden ayudar a la Gobernanza de TI:

Garantizando que la se encuentre incluida en la agenda de la gobernanza corporativa general, y promoviendo estrategias de Gobernanza de TI.

Matriz de Auditoría

La matriz de auditoría presentada en el Anexo II es un punto de partida para que los auditores evalúen los controles de mitigación que las organizaciones han puesto en marcha para gestionar los riesgos que enfrenta la gobernanza de TI o la falta de la misma. Contiene las áreas mencionadas anteriormente.

Es importante tener en cuenta los temas de Gobernanza de TI que formarán parte de la evaluación general de los auditores del entorno general de control de la organización.

[35] *ISSAI 20, Conceptos de rendición de cuentas y transparencia*, pág. 4.

Referencias / Lecturas adicionales:

1. *Qué es la Gobernanza de TI y por qué es importante para el auditor de SI*, WGITA, IntoIT. http://www.intosaiitaudit.org/intoit_articles/25_p30top35.pdf
2. *COBIT 4.1 Marco*, 2007, Instituto de Gobernanza de TI.
3. *COBIT 5 Marco*, 2012, ISACA.
4. ISO/IEC 38500 Gobernanza Corporativa de Tecnología de la Información.
5. *OECD Principios de Gobernanza Corporativa*, OECD, 1999 y 2004.
6. Michaels Paul; Anand, Navin; y Iyer, Sudha; *Qué es Gobernanza de TI*. Mundo de la Informática. Reino Unido. Abril, 2012. http://blogs.computerworlduk.com/management-briefing/2012/04/what-is-it-governance/index.htm.
7. http://www.gao.gov/new.items/d04394g.pdf

CAPÍTULO 3
DESARROLLO Y ADQUISICIÓN

I. QUÉ SIGNIFICAN EL DESARROLLO Y LA ADQUISICIÓN

Con el fin de respaldar la estrategia organizacional, los proveedores de TI ofrecen soluciones para la organización o para usuarios de la organización. El proceso para el desarrollo, la adquisición o la subcontratación de una solución debe ser planificado de manera que los riesgos puedan ser gestionados y las probabilidades de éxito puedan ser maximizadas. Además, los requerimientos para estas soluciones deben ser identificados, analizados, documentados y priorizados. Las organizaciones también deben recurrir a aseguramientos de calidad y pruebas de funcionamiento para garantizar la calidad de estas soluciones.

Normalmente, las soluciones serán elaboradas o adquiridas por un equipo de proyecto. Si bien las organizaciones pueden ocasionalmente no formalizar un proyecto, las actividades normales se deben llevar a cabo.

Las soluciones pueden ser proporcionadas ya sea mediante desarrollo interno o adquisición externa, a través de un proceso de adquisición, o contratación o subcontratación. Con frecuencia, se utiliza un enfoque mixto que combina los enfoques anteriores.

De acuerdo con el CMMI® para Adquisición, Versión 1.3, de la Universidad Carnegie Mellon, las organizaciones se están convirtiendo cada vez más en compradoras de las capacidades necesarias, ya que los productos y servicios son de fácil acceso y generalmente resulta más barato que elaborarlos internamente. Sin embargo, el riesgo de adquirir productos que no cumplan con el objetivo de la organización o dejen de satisfacer a los usuarios es real. Estos riesgos deben ser gestionados de manera que la adquisición cumpla con éxito los objetivos de la organización. Cuando se hace de una manera disciplinada, la adquisición puede mejorar la eficiencia operativa de la organización mediante el aprovechamiento de las capacidades de los proveedores para proporcionar soluciones de calidad rápidamente, a menor costo y con la tecnología más adecuada.

La adquisición de un producto o solución, naturalmente requiere que la organización comprenda sus necesidades y requerimientos. El proceso de identificación de necesidades debe comprender a todos los actores pertinentes que están involucrados en el proceso del negocio, incluidos los usuarios finales y el personal técnico que puede finalmente mantener y respaldar el sistema. Al adquirir los servicios (asistencia técnica, herramientas informáticas de escritorio, etc.) la identificación de los requerimientos debe incluir el departamento de TI que estará en contacto con el proveedor de servicios. Los requerimientos deben ser priorizados de manera que si hay un déficit presupuestario u otras restricciones de costo, algunos de ellos puedan ser postergados para futuras elaboraciones o adquisiciones, según corresponda.

La definición de requerimientos es sólo el primer paso en el proceso de adquisición. La adquisición requiere la gestión de muchas áreas adicionales, por ejemplo, el riesgo, la gestión del programa, las pruebas, la supervisión de proveedores durante la adquisición -y posteriormente si operan o dan soporte al sistema-, y la integración de capacitación interna y/o las cuestiones de implementación. Hay ciertas buenas prácticas que, una vez adoptadas, aumentan la probabilidad de éxito en la adquisición de productos o servicios.

I. 1. Elementos Clave para el Desarrollo y la Adquisición

a. Requerimientos para el Desarrollo y la Gestión

Para cualquier proyecto de desarrollo o adquisición, la organización debe documentar los requerimientos de lo que desea/necesita, y gestionarlos. La gestión de los requerimientos incluye su priorización utilizando los criterios adoptados (por ejemplo, la criticidad, el costo y la complejidad) y segmentándolos en fases en caso que no todos puedan ser implementados en un sistema inicial. Además de la alta dirección, el proceso de identificación de requerimientos debe incluir usuarios, personal de soporte, expertos en el área, y otras partes interesadas, según corresponda. Los requerimientos constituyen la base del paquete de la solicitud (solicitud de propuesta), y deben ser claros y concisos. Al analizar y priorizar los requerimientos, la organización es capaz de tomar decisiones sobre costos y otras decisiones de compensación con el fin de obtener la solución óptima.

b. Gestión y Control del Proyecto

La gestión del proyecto incluye la definición del plan y las actividades de control. La gestión del proyecto incluye la definición de costos y el cronograma de referencia, la definición de los programas del proyecto, y el involucramiento de las partes interesadas en las actividades clave. El control del proyecto consiste en la supervisión y presentación de informes periódicos para tomar acciones correctivas cuando los resultados del proyecto no estén de acuerdo con el plan. Por ejemplo, si el costo del proyecto se eleva sustancialmente, la organización puede escoger recortar ciertas funciones después de consultar con las partes interesadas, para contener los costos. La estructura de gestión del proyecto se debe describir en el enfoque del Ciclo de Vida del Desarrollo del Sistema adoptado por la organización o en la estrategia de adquisición, según corresponda. Generalmente, esta estructura está compuesta por un gerente de proyecto, un director de riesgos, personal de soporte de gestión para la configuración y el aseguramiento de la calidad, personal del grupo de prueba, que no sea parte del aseguramiento de calidad, etc. El plan del proyecto sirve de base para orientar todas las actividades. Las reuniones informativas periódicas con la dirección superior los mantienen al tanto del estado del proyecto y de qué manera se gestionan los riesgos. Además, les permite considerar las compensaciones que involucran el costo, el cronograma y el rendimiento, ya que es poco frecuente que un proyecto cumpla con todos los objetivos previstos en estas áreas.

c. Aseguramiento de la Calidad y Prueba

El aseguramiento de la calidad proporciona al personal y a la gestión del proyecto una perspectiva de la funcionalidad y la calidad de los productos finales e intermedios del proyecto. Para ello, el personal involucrado en el aseguramiento de la calidad evalúa periódicamente los productos del proyecto para verificar si cumplen con los estándares de calidad documentados por la organización y si el personal ha cumplido con los procesos necesarios para desarrollar los productos. Los organismos deben verificar que el producto desarrollado o adquirido cumpla con los requisitos, los criterios de aceptación (por ejemplo,

menos de una cantidad determinada de errores no críticos, etc.) y hayan sido objeto de pruebas con usuarios y partes interesadas. El personal de aseguramiento de la calidad también debe garantizar que se está cumpliendo con la metodología de desarrollo adoptada y aceptada y que se lleva a cabo la supervisión requerida. Por ejemplo, se debe garantizar que las revisiones (formales y/o informales) se llevan a cabo y que los informes de estado necesarios son enviados a las partes interesadas y a la gerencia correspondiente. Además, a través de la participación del personal de aseguramiento de la calidad, la gerencia senior aplica u obtiene información sobre si el equipo del proyecto está cumpliendo con las políticas internas fijadas y los procedimientos para la tarea de adquisición o desarrollo.

d. Solicitud

La solicitud es el proceso de documentación de los requerimientos del negocio y la recolección de otros materiales de referencia que ayudan al proveedor en el suministro de la solución de TI. Incluye la generación del paquete de solicitud y su puesta en licitación, recepción de propuestas y selección entre los distintos proveedores. El proceso de selección debe ser transparente y objetivo y debe basarse en criterios que sean apropiados para el sistema o el servicio adquirido. Es fundamental que el equipo del proyecto involucre a su departamento legal en este proceso. El equipo legal conoce cabalmente las leyes y reglamentos y puede contribuir a garantizar que los criterios de selección de proveedores sean justos y puedan ser defendidos en un tribunal si otros proveedores perdedores impugnan la adjudicación.

e. Gestión de la Configuración

La Gestión de la Configuración se utiliza para garantizar el mantenimiento de la integridad de los documentos, el software y otros materiales descriptivos o de apoyo que forman parte del sistema. Los cambios en estos materiales (también llamados productos de trabajo) se gestionan y los puntos de referencia (o versiones) se establecen de manera que la organización sea capaz de retomar las versiones conocidas y probadas según sea necesario. El personal de gestión de la configuración también está involucrado en la aprobación o autorización para la instalación de software en el entorno de producción. Normalmente, esto se hace después de la prueba de usuario y cualquier otra prueba adicional necesaria para asegurar que otros sistemas sigan funcionando como lo hacían anteriormente, una vez que el nuevo sistema o el software es instalado (pruebas de regresión o pruebas de integración).

II. RIESGOS PARA LA ENTIDAD AUDITADA

Cuando una entidad desarrolla un software internamente hay una serie de riesgos o desafíos a los que se enfrenta para asegurar el éxito del proyecto. Algunos de éstos incluyen riesgos relacionados con habilidades en el dominio del software, experiencia en pruebas y gestión de proyectos, que tengan estimaciones de costo-beneficio razonables y sean capaces de controlar y realizar el seguimiento del estado del proyecto.

Además, el software o la obtención y aprobación de los requerimientos del sistema debe incluir a los usuarios, y los auditores examinarán si éstos fueron consultados en la definición de los requerimientos, y si el personal involucrado en el área de aseguramiento de la calidad está evaluando objetivamente la calidad del sistema mientras se está desarrollando. Al igual que en la adquisición, la gerencia debe ser informada periódicamente sobre el estado del proyecto y debe tomar las medidas correctivas apropiadas.

El objetivo principal de los auditores cuando se enfrentan a un organismo que ha llevado a cabo la adquisición de un sistema (o producto) es determinar si están controlando al proveedor y obteniendo

informes periódicos del estado y tomando medidas correctivas. Para esto, el contrato debe especificar los principales hitos durante el desarrollo, etapa en la que se realizan revisiones formales e informes del estado que proporcionan al organismo el costo, el cronograma y la información de desempeño. El auditor deberá garantizar que la gerencia de la entidad o el personal designado reciban, revisen y tomen medidas correctivas en los informes de situación y en las actividades de contratación, según corresponda.

Matriz de Auditoría[36]

La matriz de auditoría para esta selección se describe en el Anexo III.

Referencias/Lecturas adicionales:

1. http://www.dodig.mil/Audit/pmeguide.html
2. *Manual de Auditoría de Contratos de la DCAA.* EE.UU., 2013.
3. http://www.dcaa.mil/cam.htm
4. CMMI para Desarrollo, Versión 1.3
5. http://www.sei.cmu.edu/library/abstracts/reports/10tr033.cfm
6. CMMI para Adquisición, Versión 1.3
7. http://www.sei.cmu.edu/library/abstracts/reports/10tr032.cfm
8. ISACA – *Auditoría de Desarrollo del Sistema y Gestión de Proyectos/Marco de Aseguramiento*
9. *COBIT 4.1 Marco*, 2007, Instituto de Gobernanza de TI. Adquisición e Implementación.

[36] F/N: ibid.

CAPÍTULO 4
OPERACIONES DE TI

I. QUÉ SON LAS OPERACIONES DE TI

Si bien hay muchas interpretaciones o definiciones diferentes de las Operaciones de TI, generalmente se las considera como las tareas diarias involucradas en el funcionamiento y soporte de los sistemas de información de una organización (funcionamiento de servidores, mantenimiento, suministro del almacenamiento necesario, funcionamiento del servicio de atención al cliente, etc.). Las operaciones se miden y gestionan utilizando los Indicadores Clave de Desempeño para las operaciones de TI (KPI) que establecen parámetros en relación a los cuales se puede medir la eficacia operacional. Estas medidas o su equivalente normalmente se documentan y revisan periódicamente. La mayoría de las organizaciones las documentan mediante algún tipo de acuerdo entre los usuarios y el área de TI. El Contrato de Nivel de Servicio interno (SLA) es el acuerdo formal donde se documentan los parámetros y otras disposiciones.

II. ELEMENTOS CLAVE DE LAS OPERACIONES DE TI

Algunas de las áreas o elementos de las Operaciones de TI que el auditor deberá tener en cuenta para determinar si el organismo está gestionando con eficacia las Operaciones de TI incluyen, diseño y prestación del servicio, gestión de capacitación y servicios, procedimientos de manejo de incidentes para garantizar la continuidad de las operaciones y prácticas involucradas en la gestión del cambio. Estas y otras áreas están definidas en ITIL[37], uno de los marcos más ampliamente adoptados para identificar, planificar, prestar y dar soporte de servicios de TI a la organización.

Figura 4.1: Áreas de las Operaciones de TI.

Para determinar si la entidad auditada está prestando efectivamente los servicios documentados, el auditor deberá utilizar el SLA que deberá incluir los parámetros específicos para los distintos servicios. Podría haber situaciones en organizaciones más pequeñas, en las que, en lugar de un SLA, el acuerdo entre la organización y el grupo de TI puede ser documentado en

[37] ITIL, http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx

un gráfico o en algún otro documento. Independientemente de cómo se denomine al documento, el acuerdo debe ser documentado y acordado entre la organización o grupos de usuarios y el área de TI.

a. Gestión de Continuidad de Servicios de TI

El propósito de la gestión de continuidad de servicios es mantener los requerimientos actuales y adecuados de continuidad del negocio. El área de TI logra esto mediante el establecimiento de objetivos de tiempo de recuperación de los distintos componentes de TI que soportan los procesos de negocio basados en las necesidades y los requerimientos acordados. Además, la gestión de continuidad incluye revisar periódicamente y actualizar los tiempos de recuperación para garantizar que se mantengan en concordancia con los Planes de Continuidad del Negocio y las prioridades de la organización. Esta área se aborda en más detalle en el Capítulo 6.

b. Gestión de Seguridad de la Información

La gestión de seguridad de la información se refiere a la gestión de los riesgos relacionados con la seguridad, la adopción de medidas, según corresponda, y la garantía que la información esté disponible, utilizable, sea completa y veraz, cuando sea necesario. También se refiere al hecho de garantizar que sólo los usuarios autorizados tengan acceso a la información y la misma se encuentre protegida cuando se transfiere entre destinos y sea confiable a su arribo. Esta área es abordada más detalladamente a continuación en el Capítulo 7.

c. Gestión de Capacidades

La Gestión de Capacidades incluye la gestión de los diferentes servicios que contribuyen con la organización al responder a sus necesidades de TI o la de los usuarios. La optimización del rendimiento de las redes, la disponibilidad de recursos, la optimización y aumento del almacenamiento, son parte de la gestión de capacidades. Con el fin de gestionar las capacidades, el área de TI necesita determinar las condiciones y necesidades actuales para tomar medidas que faciliten el suministro de capacidades adicionales a los usuarios, por ejemplo, mediante la adquisición de potencia de procesamiento adicional cuando se cruzan ciertos parámetros (es decir, cuando la utilización del equipo está en 75% o más durante el 60% de la jornada laboral). Además, para un área de TI que presta servicios a una entidad, la gestión de capacidades será eficaz cuando se movilice personal de TI de la organización, debidamente calificado/capacitado, cuando se comprometan suficientes recursos y herramientas adecuadas para manejar el monitoreo de las redes y las funciones de atención al cliente, y el personal se involucre de forma proactiva en el abordaje de los dificultades, mientras continúa respondiendo a las necesidades de la entidad.

d. Gestión de Problemas e Incidentes

La gestión de incidentes se refiere a los sistemas y las prácticas utilizadas para determinar si los incidentes o errores son registrados, analizados y resueltos de manera oportuna. La gestión de problemas tiene como objetivo resolver las cuestiones a través de la investigación y de un profundo análisis de incidentes relevantes o recurrentes a fin de identificar la causa fundamental. Una vez que el problema ha sido identificado y se ha realizado el análisis de la causa fundamental, ésta se convierte en un error o ineficiencia conocida, y se puede desarrollar una solución para abordarla y prevenir futuras ocurrencias

de incidentes conexos. Un mecanismo debe ser puesto en marcha para la detección y documentación de las condiciones que podrían conducir a la identificación de un incidente. La sección de operación de TI debe contar con procedimientos documentados para la detección y el registro de condiciones anormales. Un manual, un registro computarizado de software de TI especializado pueden ser utilizados para registrar estas condiciones. Los ejemplos de incidentes podrían incluir tanto el acceso no autorizado del usuario como la intrusión (seguridad), fallas en la red (operacionales), baja funcionalidad del software (prestación de servicios) o la falta de habilidades del usuario final (capacitación).

e. Gestión de Cambio

En las organizaciones de TI, el proceso de gestión de cambio se utiliza normalmente para gestionar y controlar los cambios en los activos, tales como el software, el hardware, y la documentación conexa. Se necesitan controles de cambio para garantizar que todos los cambios en las configuraciones de los sistemas estén autorizados, probados, documentados y controlados para que los sistemas continúen dando soporte a las operaciones de la organización de la manera prevista, y que existan registros adecuados de las modificaciones.

Un cambio no autorizado o accidental podría tener graves riesgos y consecuencias financieras en una organización. Las organizaciones deben cumplir con un procedimiento de gestión de cambio definido que requiere la aprobación de un consejo antes de su implementación en el entorno operativo. El proceso de gestión de cambio debe garantizar que los cambios se registren, evalúen, autoricen, prioricen, planifiquen, prueben, implementen, documenten y revisen de acuerdo con los procedimientos de gestión de cambio documentados y aprobados.

Los cambios pueden ser iniciados, por ejemplo, ante el cambio en el entorno de la organización, la modificación del modelo de negocio, las necesidades inter-operacionales o con el resultado del análisis de incidentes/problemas. Los procedimientos de control de cambio deben incluir procedimientos específicos para la autorización de gestión (en una proforma estándar o proceso de documentación para el registro de la Solicitud de Cambio (RFC)); prueba exhaustiva y autorización de la gerencia de operaciones antes de su uso en el entorno real, revisión de gestión de los efectos de cualquier cambio, mantenimiento de registros adecuados; preparación de planes alternativos (en caso de una falla) y el establecimiento de procedimientos para realizar cambios de emergencia

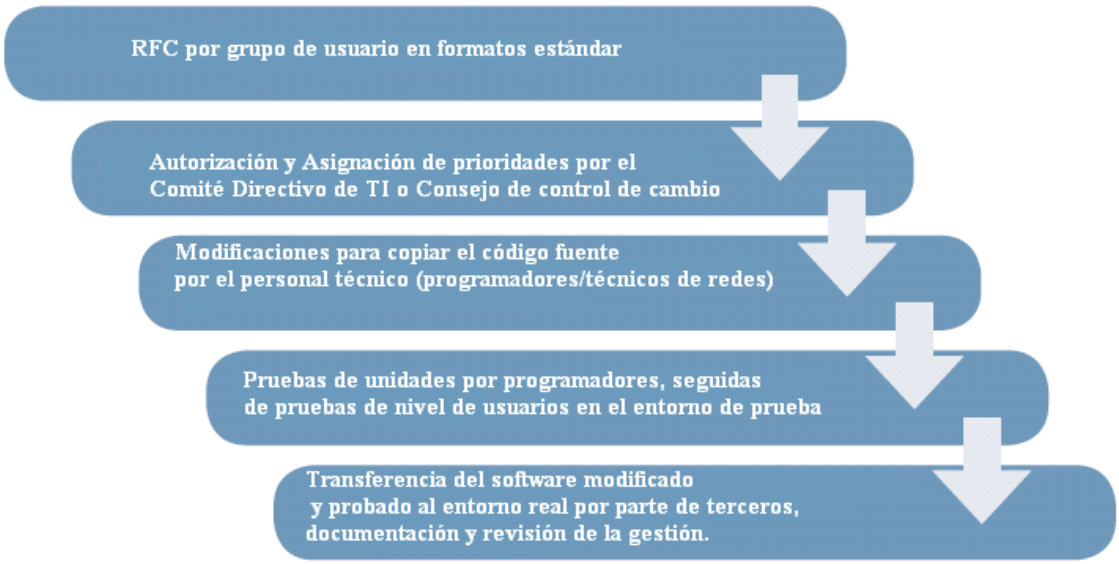


Figura 4.2: Pasos para la Gestión de Cambios

El costo del cambio, el impacto en las TI y los objetivos de la organización, las consecuencias de no implementar el cambio y los futuros requerimientos de recursos son variables significativas para autorizar y priorizar los cambios.

Los cambios de emergencia no pueden esperar para someterse a los procedimientos de control de cambios normales y deben ser implementados en un plazo mínimo. Existe un tiempo reducido para realizar y probar dicho(s) cambio(s). Esto origina un mayor riesgo de equivocaciones y errores de programación.

Cuando existen procedimientos de cambio de emergencia, el auditor debe verificar que sean razonables e incluyan algún tipo de control. Éstos podrían incluir la aprobación de un cambio de Emergencia por parte de un miembro del personal con autoridad competente, que cuente con las denominaciones de versiones y el control adecuados, junto con pistas de auditoría (el uso de las aplicaciones de control de cambio automatizadas), una aprobación anticipada por parte del consejo de cambios/titulares del sistema, pruebas anticipadas y actualización de la documentación.

f. Acuerdo de Nivel de Servicio (SLA)

El SLA documenta los distintos parámetros que la organización utiliza para prestar el servicio a la entidad. Los parámetros en el SLA son, en general, acordados por la alta dirección y el área de TI. El auditor utilizará los parámetros en el SLA para verificar si la organización está cumpliendo con los niveles de servicio y si la alta dirección de la entidad está satisfecha y toma las medidas adecuadas en caso de desviaciones de los parámetros de nivel de servicio acordados. Generalmente, también existe un SLA u otro acuerdo formal entre un área de TI y su(s) proveedor(es). Por ejemplo, un área de TI puede tener múltiples SLA entre sí y los distintos proveedores que prestan servicios subcontratados o nube virtual (*cloud computing*). El SLA que estamos analizando aquí es el SLA interno entre el área de TI y los clientes dentro de la organización.

El SLA contiene, entre otros elementos, los Indicadores Clave de Rendimiento (KPI) para los servicios de TI. La revisión de KPI ayudará al auditor a formular preguntas relacionadas con los siguientes enunciados:

- Si los sistemas están operando de conformidad con los acuerdos documentados.
- Si existen mecanismos para la identificación de desfasajes en el desempeño, para abordar desfasajes identificados y hacer un seguimiento de la implementación de las medidas correctivas adoptadas como resultado de la evaluación del desempeño de la entidad.
- La identificación de problemas de control en la entidad auditada, lo que contribuye a determinar la naturaleza, oportunidad y alcance de las pruebas.

Un ejemplo de mediciones de KPI con sus correspondientes definiciones y metas para la gestión del cambio, se presentan a continuación:

Proceso	Meta (Factor Crítico de Éxito)	Indicador Clave de Rendimiento	Arquitectura de Medición
Gestión de Cambio	Reducción de Incidentes causados por cambios no autorizados	Porcentaje de reducción en el número de incidentes derivados de un acceso no autorizado	Rastreado mediante la Gestión de Incidentes, Gestión de Cambios e informado mensualmente.

Puede haber casos en los que el área de TI ha subcontratado la mayor parte de sus funciones a un proveedor. En ese caso, el área de TI es el enlace entre el proveedor y los usuarios y es responsable de gestionar al proveedor para asegurar que se cumplan las necesidades del negocio. En el Capítulo 5 del Manual, se proporciona una guía detallada sobre auditoría de subcontratación de TI.

III. RIESGOS PARA LA ENTIDAD AUDITADA

La herramienta principal para el auditor, como se ha señalado anteriormente, es el contrato de Nivel de Servicio. Éste establece los parámetros e indicadores de desempeño y los requerimientos con los cuales se debe relacionar el área de TI. Si este documento es deficiente o no ha sido revisado formalmente y aprobado por la alta dirección de la entidad, existe el riesgo de que los recursos de TI de la organización no sean utilizados de la manera más eficaz o eficiente. Al auditar las operaciones de TI, el auditor deberá obtener el documento donde se definen el objetivo general y los parámetros técnicos de las operaciones de TI, por lo general, en el SLA.[38]

En el área de la gestión de cambio, el auditor debe verificar si existen procedimientos de control de cambios que garanticen la integridad del sistema y garanticen que sólo las aplicaciones autorizadas y probadas sean instaladas en el entorno operativo.

El auditor también debe preocuparse respecto de cómo la entidad está gestionando la capacidad (almacenamiento, CPU, recursos de red, etc.) de forma proactiva dando respuesta a los usuarios y de qué manera está gestionando los incidentes y otras cuestiones de seguridad para que las funciones de la organización no se vean comprometidas.

[38] Después de obtener el SLA, el auditor deberá obtener informes periódicos del área de TI que determinen e informen el estado de los indicadores, así como una revisión de la gestión de los mismos y cualquier medida a tomar o instrucciones al área de TI cuando existan desviaciones significativas de los parámetros acordados.

Matriz de Auditoría

La matriz de auditoría para esta sección se incluye en el Anexo IV.

Referencias/ Lecturas adicionales:

1. *CISA Manual de Revisión*. ISACA. 2011.
2. *CISA Guía de Desarrollo de Elementos*. ISACA.
3. http://www.isaca.org/Certification/Write-an-Exam-Question/Documents/CISA-Item-Development-Guide.pdf.
4. *COBiT 5*, 2012.
5. www.uservices.umn.edu/.../sla/BEST_PRACTICE_Service_Level_Agreement
6. *NIST- Guía para el Manejo de Incidentes de Seguridad Informática*.
7. http://www.cisco.com/en/US/technologies/collateral/tk869/tk769/white_paper_c11-458050.pdf
8. ISACA Programa de Aseguramiento de Auditoría de Gestión de Cambio.
9. ISACA – Programa de Aseguramiento de Auditoría de Incidentes de Seguridad.
10. Qué es ITIL http://www.itil-officialsite.com/AboutITIL/WhatisITIL.aspx

CAPÍTULO 5
SUBCONTRATACIÓN

I. QUÉ ES LA SUBCONTRATACIÓN

La subcontratación es el proceso de contratación de un proceso de negocio existente, que una organización realizaba previamente de manera interna, o bien de una nueva función comercial. La entidad contratada es responsable de la prestación de los servicios requeridos contractualmente por un monto acordado. Una entidad puede optar por subcontratar determinadas partes (o la totalidad) de su infraestructura, servicios o procesos de TI. La entidad debe contar con una política o una perspectiva sobre qué aspectos o funciones de negocio (por lo general de TI, pero podrían ser otros) subcontrata y qué funciones va a mantener internamente. Dependiendo de la criticidad del servicio subcontratado, una organización puede optar por mayores o menores controles formales sobre el servicio recibido. Las organizaciones de TI pueden decidir subcontratar la totalidad o parte de sus operaciones debido a que la subcontratación ofrece ciertas ventajas que incluyen:

- **Flexibilidad del personal**

La subcontratación permitirá que las operaciones que tienen demandas estacionales o cíclicas incorporen recursos adicionales cuando una organización los necesite y los libere cuando se concluyan las operaciones estacionales.

- **Desarrollo del personal**

Si un proyecto requiere habilidades con las que la organización no cuenta en la actualidad, ésta puede decidir subcontratar el proyecto en lugar de capacitar al personal interno para ahorrar tiempo y el costo de la capacitación. Por lo tanto, dependiendo de la ubicación física del proveedor y de su competencia técnica, la organización puede contar con personal interno que trabaje junto con el personal del proveedor por un período de tiempo, proporcionando así una capacitación práctica al personal.

- **Reducción de Costos**

La subcontratación normalmente debe resultar en una reducción de costos mediante la transferencia de costos laborales y otros al proveedor, quien tiene un costo laboral más bajo. Las organizaciones de TI buscan subcontratar las tareas que serían más costosas de llevar a cabo internamente. Un ejemplo de este tipo de tarea sería la relacionada con el software, que requiere una capacitación especializada. Las organizaciones que no cuentan con empleados calificados para realizar esta tarea pueden beneficiarse financieramente subcontratandola. La subcontratación de operaciones no esenciales también ayuda a la organización a concentrarse en su principal negocio y producir resultados de manera eficiente.

- **Expertos disponibles**

La subcontratación permite a la organización contar con expertos disponibles a la espera de necesitar asistencia con los problemas existentes o emergentes. La entidad es capaz de responder rápidamente a las cambiantes necesidades del negocio (nueva misión o funciones adicionales) con la ayuda de un experto.

- **Ejemplos de subcontratación**

De acuerdo con el documento de ISACA sobre subcontratación,[39] las entidades pueden subcontratar diversas áreas del negocio e infraestructura tecnológica. Algunos de ellos incluyen lo siguiente:

- Infraestructura operativa que puede incluir los centros de datos y los procesos conexos,
- Procesamiento de solicitudes internas por un proveedor de servicios,
- Desarrollo de sistemas o mantenimiento de aplicaciones,
- Instalación, mantenimiento y gestión de los equipos informáticos de escritorio y redes asociadas.

Un reciente avance en la subcontratación es la **Nube Virtual** (***Cloud Computing)*** [40]. En este caso, la organización subcontrata el procesamiento de los datos utilizando las computadoras de propiedad del proveedor. Básicamente, el proveedor aloja el equipo, mientras que la entidad auditada aún posee el control de la aplicación y los datos. La subcontratación puede también incluir la utilización de las computadoras del proveedor para almacenar, contar con una copia de seguridad, y proporcionar acceso en línea a los datos de la organización. La organización deberá tener un fácil acceso a internet si quiere que su personal o usuarios tengan acceso rápido a los datos o incluso a la aplicación que procesa los datos. En el entorno actual, los datos o aplicaciones también están disponibles en plataformas móviles (laptops con Wi-Fi o tarjetas celulares/móviles, teléfonos inteligentes y tabletas).

Los ejemplos de nube virtual incluyen las aplicaciones de correo electrónico en la Web y las aplicaciones regulares de la organización a las que se accede a través de un navegador, en lugar de un equipo local.

I.1 Elementos Clave de la Subcontratación

a. Política de Subcontratación

Las organizaciones necesitan contar con alguna política que defina qué funciones pueden ser subcontratadas y qué funciones deben continuar siendo internas a la organización. Normalmente, las organizaciones subcontratan las operaciones de TI de rutina, mantenimiento y hasta plataformas de hardware de escritorio. Los registros de RH y personal se mantienen generalmente dentro de las funciones internas ya que estos requieren un control estrecho y están sujetos a muchos requerimientos de seguridad y privacidad que pueden no hacerlos rentables para la subcontratación.

El auditor debe comenzar por revisar la política y los procedimientos de subcontratación de la entidad auditada. Es esencial que las entidades más grandes, que casi siempre tienen gran parte de sus operaciones subcontratadas, cuenten con una política de subcontratación aprobada, que incluya procesos de solicitud claramente establecidos. Las organizaciones más pequeñas pueden no tener una política formal, pero deben seguir procedimientos de solicitud eficientes y transparentes.

[39] Subcontratación de Auditorías Ambientales de TI/Programa de Aseguramiento, 2009.
[40] Ver Guía y Manual sobre Auditoría de *Cloud Computing*, WGITA.

b. Solicitud

La solicitud es el proceso de documentación de los requerimientos del sistema y de recopilación de otros materiales de referencia que ayudarán al proveedor a desarrollar el sistema. Incluye la generación del paquete de solicitud y su presentación a la licitación, obtención de propuestas y selección entre los distintos proveedores. El proceso de selección debe ser transparente y objetivo, y estar basado en criterios que sean apropiados para el sistema o los servicios adquiridos.

c. Gestión de Proveedores/Contratos

La gestión de proveedores es un elemento clave de la subcontratación para garantizar que los servicios se presten de acuerdo con las expectativas del cliente. La entidad auditada debe contar con procesos para garantizar el seguimiento periódico del estado del proyecto, la calidad del servicio, presenciar las pruebas de los productos fabricados antes de su introducción en el entorno operativo, etc. Además, como parte del proceso de monitoreo de los proveedores, la entidad auditada puede también auditar el proceso interno de aseguramiento de la calidad del proveedor para garantizar que el personal de este último cumple con la política contractual aprobada y los planes para la totalidad de las tareas.

El auditor deberá analizar si la entidad ha establecido sus requerimientos para la función de subcontratación antes de la selección del proveedor (los requerimientos específicos y los parámetros operativos están contenidos en el contrato y el SLA), si la entidad supervisa que el proveedor cumpla con los requerimientos establecidos en el SLA (por medio de informes de situación periódicos), y si la entidad toma medidas cuando el proveedor no cumple con los parámetros estipulados en el SLA (medidas correctivas o pago de multas).

d. Acuerdo de Nivel de Servicio (SLA)

El Acuerdo de Nivel de Servicio (SLA) es un contrato documentado entre la organización y el proveedor clave para gestionarlos.

El SLA debe definir los servicios que se espera que el proveedor preste, así como los parámetros técnicos de estos servicios, ya que se trata de un contrato legalmente vinculante entre el proveedor y la organización.

Las áreas típicas cubiertas en un SLA incluyen:

- Los tipos de servicios que prestará el proveedor,
- Asignación de responsabilidades entre la organización y proveedor,
- Los servicios que se considerarán, período de medición, duración, ubicación y cronograma de presentación de informes (porcentaje de defectos, tiempo de respuesta, horario de atención al cliente, etc.),
- Tiempo para implementar nuevas funcionalidades, niveles de reorganización,
- Tipo de documentación requerida para las aplicaciones desarrolladas por el proveedor,
- Lugar donde se prestarán los servicios,
- Frecuencia de la copia de seguridad, parámetros de recuperación de datos,
- Métodos y formatos de entrega de datos y terminación,

- Cláusulas de incentivos y sanciones.

En resumen, la mayoría de los elementos que son críticos para la organización deben ser establecidos en un contrato de nivel de servicio. El auditor de TI debe solicitar el SLA u otro documento (contrato o acuerdo formal), donde se documentan estos parámetros y se garantiza que la información del proveedor respecto de varios parámetros cumple con el requerimiento o que la organización ha tomado las medidas correctivas necesarias para hacer frente a las deficiencias.

e. Obtención de Beneficios

Generalmente, las entidades auditadas subcontratan para obtener una reducción en los costos. Esto se logra cuando el costo para la prestación de estos servicios es menor a través de un proveedor que utilizando personal y/o la infraestructura internos. Hay otros beneficios que no son directamente cuantificables, tales como aprovechar la infraestructura del proveedor para ampliar rápidamente el nivel de servicio o utilizar su experiencia para casos especiales. Siempre que sea posible, la entidad debe tratar y determinar si los ahorros previstos se están logrando de forma periódica. Esto sirve como punto de referencia para decidir si continuar o no con la capacidad subcontratada.

f. Seguridad

Al subcontratar las bases de datos y su administración, las organizaciones de TI deben evaluar si los proveedores aplican prácticas de seguridad lo suficientemente sólidas y si los proveedores pueden cumplir con los requerimientos de seguridad, a nivel interno. Si bien la mayoría de las organizaciones de TI consideran muy positivas las prácticas de seguridad de los proveedores (a menudo superan las prácticas internas), el riesgo de fallas en la seguridad o la protección de la propiedad intelectual aumenta en sí mismo debido al hecho que los datos han sido subcontratados. Las cuestiones de seguridad deben ser también abordadas. Otras cuestiones relacionadas con la seguridad incluyen el posible mal uso o la divulgación de información confidencial, el acceso no autorizado a los datos y las aplicaciones y el plan de recuperación ante desastres. A pesar que estas cuestiones pocas veces suponen obstáculos importantes a la subcontratación, los requerimientos deben ser documentados.

II. RIESGOS PARA LA ENTIDAD AUDITADA

a. Preservación del Conocimiento del Negocio y Propiedad de los Procesos del Negocio

Existe un riesgo inherente de pérdida de conocimiento del negocio que reside en los desarrolladores de las aplicaciones. Si el proveedor, por alguna razón, es incapaz de prestar este servicio, el área de TI debe estar dispuesta a asumir esta obligación nuevamente. Además, como el desarrollo de la aplicación se producirá fuera de la entidad, esta última también corre el riesgo de renunciar o perder la titularidad de los procesos del negocio, que el proveedor de servicios puede reclamar como propia. Las organizaciones deben abordar esta cuestión al momento de celebrar al contrato y deben garantizar que cuentan con la documentación completa del proceso de desarrollo del sistema y los diseños de los sistemas. Esto también ayudará a la organización a cambiar de proveedor de servicio, si es necesario.

b. Incumplimiento de Entrega del Proveedor

A veces un proveedor simplemente puede dejar de entregar un producto puntualmente, o bien se debe renunciar al mismo debido a la falta de una correcta funcionalidad. Si el proceso de solicitud no se implementa correctamente, hay una alta probabilidad de que el sistema o los servicios adquiridos puedan no satisfacer las necesidades del usuario, sean de una calidad inferior, cuesten más, requieran recursos significativos para el mantenimiento y la operación, o sean de tan mala calidad que tendrán que ser sustituidos en un futuro cercano. Un mal contrato, un sistema defectuoso de selección de proveedores, hitos no claros y/o condiciones desfavorables del mercado, son algunas de las razones más comunes del incumplimiento del proveedor.

Las organizaciones de TI deben contar con planes de contingencia para tal evento. Al considerar la subcontratación, las organizaciones de TI deben evaluar las consecuencias del incumplimiento del proveedor (es decir, ¿tiene el incumplimiento implicancias significativas en el desempeño del negocio?). La disponibilidad de documentación detallada sobre el diseño y el desarrollo del sistema ayudarán a la organización a garantizar la continuidad del negocio a través de otro proveedor de servicios, o por ellos mismos.

c. Expansión del Alcance

Todos los contratos de subcontratación contienen puntos de referencia y supuestos. Si el trabajo real varía en relación con las estimaciones, el cliente deberá pagar la diferencia. Este simple hecho se ha convertido en un obstáculo importante para las áreas de TI, que ven con sorpresa que el precio no sea "fijo" o que el proveedor espera que se le pague por los cambios graduales en el alcance. La mayoría de los proyectos se modifican entre un 10% y 15% en relación a las especificaciones durante el ciclo de desarrollo.

d. Rotación de Personal Clave

El rápido crecimiento entre los proveedores externos ha creado un mercado laboral dinámico. El personal clave demanda, por lo general, nuevos proyectos de alto perfil, o corre el riesgo de ser contratados por otros proveedores externos. Mientras que los proveedores externos a menudo citan estadísticas generales de facturación que parecen relativamente bajas, la estadística más importante para gestionar es la rotación de personal clave en una cuenta. Los niveles de rotación normales están en un rango del 15%-20%, y la creación de las condiciones contractuales en torno a esos niveles es un pedido razonable.

e. Riesgos Externos (Fuera del País)

El empleo de proveedores de servicios en el extranjero es una forma común de subcontratación, especialmente en un entorno de nube virtual. En este escenario, los riesgos de tal subcontratación implicarían reglamentaciones de otro país respecto del almacenamiento de información y la transferencia puede limitar lo que se puede almacenar y de qué manera se puede procesar, los datos pueden ser utilizados por autoridades policiales del país extranjero sin conocimiento de la organización, las normas de privacidad y seguridad no siempre pueden ser las adecuadas, y no se pueden evitar totalmente las disputas en virtud de jurisdicciones legales diferentes.

Matriz de Auditoría

La matriz de auditoría para esta sección se presenta en el Anexo V.

Referencias/ Lecturas adicionales:

1. Davison, Dean. Los *10 principales riesgos de la Subcontratación Offshore*. 2003. http://www.zdnet.com/news/top-10-risks-of-offshore-outsourcing/299274
2. *Auditoría de Entornos de TI Subcontratados/Programa de Aseguramiento*, 2009. ISACA. http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Outsourced-IT-Environments-Audit-Assurance-Program.aspx
3. *Gobernanza de Subcontratación*. ISACA, 2005. http://www.isaca.org/Knowledge-Center/Research/Documents/Outsourcing.pdf
4. *Directriz sobre Contratos de Servicio: Elementos Esenciales.* Secretaría de la Tesorería de Canadá. www.tbs-sct.gc.ca
5. NIST SP 500-292, *NIST Arquitectura de Referencia del* Cloud Computing *(nube virtual).*
6. NIST SP 800-144, *Directrices sobre Seguridad y Privacidad en la Cloud Computing (nube virtual) Pública.*

CAPÍTULO 6

PLAN DE CONTINUIDAD DEL NEGOCIO (BCP) Y PLAN DE RECUPERACIÓN ANTE DESASTRES (DRP)

I. QUÉ SON BCP y DRP

Las organizaciones gubernamentales dependen cada vez más de la disponibilidad y el correcto funcionamiento de sus sistemas informáticos a fin de cumplir con sus obligaciones legales. Los sistemas informáticos juegan un papel importante en actividades tan diversas como la evaluación y recaudación de impuestos e ingresos aduaneros, y el pago de las pensiones públicas y los beneficios de la seguridad social, en el procesamiento de las estadísticas nacionales (nacimientos, fallecimientos, crímenes, enfermedades, etc.). De hecho, muchas actividades no se podrían llevar a cabo de manera eficaz –o siquiera llevarse a cabo– sin el soporte de las computadoras.

La pérdida de energía, las acciones industriales, los incendios y los daños maliciosos pueden tener efectos desastrosos en los sistemas informáticos. Puede tomar varias semanas a una organización reanudar las operaciones comerciales de manera eficiente si no cuenta con un plan de continuidad del negocio viable.

Los términos "Plan de Continuidad del Negocio" y "Plan de Recuperación ante Desastres" algunas veces son utilizados como sinónimos, aunque en realidad son dos términos distintos, pero complementarios. Ambos son importantes para el auditor de TI, porque juntos garantizan que la organización es capaz de operar con una cierta capacidad definida después de una alteración natural o provocada por el hombre. Ambos se explican a continuación:

- **Plan de Continuidad del Negocio (BCP):** Es el proceso que una organización utiliza para planificar y poner a prueba la recuperación de sus procesos de negocio después de una alteración. Asimismo, describe de qué manera una organización seguirá funcionando bajo condiciones adversas que puedan surgir (por ejemplo, desastres naturales u otros).

- **Plan de Recuperación ante Desastres (DRP):** Es el proceso de planificación y prueba para la recuperación de la infraestructura tecnológica después de un desastre natural o de otro tipo. Es un subgrupo del Plan de Continuidad del Negocio. El BCP se aplica a las funciones organizacionales del negocio, mientras que el DRP se aplica a los recursos de TI que dan soporte a las funciones de la organización.

Básicamente, el **BCP** aborda la capacidad de una organización para seguir funcionando cuando se alteran las operaciones normales. Este plan incorpora las políticas, los procedimientos y las prácticas que permiten a una organización recuperar y reasumir los procesos manuales y automáticos fundamentales para la misión después de un desastre o crisis. Además de expresar las prácticas que se deben seguir en caso de una interrupción, algunos BCP incluyen otros componentes tales como recuperación ante desastres, respuesta ante la emergencia, recuperación del usuario, y actividades para la gestión de crisis y contingencias. Por lo tanto, en estas organizaciones, la continuidad del negocio se considera un término

abarcador que comprende tanto la recuperación ante desastres como la reanudación de las actividades de la organización.

Sin embargo, ya sea como parte del BCP o como un documento separado, el DRP debe definir los recursos, las acciones, las tareas y los datos necesarios para gestionar el proceso de recuperación de una organización, en caso de interrupción de su actividad. Este plan también debe asistir a la organización cuando se restauran los procesos afectados, delineando los pasos específicos que la organización debe seguir en su camino hacia la recuperación. Específicamente, el DRP es utilizado para la preparación y la planificación anticipadas necesarias para minimizar los daños producidos por los desastres y garantizar la disponibilidad de los sistemas de información fundamentales de la organización. En términos de TI, los DRP abordan la recuperación de activos de tecnología críticos, incluyendo los sistemas, aplicaciones, bases de datos, dispositivos de almacenamiento y otros recursos de red[41].

I.1. Elementos Clave del BCP y DRP

Se requiere que el auditor de TI evalúe los programas de gestión de continuidad del negocio de la entidad, lo cual implica la evaluación de los planes de continuidad del negocio y recuperación ante desastres, y los sistemas de gestión de crisis. Para ello, los auditores deben comprender qué implica el desarrollo de una estrategia de gestión de continuidad del negocio y los pasos que deben tomar para evaluar la eficacia de los programas existentes, que incorporan la continuidad necesaria, la recuperación ante desastres y las tareas de gestión de crisis.

Una planificación de la continuidad efectiva tiene varias fases comunes a todos los sistemas de información. Los pasos genéricos en el proceso son[42]:

1. Política y Plan de Continuidad del Negocio;
2. Organización de la función de Continuidad del Negocio;
3. Análisis de Impacto en el Negocio (BIA) y Gestión de Riesgos;
4. Controles preventivos, incluidos los ambientales;
5. Plan de Recuperación ante Desastres;
6. Documentación del plan de continuidad del negocio;
7. Plan de pruebas y capacitación;
8. Seguridad durante la implementación del BCP/DRP;
9. Copia de seguridad y recuperación ante desastres para los servicios subcontratados.

Estos pasos representan elementos clave para una capacidad de planificación de continuidad del negocio integral. Los elementos se explican de la siguiente manera:

a. Política, Planificación y Organización de la Continuidad del Negocio

Una planificación de la continuidad efectiva comienza con el establecimiento de la política de continuidad del negocio de una organización. El equipo de gestión de continuidad de negocio[43] que representa todas las funciones apropiadas de la organización, también juega un papel importante en el éxito del plan de

[41] *La función del auditor de TI en la Gestión de Continuidad del Negocio*, Publicación IIA. http://www.theiia.org/intAuditor/itaudit/archives/2008/january/the-it-auditors-role-in-business-continuity-management

[42] Publicación Especial del NIST 800-34, *Guía para la Planificación de Contingencia de los sistemas de Información Federal*, proporciona asesoramiento sobre los procesos de planificación de contingencias.

[43] Explicado en la siguiente sección.

continuidad. El documento que establece la política de Planificación de Continuidad del Negocio debe definir los objetivos generales de la continuidad de la organización, y establecer el marco organizacional y las responsabilidades para la planificación de la continuidad.

b. Establecimiento de la Función de Continuidad del Negocio

Para que esta función sea exitosa, el equipo de gestión de continuidad del negocio debe estar organizado para representar todas las funciones adecuadas del negocio. La gerencia senior y otros funcionarios relacionados con el área deben respaldar el programa de continuidad y deben estar vinculados con el proceso de desarrollo de la política. Los roles y las responsabilidades del equipo deben estar claramente identificados y definidos.

c. Evaluación del Impacto y Gestión de Riesgo del Negocio

i. Evaluación de la criticidad y la sensibilidad de las Operaciones Informáticas e Identificación de los Recursos de Soporte

En cualquier organización, la continuidad de ciertas operaciones es más importante que la de otras, y no es rentable proporcionar el mismo nivel de continuidad para todas las operaciones. Por esta razón, es importante que la organización determine cuáles son los recursos más importantes y qué recursos se necesitan para recuperarlos y respaldarlos. Esto se lleva a cabo mediante la realización de una evaluación de riesgo, la identificación de las posibles amenazas y sus impactos en la información de la organización y los recursos conexos, como los datos, software de aplicación y las operaciones. El riesgo y la evaluación del impacto deben cubrir todas las áreas funcionales. En consecuencia, se debe tomar una decisión sobre el riesgo residual cuando el impacto de una posible amenaza sea mínimo o los sistemas de control sean los adecuados para resaltar tales instancias a tiempo.

ii. Identificación y Priorización de Operaciones y Datos Fundamentales

La criticidad y sensibilidad de diversos datos y de las operaciones se deben determinar y priorizar en base a categorizaciones de seguridad y de una evaluación general del riesgo de las operaciones de la organización. Dicha evaluación de riesgo debe servir como base del plan de seguridad de una organización. Los factores a considerar incluyen la importancia y la sensibilidad de los datos y otros activos de la organización, y el costo de no restablecer los datos u operaciones inmediatamente. Por ejemplo, una interrupción de un día de los principales sistemas de pago y recaudación de impuestos o una pérdida de datos conexos podría interrumpir significativamente o demorar la recepción de los ingresos, debilitar el control de millones de dólares en ingresos, y reducir la confianza pública. Por el contrario, un sistema que controla la capacitación de los empleados podría estar fuera de servicio quizás durante varios meses sin graves consecuencias.

Generalmente, los datos críticos y las operaciones deben ser identificados y clasificados por el personal que participa en el negocio de la organización o de las operaciones del programa. También es importante obtener el consentimiento de la gerencia senior a tales determinaciones, así como la concurrencia de los grupos afectados.

La lista de prioridades de recursos y operaciones de información críticos debe ser revisada periódicamente para determinar si las condiciones actuales se reflejan en ella. Estas revisiones deben

ocurrir cada vez que haya un cambio significativo en la misión y las operaciones de la organización o en la ubicación o diseño de los sistemas que apoyan estas operaciones.

iii. Identificación de los Recursos que dan Soporte a las Operaciones Críticas

Una vez que se hayan determinado los datos y las operaciones críticas, se deben identificar los recursos mínimos necesarios para respaldarlos y se deben analizar sus roles. Los recursos a ser considerados incluyen recursos tecnológicos, como el hardware, el software y los archivos de datos; redes, incluidos componentes tales como *routers* y *firewalls*; suministros, incluidos el papel y los formularios pre impresos, servicios de telecomunicaciones; y otros recursos que son necesarios para la operación, como el personal, las instalaciones, suministros de oficina y registros no informatizados.

Dado que es probable que los recursos esenciales sean gestionados por una variedad de grupos dentro de una organización, es importante que el personal de soporte de seguridad de la información y del programa trabaje en forma conjunta para identificar los recursos necesarios para las operaciones críticas.

iv. Establecimiento de Prioridades en el Procesamiento de Emergencias

Conjuntamente con la identificación y clasificación de las funciones críticas, la organización debe desarrollar un plan para restaurarlas. El plan debe identificar claramente el orden en que se deben restaurar los diversos aspectos del procesamiento, quién es responsable, y qué equipo de soporte u otros recursos se necesitarán. Un plan de restauración de procesamiento cuidadosamente desarrollado puede ayudar a los empleados a comenzar inmediatamente el proceso de restauración y a hacer más eficiente el uso de los recursos informáticos limitados durante una emergencia. Tanto los usuarios del sistema como el personal de soporte de seguridad de la información deben participar en la determinación de las prioridades en el procesamiento de emergencia.

v. Prevención y Minimización de Posibles Daños e Interrupción

Hay una serie de pasos que una organización debe seguir para evitar o minimizar el daño a las operaciones informáticas que puede ocurrir a raíz de eventos inesperados. Estos se pueden clasificar como:

- Duplicación o copias de seguridad de rutina de archivos de datos, programas informáticos y documentos clave con almacenamiento externo, y/o disposición de instalaciones de seguridad remotas que pueden ser utilizadas si las instalaciones habituales de la entidad están dañadas más allá del uso;
- Establecimiento de un sistema de recuperación de información y capacidad de reconstitución de modo que el sistema de información se pueda recuperar y reconstituir a su estado original después de una interrupción o falla;
- Instalación de controles ambientales, tales como sistemas de extinción de incendios o fuentes de respaldo de alimentación de energía;
- Garantizar que el personal y otros usuarios del sistema comprendan sus responsabilidades en situaciones de emergencia; y
- Mantenimiento eficaz del hardware, gestión de problemas y gestión de cambios.

vi. Implementación de Datos y Procedimientos de Copia de Seguridad del Programa

La copia de rutina de archivos de datos y software, y el almacenamiento de estos archivos en una ubicación segura y remota suelen ser las medidas más rentables que una organización puede tomar para mitigar las interrupciones del servicio. Si bien los equipos a menudo se pueden reemplazar con facilidad, el costo podría ser significativo. Reconstruir los archivos de datos y reemplazar el software puede ser muy costoso y consumir tiempo. Ciertamente, los archivos de datos no siempre pueden ser reconstruidos. Además de los costos directos de reconstrucción de archivos y obtención de software, las interrupciones de servicios conexos pueden dar lugar a importantes pérdidas financieras.

vii. Capacitación

El personal debe estar capacitado y debe ser consciente de sus responsabilidades en cuanto a la prevención, mitigación y respuesta a situaciones de emergencia. Por ejemplo, el personal de soporte de seguridad de la información debe recibir capacitación periódica en procedimientos de emergencia, incendios, inundaciones, e incidentes de alarma, así como en sus responsabilidades en la puesta en marcha y funcionamiento de un sitio de procesamiento de datos alternativo. Además, si los usuarios externos son esenciales para las operaciones de la organización, se les debe informar los pasos que deben adoptar como consecuencia de una emergencia.

viii. Planes de Mantenimiento de Hardware, Gestión de Problemas y Gestión

Interrupciones inesperadas del servicio pueden ocurrir por fallas en el hardware o cambios en los equipos, sin notificación anticipada a los usuarios. Para evitar dichas situaciones, se requiere un programa eficaz de mantenimiento, gestión de problemas y gestión de cambios para el hardware.

d. Controles Preventivos y Ambientales

Los controles ambientales previenen o mitigan los posibles daños a las instalaciones y las interrupciones en el servicio. Ejemplos de controles ambientales incluyen:

- Extintores y sistemas contra incendios;
- Alarmas contra incendios;
- Detectores de humo;
- Detectores de agua;
- Iluminación de emergencia;
- Redundancia en los sistemas de refrigeración de aire;
- Fuentes de alimentación de respaldo;
- Existencia de llaves de paso y procedimientos para toda la plomería de construcción que pueda poner en peligro las instalaciones de procesamiento;
- Instalaciones de procesamiento construidas con materiales resistentes al fuego y diseñadas para reducir su propagación; y
- Políticas que prohíban comer, beber y fumar dentro de las instalaciones informáticas.

Los controles ambientales pueden disminuir las pérdidas originadas por algunas interrupciones, tales como incendios, o prevenir incidentes mediante la detección temprana de problemas potenciales, como fugas de agua o humo. Además, los sistemas de alimentación ininterrumpida o las fuentes de alimentación de respaldo pueden permitir que transitar los cortes de energía, o proporcionar tiempo suficiente para realizar copias de seguridad de datos y llevar a cabo procedimientos ordenados cuando el corte es por periodos prolongados.

e. Plan de Recuperación ante Desastres

Un plan de recuperación ante desastres debe ser desarrollado a los fines de la restauración de las aplicaciones esenciales, lo que incluye la disposición de instalaciones de procesamiento alternativas en caso que las instalaciones habituales se encuentren significativamente dañadas o no se pueda acceder a ellas. Las políticas y procedimientos a nivel de la organización definen el proceso de planificación de la recuperación y los requerimientos de documentación. Además, un amplio plan para toda la organización debe identificar los sistemas críticos, las aplicaciones y cualquier plan secundario o conexo. Es importante que estos planes estén claramente documentados, sean comunicados al personal involucrado, y actualizados para reflejar las operaciones en curso.

i. Documentación del Plan de Recuperación Actualizado

Los planes de recuperación ante desastres deben estar documentados, acordados por las áreas operativas y de seguridad de la información, y comunicados al personal afectado. El plan debe reflejar los riesgos y las prioridades operacionales que la entidad ha identificado. Debe estar diseñado de manera que los costos de la planificación de la recuperación no superen los costos asociados con los riesgos que se espera que el plan pueda reducir. El plan también debe ser lo suficientemente detallado y documentado para que su éxito no dependa de los conocimientos o la experiencia de uno o dos individuos.

Varias copias del plan de continuidad deben estar disponibles y algunas de ellas deben estar almacenadas en ubicaciones externas para garantizar que no se destruyan a raíz de los mismos eventos que hicieron que las instalaciones de procesamiento de datos primarios no estén disponibles.

ii. Disposiciones en Lugares Alternativos

Dependiendo del grado de continuidad del servicio necesario, las opciones para los sitios o instalaciones alternativas van desde un lugar equipado listo para el servicio de copia de seguridad inmediata, conocido como un "*hot site*", a un lugar sin equipar, que tomará un tiempo de preparación para las operaciones, conocido como un "*cold site*". Además, los distintos tipos de servicios pueden ser acordados previamente con los proveedores. Éstos incluyen acuerdos con los proveedores de servicios de telecomunicaciones y hardware, así como con los proveedores de formularios y otros insumos de oficina.

f. Pruebas

i. Prueba Periódica del Plan de Continuidad

La prueba de los planes de continuidad es esencial para determinar si van a funcionar tal cual lo previsto en una situación de emergencia. La realización de la prueba revelará importantes debilidades en los planes, como los mecanismos de copia de seguridad que no pudieron replicar adecuadamente las

operaciones críticas, tal como se esperaba. A través del proceso de prueba, estos planes tienen que ser mejorados sustancialmente.

La frecuencia de la prueba del plan de continuidad variará dependiendo de la criticidad de las operaciones de la organización. Generalmente, los planes de continuidad para funciones muy críticas deben ser totalmente probados una vez cada uno o dos años, cuando se hayan realizado cambios significativos en el plan o cuando se produzca una importante rotación de personal clave. Es importante para la gerencia senior evaluar los riesgos de los problemas del plan de continuidad y desarrollar y documentar una política sobre la frecuencia y alcance de tales pruebas.

ii. Actualización del Plan de Continuidad en Base a los Resultados de la Prueba

Los resultados de las pruebas de continuidad proporcionan un importante indicador de viabilidad del plan de continuidad. Por lo tanto, deben ser informados a la gerencia senior para poder determinar la necesidad de modificación y de pruebas adicionales, y para que la gerencia senior tenga conocimiento de los riesgos de continuar las operaciones con un plan de continuidad deficiente.

g. Seguridad

La seguridad de los recursos y de las operaciones debe ser incorporada al plan de continuidad del negocio, ya que los datos críticos, software de aplicaciones, operaciones y recursos pueden verse comprometidos fácilmente ante cualquier caso de desastre o durante una actividad de gestión de continuidad del negocio. Por ejemplo, durante la realización de la copia de seguridad de datos, la falta de seguridad puede conducir a la creación de copias duplicadas y pérdida de datos importantes. Al mismo tiempo, podría suceder que los datos que se están resguardando se vean comprometidos durante el proceso (datos copiados del servidor de producción a datos que se resguardados en un servidor de back ups).

h. Resguardo y Recuperación de Datos para Servicios

Muchas organizaciones subcontratan la totalidad o parte de su actividad a un proveedor de servicios. Puesto que las operaciones y los controles diarios son llevados a cabo por el proveedor de servicios, será fundamental para la organización garantizar que el plan de continuidad del negocio y de recuperación ante desastres sea incorporado al contrato. La organización también tendrá que controlar que la continuidad del negocio y la preparación para la recuperación ante desastres sean garantizadas por el proveedor de servicios. Esto incluirá también la preparación de la seguridad del proveedor de servicios. La organización también debe garantizar que el proveedor de servicios mantenga la confidencialidad de los datos y que éste conserve el software de aplicación. La titularidad del proceso del negocio debe quedar en poder de la organización. La organización también debe contar con un plan de continuidad para garantizar la continuidad del proveedor de servicios, o si éste es adquirido por otra empresa.

II. RIESGOS PARA LA ENTIDAD AUDITADA

Los servicios o productos esenciales son aquellos que deben ser entregados para garantizar la supervivencia, evitar pérdidas, y cumplir con las obligaciones legales u otro tipo de obligaciones de una organización. El BCP/DRP es un proceso de planificación proactivo que garantiza que los procesos del negocio y la infraestructura tecnológica de una organización sean capaces de respaldar las exigencias de

la misión luego de un desastre o interrupción. Las entidades gubernamentales cumplen con muchas exigencias esenciales de la misión (pago a ciudadanos, atención médica, educación, defensa, y otros servicios de los que depende el ciudadano). Si estos servicios se interrumpen durante largos períodos de tiempo, esto dará lugar a pérdidas financieras o de otros tipos. Los auditores deben garantizar que todas las entidades gubernamentales cuenten con un proceso de BCP/DRP que garantice que la entidad es capaz de seguir sirviendo a los ciudadanos.

Al evaluar si los procesos de BCP/DRP son capaces de garantizar y proteger la confiabilidad de la infraestructura tecnológica y la continuidad del proceso del negocio, hay algunos riesgos en los que los auditores pueden enfocarse para evaluar su eficacia. Estos incluyen la elaboración de planes de continuidad del negocio y recuperación ante desastres para cubrir todas las áreas funcionales esenciales. Si la recuperación ante desastres de un área funcional esencial se ve comprometida, lo mismo sucederá con la continuidad del negocio. Si los roles y responsabilidades no son claros y comprensibles para el personal pertinente, un buen plan de continuidad también puede resultar ineficaz.

El procedimiento de evaluación de impacto del negocio, los controles preventivos y ambientales, la documentación, las pruebas del plan de continuidad y la capacitación del personal afectado contribuyen con la implementación efectiva del plan de continuidad del negocio de la organización. Una implementación deficiente del plan de continuidad del negocio o del plan de recuperación ante desastres plantea el riesgo de pérdida de datos, pérdida de tiempo, entre otros costos.

Los servicios subcontratados presentan un área de riesgo distinta donde el BCP y DRP no están totalmente bajo el control de la organización. Existen riesgos relacionados con la seguridad de los datos, pérdida de datos, manipulación no autorizada y filtración, que deben ser abordados. La continuidad de la función a través del propio proveedor de servicios subcontratado presenta un riesgo, ya sea por la pérdida de conocimiento del negocio, o la titularidad de los procesos y, por lo tanto, por la dificultad para cambiar el proveedor de servicios en caso de un desempeño deficiente o, alternativamente, debido al cierre o adquisición del proveedor de servicios por parte de otras entidades.

Matriz de Auditoría

La matriz de auditoría para esta sección se describe en el Anexo VI.

Referencias

1. *Manual de Auditoría de Sistemas de Información Federal de GAO* (FISCAM).
2. COBIT 4.1 *Marco*, 2007, Instituto de Gobernanza de TI.
3. *Guía para la Planificación de Contingencias para los Sistemas de Información Federal* de NIST, Publicación Especial 800-34.
4. *El Rol del Auditor de TI en la Gestión de Continuidad del Negocio*, Auditor Interno, edición Enero 2008.

CAPITULO 7
SEGURIDAD DE LA INFORMACIÓN

I. QUÉ ES LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información puede ser definida como la capacidad de un sistema para proteger la información y sus recursos en relación con la confidencialidad y la integridad. Se refiere a la protección de la información y de los sistemas de información contra el acceso no autorizado o la modificación de la información, ya sea en el almacenamiento, procesamiento o tránsito, y contra la no prestación del servicio a los usuarios autorizados. La seguridad de la información incluye las medidas necesarias para detectar, documentar y mitigar esas amenazas, y permite a una organización proteger la infraestructura tecnológica de usuarios no autorizados. La seguridad de la información comprende la seguridad informática y la seguridad de las comunicaciones.

Un aspecto fundamental de la gobernanza de TI es la seguridad de la información para garantizar su **disponibilidad, confidencialidad** e **integridad** – de la cual depende el resto. La seguridad de la información debe comprender muchos aspectos de la organización. Es la puerta de acceso a los activos de la información de la organización. Esto exige que el programa de seguridad de la información proteja los datos de la organización al tiempo que le permita alcanzar los objetivos del negocio y tolerar un nivel aceptable de riesgo al hacerlo. Proporcionar información a aquellos que deben tenerla es tan importante como protegerla de aquellos que no deben tenerla. La seguridad debe contribuir con el negocio y con el logro de los objetivos organizacionales, más que servir a sus propios intereses.

I.1. Necesidad de Seguridad de la Información

La seguridad de la información es cada vez más importante para las instituciones gubernamentales a medida que la interconexión de las redes públicas y privadas y el intercambio de recursos de información aumentan la complejidad para controlar el acceso y preservar la confidencialidad, integridad y disponibilidad de los datos.

Los sistemas de información son ensamblajes muy complejos de tecnología, procesos y personas que actúan conjuntamente para adecuar el procesamiento, almacenamiento y transmisión de la información a fin de apoyar la misión y las funciones de la organización. Por lo tanto, es esencial que cada organización elabore un programa de seguridad de la información.

El objetivo de un programa de seguridad del sistema de información es proteger la información de una organización reduciendo el riesgo de pérdida de la confidencialidad, integridad y disponibilidad a un nivel aceptable. Si la organización no garantiza la seguridad de la información, entonces, se enfrentará a riesgos y posibles amenazas a las operaciones de la organización, la consecución de los objetivos generales y, en definitiva, afectará su credibilidad.

A medida que el potencial, la complejidad y el papel de las Tecnologías de Información crecen, la seguridad de la información se convierte en un tema cada vez más importante de las auditorías de TI. Es

un factor fundamental de las actividades de las organizaciones, debido a que las debilidades en la seguridad de información pueden causar graves daños como:

- **Ley** – violaciones de los requisitos legales y reglamentarios.
- **Reputación** – daño a la reputación de la organización, de otras organizaciones, o de la imagen del gobierno o del Estado.
- **Finanzas** – por ejemplo, multas, indemnizaciones, reducción de ventas o aumento de costos.
- **Productividad** – reducción de la eficacia y/o eficiencia de un proyecto, programa o servicio proporcionado por la organización.
- **Vulnerabilidad** – los sistemas y datos a los que se accede en forma no autorizada son susceptibles a programas maliciosos y pueden estar expuestos a nuevas intrusiones.

Estos daños pueden ser causados por:

- Violaciones a la seguridad, tanto detectadas como no detectadas.
- Conexiones externas no autorizadas a sitios remotos.
- Exposición de la información – divulgación de activos corporativos e información confidencial a terceros no autorizados.

I.2. Formación de la Cultura de Seguridad de la Información

Un factor que determina el éxito de los programas de seguridad de la información en una organización es la creación de una cultura organizacional que contemple esas cuestiones. Para abordar de manera uniforme estas y otras cuestiones en una gran organización, se debe seguir un modelo de negocio relativo a la seguridad de la información.[44] Éste debe contener los siguientes puntos:

- **Crear conciencia sobre la seguridad:** este punto consiste en actividades generales de toma de conciencia sobre los sistemas de información y capacitación dirigida a los empleados. Estas sesiones son una buena oportunidad para comenzar a dar a conocer las responsabilidades de seguridad de la información. El área de recursos humanos puede ser responsable de la capacitación inicial sobre la toma de conciencia para los nuevos empleados. La capacitación debe realizarse durante la duración del empleo del personal y hasta la finalización de su trabajo en la organización, promoviendo la toma de conciencia respecto a la seguridad.

- **Obtener el compromiso de la administración:** el compromiso de la administración es un atributo único en la formación de la cultura de seguridad de la información. La administración muestra su compromiso no sólo al preparar documentación oficial que contenga información sobre las políticas de seguridad, sino también al participar activamente. Si la administración no apoya seriamente el programa de seguridad de la información, puede desmotivar el sentido de obligación o responsabilidad con el programa de cualquier otro empleado. Por lo tanto, es esencial que la administración asuma la titularidad del programa de seguridad de la información y lo respalde por completo.

- **Construir una coordinación sólida mediante la conformación de equipos con personal de diversas áreas:** Debido a que la seguridad de la información comprende muchos aspectos de la organización que deben ser coordinados, se debe considerar la conformación de equipos con personal

[44] ISACA Modelo de Negocios para Seguridad de la Información, 2010.

de distintas áreas de la organización. La formación de tales equipos fomenta la comunicación y la colaboración, y reduce el aislamiento de los departamentos y la duplicación de tareas.

El establecimiento de una cultura de seguridad de la información es una parte integral de la implementación de la gobernanza en la organización de SI, y se caracteriza por lo siguiente:

- **Correspondencia entre la seguridad de la información y los objetivos de la organización:** Es necesario que exista una correspondencia entre la seguridad de la información y los objetivos de la organización, ya que permite y respalda sus. El programa de seguridad de la información se alinea con la organización y requiere que los controles sean prácticos y proporcionen una reducción del riesgo real y cuantificable.

- **Evaluación de riesgo:** La aplicación de la seguridad de la información debe complementarse con una evaluación de riesgos para determinar el tipo de control requerido. Con frecuencia se desestima la evaluación de riesgos, lo cual puede dar como resultado que la infraestructura y la información sensible no estén protegidas adecuadamente o, en algunos casos, se las sobreproteja innecesariamente. La aplicación de la evaluación de riesgos ayudará a la gerencia a seleccionar los controles adecuados para mitigarlo de manera efectiva.

  El proceso de evaluación de riesgos incluye la identificación y el análisis de:

  - Todos los activos y los procesos relacionados con el sistema.
  - Amenazas potenciales que podrían afectar la confidencialidad, la integridad o la disponibilidad del sistema.
  - Vulnerabilidades del sistema y amenazas conexas.
  - Impactos y riesgos potenciales por acción de la amenaza.
  - Requerimientos referidos a la protección para mitigar los riesgos.
  - Selección de medidas de seguridad adecuadas y análisis de las relaciones de riesgo.

- **Equilibrio entre la organización, las personas, los procesos y la tecnología:** la seguridad de la información efectiva requiere el respaldo de la organización, personal competente, procesos eficientes y selección de tecnología apropiada. Cada elemento interactúa con una u otra área, afecta y complementa al resto de los elementos, a menudo en formas complejas y, por lo tanto, es esencial lograr un equilibrio entre ellos. Si cualquiera de los elementos es deficiente, la seguridad de la información disminuye.

I.3 Elementos Clave de la Seguridad de la Información

a. Entorno de la Seguridad de la Información

A fin de respaldar la implementación exitosa y efectiva de la Seguridad de la Información, hay algunos aspectos esenciales que se deben cumplir. Éstos son los siguientes:

- **Confidencialidad:** significa preservar las restricciones autorizadas sobre el acceso a la información y la divulgación, incluidos los medios para la protección de la privacidad personal y la información reservada. El aspecto de confidencialidad es muy importante porque involucra cuestiones de privacidad que deben ser consideradas. Para preservarla de manera constante, el sistema debe garantizar que cada individuo conserve el derecho de controlar qué información se recopila sobre ellos, cómo se utiliza, quién la utiliza, quién la preserva y cuál es el propósito de su utilización.

- **Integridad:** significa la protección contra la modificación o destrucción indebida de información, lo que incluye garantizar su irrefutabilidad y autenticidad.[45] Para certificar la integridad de la información es necesario un mecanismo de autenticación que garantice que los usuarios son las personas que dicen ser; mientras que el proceso para garantizar la información creada o transmitida, debe cumplir los requisitos de irrefutabilidad. [46]

- **Disponibilidad:** significa garantizar que todos los sistemas de información, incluido el hardware, redes de comunicación, aplicaciones de software y los datos que poseen estarán a disposición de los usuarios cuando sea necesario para llevar a cabo las actividades del negocio. También debe garantizar el acceso oportuno y confiable a la información. Sin embargo, cumplir con el principio de seguridad respecto del uso de hardware, redes de comunicación, aplicaciones de software, y acceso a datos requiere una política de control de acceso. El objetivo del control de acceso es garantizar que los usuarios sólo accedan a los recursos y servicios a los que tienen derecho a acceder y que no se niegue a los usuarios calificados el acceso a los servicios que legítimamente esperan recibir.

La seguridad de la información se refiere a minimizar la exposición, en base a la gestión de riesgos, en todas las áreas del modelo de Gobernanza de TI. La falta de implementación y de monitoreo de los procesos de mitigación de riesgos en un área puede causar daños en toda la organización. Aún cuando exista un conocimiento amplio en cuanto a que la gestión eficaz de los riesgos de seguridad de la información es esencial para la seguridad de una organización, estos riesgos son a menudo pasados por alto o las medidas de seguridad no se actualizan en respuesta a las condiciones cambiantes.

La discusión sobre la Seguridad de la Información en la organización cubre las siguientes doce áreas:

b. Evaluación de Riesgo

La evaluación de riesgos es el proceso de identificación, análisis y estimación de riesgos en la infraestructura de Seguridad de TI. Es el proceso de evaluación de los riesgos relacionados con la seguridad a partir de amenazas internas y externas a la entidad, sus activos y personal.

c. Política de Seguridad

La política de seguridad de la organización es el conjunto de leyes, normas y prácticas que regulan de qué manera una organización administra, protege y distribuye los recursos para lograr objetivos de seguridad específicos. Estas leyes, normas y prácticas deben identificar los criterios para conceder facultades a los individuos, y pueden especificar las condiciones bajo las cuales se permite a los individuos ejercer sus facultades. Para que tengan sentido, estas leyes, normas y prácticas deben proporcionar a las personas una capacidad razonable para determinar si sus acciones violan o cumplen con la política.

Una plantilla recomendada para la política de Seguridad de TI, es la siguiente:

[45] **Autenticidad** es la propiedad de ser genuino y verificable y comprobable; confianza en la validez de una transmisión, un mensaje, u originador de mensaje. La autenticidad puede no ser necesaria para evaluar la integridad a fin de cumplir un objetivo de auditoría.

[46] **Irrefutabilidad** es la garantía de que el remitente de la información reciba un comprobante de entrega y el destinatario reciba la prueba de la identidad del emisor, por lo que ninguno se puede negar posteriormente después de haber procesado la información. La Irrefutabilidad puede no ser necesaria para evaluar la integridad a fin de cumplir con un objetivo de auditoría.

Elementos de una Política de Seguridad de TI	Definición de seguridad de la información - objetivos y alcance (incluida la confidencialidad de los datos).
	Principios detallados de seguridad, normas y requerimientos de cumplimiento • El personal del Departamento de TI no debe tener funciones operativas o contables
	Definición de las funciones generales y específicas para todos los aspectos de seguridad de la información.
	Uso de los activos de información y acceso al correo electrónico, -Internet.
	Modo y método de acceso.
	Procedimientos de copia de seguridad.
	Procedimientos para tratar programas y software maliciosos.
	Elementos de educación y capacitación en la seguridad.
	Procesos para informar incidentes de seguridad sospechosos.
	Planes de continuidad del negocio.
	Métodos para comunicar al personal la política y los procedimientos adoptados para la seguridad de SI.

d. Organización de la Seguridad de TI

La organización de la seguridad de TI implica la implementación de la política de seguridad para la entidad. Éste podría ser el trabajo para una unidad o individuo, que trabaje con el área de TI para incorporar las herramientas apropiadas y aplicar los procesos correctos para implementar eficientemente la política de seguridad. Además, son los responsables de proporcionar la capacitación inicial actualizada al personal y abordar los incidentes de seguridad. Asimismo, hay una necesidad de garantizar que los datos de la organización a los que se accede o que se transfieren a organizaciones externas estén adecuadamente protegidos. El auditor deberá verificar si esta entidad es capaz de implementar los requerimientos de SI de conformidad con los documentados por la organización.

e. Gestión de Operaciones y Comunicaciones

Una organización debe realizar un seguimiento del proceso y los procedimientos que utiliza para sus operaciones de negocios. Esto Incluye el conjunto de procedimientos y procesos organizacionales que garantizan el procesamiento correcto de los datos de la organización. Incluye además, la documentación de los procedimientos para el manejo de los medios de comunicación y de datos, procedimientos de emergencia, registro de seguridad de la red y procedimientos de copia de seguridad.

f. Gestión de Activos

La gestión de activos, en sentido más amplio, se refiere a cualquier sistema mediante el cual todo lo que tiene valor para una entidad o grupo es monitoreado y preservado. La gestión de activos es un proceso sistemático de operación, mantenimiento, actualización y disposición de activos de manera rentable.

Para la Tecnología de la Información, la gestión de activos incluye mantener un inventario preciso de los equipos de TI, saber qué licencias corresponden a los equipos conexos, el mantenimiento y su protección (bloqueo, sala controlada, etc.). La gestión de activos de TI también incluye la gestión del software y la documentación de procesos valiosos para la entidad.

Para una entidad de gobierno, la gestión de activos de TI es muy importante en el entorno fiscal actual, porque las restricciones financieras pueden no permitirle reemplazar razonablemente los activos perdidos

o robados. Además, la organización puede estar en riesgo si no cuenta con un inventario completo de sus activos al momento de actualizar el software, para satisfacer las necesidades futuras del negocio.

g. Seguridad de los Recursos Humanos

Los empleados que manejan datos personales en una organización deben recibir capacitación adecuada sobre la concientización y actualizaciones periódicas, en un esfuerzo por proteger los datos que se les han confiado. Las funciones y responsabilidades apropiadas asignadas para cada descripción de funciones deben ser definidas y documentadas de conformidad con la política de seguridad de la organización. Los datos de la institución deben estar protegidos contra el acceso no autorizado, la divulgación, la modificación, la destrucción o la interferencia. La gestión de la seguridad de los recursos humanos y de los riesgos para la privacidad es necesaria en todas las fases de la relación laboral con la organización.

Las tres áreas de seguridad de Recursos Humanos son:

- **Previo al empleo:** Este tema incluye la definición de roles y responsabilidades del puesto de trabajo, la definición de un acceso adecuado a información sensible relacionada con la función y la determinación de la profundidad de los niveles de investigación de antecedentes de los candidatos - todo ello de conformidad con la política de seguridad de TI de la organización. Durante esta fase, también se deben establecer las condiciones del contrato.
- **Durante el empleo:** Los empleados con acceso a la información sensible en una organización deben recibir recordatorios periódicos de sus responsabilidades y capacitación actualizada sobre concientización de la seguridad para garantizar la comprensión de las amenazas actuales y las prácticas de seguridad correspondientes para mitigar esas amenazas.
- **Terminación o cambio de empleo:** Para evitar el acceso no autorizado a la información confidencial, éste debe ser revocado inmediatamente después de la terminación/separación de un empleado con acceso a dicha información. Esto también incluye la restitución de todos los activos de la organización que utilizó el empleado.

Debe existir un programa de concientización sobre la seguridad para recordar a todo el personal los posibles riesgos y exposiciones, y sus responsabilidades como encargados del resguardo de la información corporativa.

h. Seguridad Física y Ambiental

La seguridad física describe las medidas diseñadas para rechazar el acceso físico del personal no autorizado (incluidos atacantes o intrusos accidentales) a un edificio, instalaciones, recursos o información almacenada, y una guía sobre cómo diseñar estructuras para contrarrestar actos potencialmente hostiles. La seguridad física puede referirse a algo tan simple como una puerta cerrada o tan complejo como varios niveles de barreras, guardias de seguridad armados e instalación de cabinas de seguridad.

La seguridad física se refiere principalmente a la restricción del acceso físico a personas no autorizadas (comúnmente interpretado como intrusos) a las instalaciones controladas, si bien existen otras consideraciones y situaciones en las que las medidas de seguridad física son valiosas (por ejemplo, limitar el acceso dentro de una instalación y/o activos específicos y controles ambientales para reducir los incidentes físicos, como incendios e inundaciones).

La seguridad inevitablemente genera costos y, de hecho, nunca puede ser perfecta o completa; en otras palabras, la seguridad puede reducir, pero no eliminar por completo los riesgos. Dado que los controles son imperfectos, una fuerte seguridad física aplica el principio de defensa en profundidad, mediante la utilización de una combinación adecuada de controles complementarios y superpuestos. Por ejemplo, los controles de acceso físico a las instalaciones protegidas están generalmente destinados a:

- Disuadir a posibles intrusos (por ej. señales de advertencia y marcas perimetrales);
- Distinguir a las personas autorizadas de las no autorizadas (por ej. uso de tarjetas de pase/credenciales y claves);
- Retrasar, frustrar y evitar, en el mejor de los casos, intentos de intrusión (por ej. paredes fuertes, cerraduras y cajas fuertes);
- Detectar intrusiones y monitorear/registrar la presencia de intrusos (por ej. alarmas de intrusión y sistemas de circuito cerrado de televisión);
- Generar respuestas adecuadas para los incidentes (por ej. por medio de guardias de seguridad y policías).

i. Control de Acceso

El control de acceso se refiere al ejercicio del control sobre quién puede interactuar con un recurso. Con frecuencia, pero no siempre, involucra una autoridad, que lleva a cabo el control. El recurso puede ser un determinado edificio, conjunto de edificios, o un sistema informático. El control de acceso -ya sea físico o lógico- es, de hecho, un fenómeno cotidiano. Una cerradura de una puerta de automóvil es esencialmente una forma simple de control de acceso. Un PIN en un sistema de cajero automático de un banco es otro medio de control de acceso, así como los dispositivos biométricos. La posesión de un control de acceso es de vital importancia cuando las personas pretenden asegurar información importante, confidencial y sensible, y equipos.

En un entorno gubernamental, el control de acceso es importante, ya que muchas entidades gubernamentales procesan datos sensibles y las cuestiones de privacidad ponen un límite a quiénes pueden acceder a las distintas partes de la información. El control de acceso garantiza que sólo los usuarios que cuentan con credenciales de proceso tengan acceso a los datos sensibles.

j. Adquisición, Desarrollo y Mantenimiento de Sistemas de TI

El Ciclo de Vida de Desarrollo de Sistemas (SDLC), o el proceso de desarrollo de software en la ingeniería de sistemas, ingeniería de software y sistemas de TI, es un proceso de creación o alteración de los sistemas de TI y los modelos y metodologías que utilizan las personas para desarrollarlos. En la ingeniería de software, el concepto SDLC respalda muchos tipos de metodologías de desarrollo de software. Estas metodologías constituyen el marco para la planificación y el control de la creación de un sistema de TI o el proceso de desarrollo de software.

El mantenimiento de un Sistema de TI durante su ciclo de vida incluye modificaciones y actualizaciones como resultado de nuevos requerimientos, solución de errores y mejoras efectuadas en virtud de nuevas interfaces.

k. Gestión de Incidentes de Seguridad de TI

En el campo de la seguridad informática y las tecnologías de la información, la gestión de incidentes de seguridad de TI implica el control y la detección de eventos de seguridad en una computadora o red informática, y el aporte de respuestas adecuadas a esos eventos. La gestión de incidentes de seguridad de TI es una forma específica de gestión de incidentes.

l. Gestión de Continuidad del Negocio

El Plan de Continuidad del Negocio es el proceso que una organización utiliza para planificar y poner a prueba la recuperación de sus procesos de negocio después de una interrupción. También describe de qué manera una organización continuará funcionando en condiciones adversas que puedan surgir (por ejemplo, desastres naturales u otro tipo de desastres).

m. Cumplimiento

El auditor de TI debe revisar y evaluar el cumplimiento de todos los requerimientos internos y externos (legales, ambientales, de calidad de la información, fiduciarios y de seguridad).

II. RIESGOS PARA LA ENTIDAD AUDITADA

Las políticas de seguridad de TI, los procedimientos y su aplicación permiten a una organización proteger su infraestructura tecnológica de usuarios no autorizados. La política de seguridad de TI de una organización establece los requerimientos esenciales para la organización y sus empleados, que se deben cumplir a fin de salvaguardar los activos clave. También proporciona capacitación al personal sobre temas de seguridad y garantiza que éste cumpla con los procedimientos establecidos para el acceso de datos y el control. Además, la política de seguridad de TI se refiere a las leyes y demás reglamentaciones que la organización está obligada a cumplir. Las organizaciones enfrentan muchos obstáculos en relación con la implementación de un sistema de seguridad de la información eficaz. Sin una gobernanza eficaz para hacer frente a estos obstáculos, la seguridad de TI tendrá un mayor riesgo de incumplimiento de los objetivos de la organización.

Toda organización enfrenta sus propios desafíos ya que sus cuestiones individuales ambientales, políticas, geográficas, económicas y sociales difieren. Cualquiera de estas cuestiones puede presentar obstáculos en cuanto al suministro de una gobernanza eficaz de TI y es responsabilidad del auditor de TI señalar los riesgos a la administración.

Los siguientes son los riesgos significativos identificados en la mayoría de las organizaciones:

- Divulgación no autorizada de la información.
- Modificación no autorizada o destrucción de la información.
- Vulnerabilidad de ataques a SI.
- Destrucción de la infraestructura de SI.
- Alteración del acceso o uso de información o de un sistema de información.
- Interrupción del proceso del sistema de información.
- Información o datos robados.

Al observar las exposiciones al riesgo que poseen las organizaciones auditadas, se debe prestar especial atención a las siguientes áreas:

- **Estrategias** de seguridad de la información que no se corresponden con los requerimientos del negocio o de TI.
- **Políticas** no aplicadas uniformemente y de ejecución dispar.
- **Incumplimiento** de los requerimientos internos y externos.
- Seguridad de la información no incluida en los procesos de desarrollo y mantenimiento de la cartera de **proyectos.**
- Diseño de la **arquitectura** que resulta en soluciones de seguridad de información ineficaces, ineficientes o equivocadas.
- Medidas de seguridad **física** y de gestión de activos inadecuadas.
- **Configuración** inadecuada de la aplicación del sistema de hardware.
- **Organización** ineficiente de los procesos de seguridad de la información y estructura de responsabilidad de SI no definida o confusa.
- Soluciones inapropiadas en cuanto a **recursos humanos.**
- Uso ineficaz de los **recursos financieros** asignados a la seguridad de la información, estructura de **valor** (costo-beneficio) de la seguridad de la información no alineada a las necesidades u objetivos del negocio.
- Seguridad de la información no **monitoreada** o monitoreada ineficazmente.

El auditor debe comenzar con la evaluación de la conveniencia de los métodos de evaluación de riesgos y tomar en consideración las cuestiones de auditoría relacionadas con la implementación de la seguridad de la información. Una Matriz de Auditoría asistirá al auditor a plantear cuestiones de auditoría, criterios de evaluación, documentos requeridos y análisis técnicos, que pueden ser utilizados. En conclusión, el auditor puede desarrollar un programa detallado de auditoría de acuerdo con las necesidades y el desarrollo durante el trabajo de campo de la auditoría.

Al llevar a cabo una auditoría de seguridad de la información, el auditor debe abordar las cuestiones relacionadas con las doce áreas (conforme a las indicadas anteriormente) de la seguridad de la información.[47]

Matriz de Auditoría

La matriz de auditoría para esta sección se incluye en el Anexo VII.

Referencias/ Lecturas adicionales

1. ISSAI 5310 Metodología *de Revisión de la Seguridad de los Sistemas de Información*.
2. Serie ISO 27000 *Sistema de Gestión de Seguridad de la Información*.
3. ISO 27005 *gestión de riesgos de seguridad de la información*.
4. ISACA *Marco de Riesgos de TI*.
5. COBIT 4.1 Marco, 2007, Instituto de Gobernanza de TI.
6. COBIT 5 Marco, 2012, Isaca.
7. ISACA ITAF – *Marco de Prácticas Profesionales para el aseguramiento de TI*. EE.UU. 2008.
8. ISACA, *Auditoría de Seguridad de la Información/Programa de Aseguramiento*, 2010.
9. ISACA, *Auditoría de Gestión de Riesgos de TI/Programa de Aseguramiento*, 2012.
10. COSO *Marco de Gestión de Riesgos Empresariales*.

[47] Series ISO 27000 *Sistema de Gestión de Seguridad de la Información.*

CAPÍTULO 8
CONTROLES DE APLICACIÓN

I. QUÉ SON LOS CONTROLES DE APLICACIÓN

Una aplicación es un software específico utilizado para llevar a cabo y apoyar un proceso de negocio específico. Puede incluir tanto los procedimientos manuales como informatizados para la generación de registros, procesamiento de datos, mantenimiento de registros y preparación de informes. Es probable que cada entidad tenga una serie de aplicaciones en ejecución, que varían en tamaño desde un sistema para toda la organización al que acceden todos los empleados, hasta una aplicación de clientes pequeños a la cual accede un empleado. El software de aplicación podría ser un sistema de nóminas, un sistema de facturación, un sistema de inventario, o, posiblemente, un sistema integrado (ERP) de planificación de recursos de la organización.

Una revisión de los controles de aplicación permite al auditor proporcionar a la administración una evaluación independiente sobre la eficacia y la efectividad del diseño y la operación de los controles internos, y los procedimientos operativos relacionados con la automatización del proceso del negocio, e identificar problemas relacionados con las aplicaciones que requieren atención.

Dado que los controles de aplicación están estrechamente relacionados con los registros individuales, se desprende que una prueba de dichos controles proporcionará al auditor garantías sobre la exactitud de una funcionalidad en particular. Por ejemplo, una prueba de los controles de una aplicación de nóminas garantizará las cifras de la nómina de la organización. La prueba de los controles generales de TI de la organización (por ejemplo, procedimientos de control de cambios) no siempre proporciona un nivel similar de seguridad para el mismo saldo contable.

Dependiendo de los objetivos específicos de la auditoría, la revisión de la aplicación puede tener diferentes enfoques. Por lo tanto, la forma en que se deben probar los controles puede variar de una auditoría a otra. Por ejemplo, la revisión de la aplicación podría estar centrada en el cumplimiento de leyes y normas, por lo que el punto principal es verificar si los controles de aplicación ayudan adecuadamente al abordaje de esas cuestiones. Desde otro punto de vista, la revisión de la aplicación podría ser parte de una auditoría de desempeño, por lo que es importante verificar de qué manera las reglas del negocio se trasladan a la aplicación. Durante un análisis de seguridad de la información, el enfoque podría estar en los controles de aplicación responsables de garantizar la confidencialidad, integridad y disponibilidad de los datos.

Los pasos que se deben seguir para llevar a cabo una revisión del control de aplicación podrían incluir un proceso cíclico de actividades. A pesar de que podría ser interesante comenzar desde la perspectiva de la organización, es importante mencionar que no existe un ordenamiento estricto entre estos pasos. Algunos de ellos se presentan a continuación y se describen brevemente en las siguientes secciones.

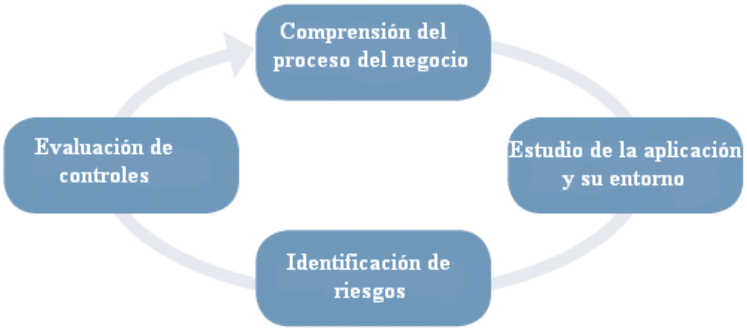


Figura 8.1 Ciclo de Revisión de la Aplicación.

- **Comprensión del proceso del negocio:** Antes de examinar las cuestiones técnicas relativas a la aplicación, podría ser útil contar con una visión general de los procesos del negocio automatizados por la aplicación, sus reglas, flujos, actores, roles y requerimientos de cumplimiento conexos. La comprensión del negocio subyacente es un paso importante para poder verificar la coherencia de los controles de aplicación y de los procesos automatizados. El alcance de este paso variará de acuerdo con el objetivo de la auditoría. Esto generalmente se realiza a través del análisis de los procedimientos de operación/trabajo, el diagrama de flujo del proceso de la organización u otro material de referencia. El equipo de auditoría también deberá conocer y entrevistar a los gerentes de las organizaciones, los ejecutivos de TI y usuarios clave de la aplicación.

- **Estudio de la aplicación y su entorno:** Estudio del diseño y el desempeño de la aplicación, ya sea mediante la revisión de la documentación (diagramas de la organización, diagramas de flujo de datos y manuales de usuario) o mediante entrevistas al personal clave. Estudio de las funciones clave del software en operación, mediante la observación e interacción con el personal operativo durante el trabajo. A través de discusiones, realizar inspecciones del proceso del negocio y de la aplicación, desde el ingreso a las fuentes hasta la salida y conciliación para verificar de qué manera fluyen los procesos, y observar las actividades manuales conexas, que podrían actuar como controles complementarios. Discutir con los administradores, operadores y desarrolladores, y obtener documentación sobre la infraestructura técnica: el sistema operativo, entorno de red, sistema de gestión de base de datos, interfaces con otras aplicaciones originadas interna o externamente, procesamiento de registros *on line*, ingresados por lotes, o en tiempo real. Esto muestra cómo la infraestructura tecnológica impacta en la aplicación.

- **Identificación de riesgos:** Principalmente, para identificar los riesgos asociados con la actividad/función de la organización que cubre la aplicación (¿qué puede salir mal?) y para verificar de qué manera estos riesgos son manejados por el software (¿qué lo controla?). A veces, una evaluación de riesgo del proceso del negocio podría estar disponible (podría haber sido realizada por una auditoría previa, auditoría interna o por la gerencia) y el auditor podría beneficiarse de su uso después de evaluar la confiabilidad de la evaluación del riesgo existente.

- **Evaluación de controles:** Luego de tomar conocimiento del entorno (de la organización y técnico) en el que la aplicación opera, el auditor tendrá más confianza para evaluar los controles utilizados a fin de abordar los riesgos existentes. El auditor debe actuar con criterio al evaluar los controles de aplicación y debe ser cuidadoso al proponer recomendaciones para mejoras. Por ejemplo: el exceso de detalles sobre los registros puede incrementar el costo de los gastos generales de la entidad, sin mejorar su trazabilidad a niveles deseables. La evaluación involucra

el análisis de los distintos tipos de controles de aplicación que se describen en la siguiente sección.

I.1. Elementos Clave de los Controles de Aplicación

Los controles de aplicación son controles específicos y únicos para cada aplicación informática. Cuando los procesos del negocio están automatizados en una aplicación informática, las normas de la organización también se integran en la aplicación en forma de controles. Estos se aplican a segmentos de la aplicación y están relacionados con los registros y los datos vigentes.

Mientras que los controles generales de TI en una entidad marcan la pauta para el entorno general de control de los sistemas de información, los controles de aplicación están integrados a aplicaciones específicas para garantizar y proteger la exactitud, integridad, confiabilidad y confidencialidad de la información. Estos garantizan que el inicio de las operaciones esté debidamente autorizado, los datos de entrada válidos sean procesados, registrados en su totalidad y presentados con precisión.

Ilustración

En una aplicación de pago en línea (ver la captura de pantalla de ingreso de pago en línea que se presenta a continuación), una condición de entrada podría ser que la fecha de vencimiento de la tarjeta de crédito sea posterior a la fecha de la transacción. Otra podría ser que el número de la tarjeta sea válido y se corresponda tanto con el nombre del titular de la tarjeta como con el valor de verificación (número de CVV), según la base de datos del emisor de la tarjeta de crédito. Otra sería que se encripten los detalles cuando se transmiten a través de la red. Los controles integrados a la aplicación garantizarán que estas condiciones sean inviolables, lo cual validará las transacciones.

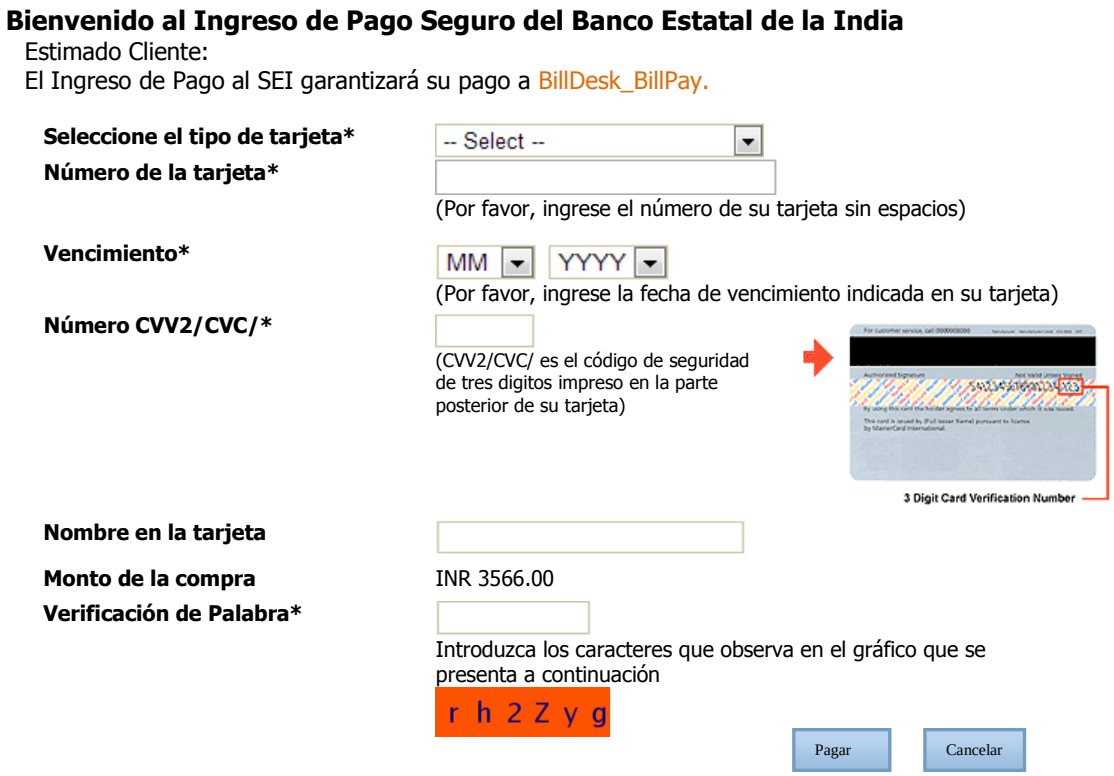


Figura 8.2: Ejemplo de control de Aplicación.

Los controles de aplicación también incluyen procedimientos manuales que operan en proximidad a la aplicación. Estos controles no sólo se incorporan a aplicaciones específicas, sino también a todos los procesos del negocio más próximos. Por ejemplo, un empleado a cargo del ingreso de datos puede requerir que el formulario de ingreso de datos sea firmado (aprobado) antes de ser ingresado al sistema.

La combinación del control manual y automatizado elegido es, a menudo, el resultado de las consideraciones de costos y control en la etapa de diseño de una aplicación.

Una aplicación puede dividirse en los siguientes segmentos: **ingreso de datos** (originación y entrada de datos), **procesamiento** de registros, **salida** de datos (distribución de resultados) y **seguridad** (registro, comunicaciones, almacenamiento). Los controles en una aplicación se incorporan a cada segmento de la aplicación junto con los controles que restringen el acceso a la aplicación y archivos maestros.

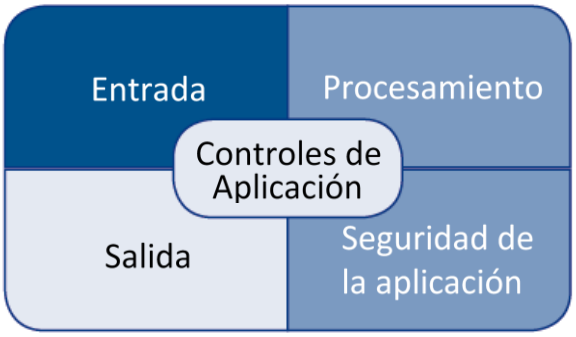


Figura 8.3 "Elementos clave" de los controles de aplicación.

A pesar de que no es viable proporcionar los pasos de prueba y la lista de verificación detallados para cada posible modificación de una aplicación, un auditor de TI debe estar en conocimiento de los conceptos de control comunes a casi todas las aplicaciones. Esto puede ser utilizado para generar reflexiones e ideas con respecto a medidas más específicas de prueba de auditoría para la aplicación que está siendo auditada.

Algunos de los elementos de control más comunes se resumen en la siguiente tabla:

Controles de Entrada	▪ Ingresos de datos/verificación de campos (ejemplo: validación de los números de las tarjetas de crédito ingresados). ▪ Gestión de documentos fuente (ejemplo: procedimientos de preparación y conservación). ▪ Mecanismos de gestión de errores (mensajes de error, archivos transitorios). ▪ Reglas de autorización de ingreso de datos (ejemplo: división de tareas)
Controles de Procesamiento	▪ Mapeos de reglas del negocio. ▪ Verificaciones de integridad, informe de condiciones de no conciliación. ▪ Cálculos automatizados. ▪ Conciliaciones de datos de ingreso
Controles de Salida	▪ Validaciones de integridad y exactitud, conciliación. ▪ Revisión y seguimiento de salida. ▪ Revisión y seguimiento de informes de excepciones generados por la aplicación. ▪ Procedimientos de etiquetado, gestión, retención y distribución de datos de salida
Controles de Seguridad de la Aplicación	▪ Mecanismo de trazabilidad (pistas de auditoría, revisión de registro, uso de identificadores únicos). ▪ Control de acceso lógico a funcionalidades y datos en las aplicaciones. ▪ Protección de datos almacenados.

Figura 8.4: Ejemplos de controles de aplicación.

a. Controles de Entrada

Los objetivos de los controles de entrada pretenden validar y autenticar los actos de preparación de datos de origen, la autorización y el ingreso de manera que la aplicación acepte datos precisos, confiables y completos de manera oportuna.

Una parte significativa de estas medidas se diseña en la etapa de desarrollo de una aplicación, luego de establecidas las reglas del negocio en la definición de los requerimientos. Si bien el ingreso de datos puede ser manual o mediante la interfaz del sistema, se pueden minimizar los errores y las omisiones a través de un buen diseño de la interfaz de entrada, una división apropiada de funciones con respecto al origen y aprobación de los documentos de entrada, y la implementación de controles de autenticidad, precisión e integridad pertinentes (con menú de opciones o mensajes interactivos).

Elementos de control de entrada	Descripción
Controles de entrada de datos (validez, integridad, y verificación de duplicaciones)	Controles de validez automatizados de los datos ingresados (Ejemplo: Fecha de viaje se encuentra fuera del período de reserva abierta); controles de integridad para garantizar que toda la información clave de la transacción haya sido ingresada (Ejemplo: fecha de viaje, nombres de pasajeros, números de identificación son campos obligatorios); los controles duplicados comparan transacciones nuevas con transacciones contabilizadas anteriormente (Ejemplo: verificación de facturas duplicadas).
Gestión de documentos fuente	Documentación de los procedimientos de preparación de documentos fuente, registro de documentos fuente, numeración de documentos fuente (trazabilidad) y procedimientos de conservación de documentos.
Procedimiento de gestión de errores	Procedimiento para tratar un ingreso rechazado. (Ejemplo: mensajes de error, medidas de corrección posteriores, indicaciones que permiten el reingreso, uso de datos transitorios).
Autorización de entrada	Procedimientos manuales/autorización a nivel de supervisión de los datos en el formulario de ingreso de datos (ejemplo: autorización de los detalles de la declaración de aduana por parte del supervisor antes de ser ingresada por el empleado a cargo del ingreso de datos, para procesamiento en las aplicaciones aduaneras.

b. Controles de Procesamiento

El objetivo de las medidas de control del procesamiento es proteger la integridad, la validez y confiabilidad de los datos, y resguardar los datos contra errores durante todo el ciclo de procesamiento de registros, desde el momento en que se reciben los datos del subsistema de entrada hasta el momento en que los datos se envían al subsistema de la base de datos, comunicación o salida. También es garantizar que los datos de entrada válidos se procesen sólo una vez y que la detección de registros erróneos no interrumpa el procesamiento de registros válidos. Además, buscan mejorar la confiabilidad de los programas de aplicación que ejecutan las instrucciones para satisfacer los requerimientos específicos del usuario.

Los procedimientos de control incluyen el establecimiento y la implementación de mecanismos para autorizar el inicio del procesamiento de registros y para obligar a que se utilicen solo aplicaciones y herramientas autorizadas y apropiadas. Éstos verifican con regularidad que el procesamiento se realice con precisión y en forma completa, con controles automatizados, según corresponda.

Los tipos de control pueden incluir la verificación de errores en la secuencia y errores de duplicación, cómputos de registros, verificación de la integridad referencial, control y cálculos de totales, verificación de rango y del desbordamiento de Búfer.

En los sistemas en tiempo real, algunos de los controles de compensación son las verificaciones minuciosas, dosificación retrospectiva, excepción y presentación de informes de cuentas transitorias.

c. Controles de Salida

Los objetivos de los controles de salida son medidas incorporadas a las aplicaciones para garantizar que la salida de datos sea completa, exacta y distribuida correctamente. También tratan de proteger los datos procesados por una aplicación contra una modificación y distribución no autorizada.

Los procesos de control incluyen la definición adecuada de las salidas, los informes deseados en la etapa de desarrollo y diseño del sistema, la documentación apropiada de la lógica de obtención del informe, controles que limitan el acceso a los datos procesados, examen de salida, conciliación y revisión.

d. Controles de Seguridad de la Aplicación

La seguridad de la aplicación está relacionada con el mantenimiento de la confidencialidad, integridad y disponibilidad de la información a nivel de la aplicación. A los fines de una auditoría, es importante comprender las interfaces, es decir, las diferentes fuentes de entrada y de salida de datos de la aplicación y también la forma en la que se almacenan los datos.

A la mayoría de las aplicaciones se accede a través de la identificación del usuario y contraseñas. Sin embargo, otras formas de acceso, tales como mecanismos únicos de inicio de sesión, son cada vez más populares, dada la magnitud de las aplicaciones utilizadas en un entorno corporativo. Por lo tanto, el diseño de la aplicación para el ingreso de usuarios debe ser considerado con anterioridad. Un auditor puede necesitar revisar las políticas y los procedimientos de la entidad para el otorgamiento y revocación de acceso de los usuarios con el fin de comprender hasta qué punto las reglas de acceso se integran en cada nivel de la aplicación y de garantizar que la aplicación dispone de controles respecto del otorgamiento y revocación de acceso.

Para poder entender los procedimientos de control de seguridad de la aplicación, el auditor debe comprender a los actores, los roles y las responsabilidades involucradas en la aplicación, tales como los administradores, los usuarios avanzados, los usuarios regulares, etc. El diseño del módulo de control de acceso lógico puede ser de diversos tipos. La mayoría de los aplicativos pueden utilizar una combinación de identificación del usuario y contraseña antes de permitir el acceso. El acceso puede ser controlado en cada módulo, opción del menú, cada pantalla o a través de objetos y roles. El auditor de TI debe revisar el diseño del módulo de control de acceso teniendo en cuenta la criticidad de las funciones/acciones disponibles. De hecho, es necesario poder identificar los mecanismos utilizados para garantizar la generación y la trazabilidad de los registros, así como para proteger los datos almacenados por la aplicación.

A continuación, se presenta una lista de ejemplos de temas auditables en relación a los controles de seguridad de la aplicación:

- Pistas de auditoría: el registro de transacciones, el uso de identificación única de usuario, monitoreo e información de registros, preferentemente el registro de auditoría debe indicar qué registros o

campos fueron modificados, cuándo se modificaron, qué se modificó, cuál fue su reemplazo y quién hizo la modificación.

- Administración de las cuentas, los permisos y contraseñas de los usuarios: el uso de cuentas de invitado, prueba y genéricas, uso de cuentas de administrador y cuentas privilegiadas, y controles compensatorios, procedimientos para el otorgamiento y revocación de acceso, procedimientos de terminación de las tareas y la eliminación de acceso; la adopción del principio de mínimo privilegio; acceso del equipo de desarrollo/TI a bases de datos de producción; procedimientos formales para la aprobación y el otorgamiento de acceso; uso de contraseñas seguras; imposición de cambios periódicos; contraseñas encriptadas, etc.
- Archivo maestro y protección de datos permanentes (semi-permanentes): controles para garantizar que las modificaciones de los datos permanentes estén autorizadas; que los usuarios se responsabilicen por los cambios realizados, que los datos permanentes estén actualizados y sean precisos, y que se mantenga la integridad de los archivos maestros. Ejemplos de datos permanentes: detalles de los proveedores y clientes (nombre, dirección, teléfono, número de cuenta), tasas de inflación, datos de administración del sistema, tales como archivos de contraseñas y permisos de control de acceso, etc.
- Adopción de división de funciones y funciones en conflicto: diferentes roles de usuario, derechos de acceso disponibles para cada perfil de usuario, normas para la división de funciones.

II. RIESGOS PARA LA ENTIDAD AUDITADA

Las consecuencias de las fallas en el control de las aplicaciones, por lo general, dependerán de la naturaleza de la aplicación del negocio. Los riesgos pueden variar desde la insatisfacción del usuario hasta verdaderos desastres y pérdida de vidas. Por ejemplo, la organización puede perder una cuota del mercado si un servicio no está disponible; la organización puede perder dinero si los sistemas de venta *on line* pierden las órdenes de compra; la confianza de los ciudadanos en los servicios públicos puede disminuir; la falta de cumplimiento con las normas legales puede llevar a demandas judiciales; la electricidad podría no llegar a los hogares; las cuentas bancarias pueden ser susceptibles al fraude, etc.

Específicamente, los riesgos significativos que posiblemente ocurran en ausencia de controles de entrada adecuados son los riesgos de procesamiento erróneo o fraudulento, y la aplicación no podrá alcanzar los objetivos del negocio. Los datos procesados por la aplicación pueden ser incompatibles y los programas aportarán información errónea. Además, incluso en presencia de tales controles, existe la posibilidad de anularlos en situaciones muy específicas. En este caso, debe haber controles compensatorios tales como registros y reglas de autorización, de lo contrario, el privilegio de anulación podría ser mal utilizado y dar lugar al ingreso de datos incompatibles en la aplicación.

Los procedimientos para la gestión de documentos fuente y la autorización de entrada de datos son también un tipo importante de control de entrada. En ausencia de una gestión adecuada de los documentos fuente, no sería posible rastrear la fuente de la información que se introdujo en el sistema, no se lograría el cumplimiento legal, se podrían violar las políticas de conservación y se ingresarían datos poco confiables en la aplicación. Por otra parte, en ausencia de controles de autorización, los datos no autorizados pueden dar lugar a errores o fraude.

En general, las fallas en los controles de procesamiento pueden dar lugar a errores de procesamiento y al incumplimiento de los objetivos del negocio. Éstas surgen debido al diseño incorrecto de las reglas del negocio, a las pruebas inadecuadas de código de programa o al control inadecuado de las diferentes versiones de los programas para restaurar la integridad del procesamiento después de producido un problema o una interrupción inesperada. En ausencia de prácticas de control de procesamiento

necesarias, podría haber recurrencia de registros erróneos que afecten los objetivos y el valor de la organización.

Con los sistemas de procesamiento en tiempo real, algunas de las medidas de control como la conciliación de totales de lotes de entrada y salida para la determinación de la integridad de los datos de entrada, o la conservación de algunos documentos del origen de los datos para las pistas de auditoría, no estarán disponibles. Sin embargo, los sistemas en tiempo real incorporan otros controles de compensación dentro de la aplicación, incluida la integridad de datos interactivos, indicaciones de validación, registro de intentos de acceso, etc.

La falta de un control de salida adecuado conduce al riesgo de modificación/eliminación no autorizada de datos, creación de informes de gestión erróneamente personalizados y violación de la confidencialidad de los datos. Además, los resultados de una generación errónea de salida dependerán en gran medida de la forma en que la información sea utilizada por la organización.

En el contexto de seguridad de la aplicación, la insuficiencia de mecanismos de registro puede ocasionar que el rastreo de la mala conducta hasta los autores específicos, resulte imposible. Asimismo, el conocimiento por parte de los usuarios de la existencia de procedimientos de revisión de los registros y mecanismos de información puede por sí mismo mitigar el riesgo del uso indebido de los sistemas de información. Los errores en los datos permanentes tienen un efecto trascendental en la aplicación, ya que estos datos pueden ser usados por gran parte de las funcionalidades de la aplicación.

De hecho, los riesgos de no tratar adecuadamente la seguridad de la información exceden lo antedicho. Pueden dar lugar a consecuencias con diferentes grados de severidad que incluyen: pérdida de ingresos, interrupción del servicio, pérdida de credibilidad, interrupción del negocio, uso indebido de la información, consecuencias legales, causas judiciales y abuso de la propiedad intelectual, etcétera. Estos riesgos y los controles de mitigación se cubren más detalladamente en el capítulo sobre Seguridad de la Información.

Matriz de Auditoría

La matriz de auditoría para esta sección se describe en el Anexo VIII.

Referencias:

1. ISACA Directriz sobre Auditoría de TI y Aseguramiento G38, Controles de Acceso.
2. *Manual de Auditoría de TI*, Volumen I, EFS de la India.
3. *Auditoría de IT: Utilización de controles para proteger los Activos de la Información*, segunda edición por Chris Davis, Mike Schiller y Kevin Wheeler McGraw-Hill/Osborne.
4. Singleton, Tommie W."Aplicaciones de Auditoría – Parte 2". Publicación ISACA, Vol. IV. 2012.

CAPÍTULO 9
TEMAS ADICIONALES DE INTERÉS

Esta sección presenta una visión general de otros temas relacionados con la auditoría de TI, con los que el auditor puede encontrarse en el transcurso de sus auditorías. Existen varias áreas emergentes de TI que podrían convertirse en temas auditables. Por lo tanto, el auditor debe tener conocimiento de la existencia de estas áreas y ser capaz de progresar en una auditoría sobre este tipo de temas.

A pesar de que estas áreas podrían tener algunas diferencias técnicas o aspectos específicos, pueden ser auditadas utilizando los mismos enfoques y técnicas que se describen en esta guía. Posiblemente, podrían requerir algunas preguntas o temas adicionales de auditoría que el auditor podría desarrollar por sí mismo al tratarlos, dependiendo de los objetivos de la auditoría.

1. Sitios y Portales Web

Los sitios Web son sistemas de información que se encuentran en Internet o incluso en las Intranets, que ofrecen servicios y contenido, tales como textos, imágenes, video, audio, etcétera. Un portal web organiza la información de diferentes fuentes de una manera uniforme, al tiempo que proporciona un aspecto coherente. Por lo general, los portales web ofrecen servicios, tales como motores de búsqueda, noticias, información, acceso a los sistemas, bases de datos y entretenimientos. Ejemplos de portales web públicos: AOL, Google, Yahoo, India.com.

Áreas de Auditoría

- Experiencia del usuario.
- Seguridad, privacidad.
- Tiempo de respuesta.
- Asuntos relacionados con la subcontratación.

Referencias/Lecturas adicionales:

1. http://en.wikipedia.org/wiki/Web_site
2. http://en.wikipedia.org/wiki/Web_portal
3. Kenyon, Geoff. *Lista de Verificación de Auditoría del Sitio Técnico*. 2011, http://www.seomoz.org/blog/how-to-do-a-site-audit
4. Jones, Harrison. *Cómo: Guía –para la realización de Auditorías de Sitios Web*. 2011. http://www.techipedia.com/2011/website-audit-guide/

2. Informática Móvil

Se observa un esfuerzo cada vez mayor por prestar servicios al público a través de todo tipo de canales de TI. Esto está relacionado con el uso de tecnologías de comunicación inalámbrica para proporcionar aplicaciones e información. Actualmente, se ofrece una gran cantidad de aplicaciones en un entorno móvil. Los teléfonos celulares, las tabletas, las redes Wi-Fi, TV y una amplia gama de nuevos dispositivos y herramientas electrónicas proporcionan información. La informática móvil puede ser considerada como un punto de acceso de TI (PC, laptop, etc.), pero posee algunas áreas de auditoría especiales que pueden ser importantes.

Áreas de Auditoría

- Seguridad inalámbrica, privacidad, encriptado.
- Experiencia del usuario.
- Políticas específicas respecto de la informática móvil en la organización.
- Riesgos en la utilización de dispositivos personales para acceder a servicios y datos corporativos.
- Riesgos de acceso no autorizado a los datos existentes en el dispositivo.
- Mayor riesgo de daño o robo de dispositivos corporativos.

Referencias /Lecturas adicionales:

1. Isaca Directriz de Auditoría de TI y Aseguramiento G 27 – Informática Móvil. http://www.isaca.org/Knowledge-Center/Standards
2. ISACA Programa de Aseguramiento/Auditoría de Seguridad de Informática Móvil. http://www.isaca.org/auditprograms

3. Auditoría Forense (o Informática Forense)

La auditoría forense es un tipo de auditoría que se lleva a cabo para examinar los medios digitales a fin de obtener evidencias respecto de una investigación o disputa. La preservación de la evidencia es imprescindible durante un análisis de informática forense. Esta auditoría comprende el enfoque, las herramientas y las técnicas para examinar la información digital a los fines de la identificación, preservación, recuperación, análisis, y presentación de hechos y opiniones sobre la información almacenada.

Está mayormente asociada a las investigaciones criminales a fin de ayudar a los organismos de seguridad y a proporcionar evidencias contundentes en un juicio. La informática forense ha sido aplicada en una serie de áreas que incluyen, pero no se limitan a, fraude, espionaje, asesinato, chantaje, abusos informáticos, abusos tecnológicos, difamación, correos electrónicos maliciosos, fuga de información, robo de propiedad intelectual, pornografía, *spam*, hackers y transferencia ilegal de fondos.[48]

[48] Directriz de ISACA sobre Auditoría de TI y Aseguramiento G38 Informática Forense.

Áreas de Auditoría

La disciplina involucra técnicas y principios similares de recuperación de datos, pero con directrices adicionales y prácticas diseñadas para reforzar el sustento legal de las evidencias de auditoría.

- Retención de evidencias para análisis (datos, acceso, registro).
- Captura y conservación de los datos que se hallen más próximos al incumplimiento.
- Normas de recolección de datos para la posible aplicación de la ley.
- Proceso de captura de datos mínimamente invasivo, sin interrupción de las operaciones de la organización.
- Identificación de atacantes, si es posible.

Referencias / Lecturas adicionales:

1. ISACA Directriz sobre Aseguramiento y Auditoría de TI G27 - Informática Móvil. http://www.isaca.org/Knowledge-Center/Standards
2. *Examen forense de evidencia digital: Guía para aplicación de la ley*. http://www.ncjrs.gov/pdffiles1/nij/199408.pdf
3. *Investigación electrónica de la escena del crimen: Guía de buenas prácticas para evidencias electrónicas basadas en la informática*. http://www.met.police.uk/pceu/documents/ACPOguidelinescomputerevidence.pdf
4. Informática forense. Wikipedia. http://en.wikipedia.org/wiki/Computer_forensics

4. Administración Electrónica, Gobernanza Electrónica y Gobernanza Móvil (Egov, E-Gov y M-Gov)

El advenimiento de las tecnologías de la información ha cambiado de manera generalizada la forma en la que los gobiernos proporcionan servicios a sus ciudadanos. A medida que la tecnología se extiende entre la población, los gobiernos toman en consideración los nuevos enfoques para proporcionar información y aplicaciones en beneficio del público. La administración electrónica, la gobernanza electrónica (conocidas como eGov y e-gov) y la gobernanza móvil son algunas áreas que se ocupan de este tema. Estos conceptos están relacionados, aunque no son sinónimos perfectos.

Áreas de Auditoría

A los fines de la auditoría, el auditor debe tener en cuenta que generalmente se requiere que los gobiernos presten servicios de manera económica, eficiente y eficaz. Muy frecuentemente, la prestación de los servicios de manera electrónica permite un mayor alcance a un costo razonable.

Desde el punto de vista de auditoría, la auditoría de los sistemas de información o procesos de negocios contemplados en una estrategia de e-gov o m-gov no difiere de una auditoría tradicional de TI. El auditor debe considerar algunos mecanismos adicionales de política y aplicación (por ejemplo, una

política organizacional sobre informática móvil, software de encriptación, lo cual limita el uso de los teléfonos inteligentes personales, etc.).

Referencias / Lecturas adicionales:

1. Gobernanza electrónica. Wikipedia
   http://en.wikipedia.org/wiki/E-Governance
2. Gobernanza móvil. Ministerio de Comunicaciones y Tecnología de la Información. Gobierno de la India.
   http://mgov.gov.in/msdpbasic.jsp
3. Encuesta sobre Gobernanza Electrónica de las Naciones Unidas.
   http://www2.unpan.org/egovkb/global_reports/10report.htm

5. Comercio Electrónico (e-commerce)

El comercio electrónico (e-commerce) se refiere a cualquier tipo de negocio o transacción comercial efectuadas a través de las redes. Incluye, pero no se limita, a la venta y comercialización de información, productos primarios y servicios.

Si bien el comercio electrónico es definido comúnmente como la comercialización de bienes y servicios a través de Internet, implica una actividad económica más amplia. El comercio electrónico consiste en el comercio de empresa a consumidor y de empresa a empresa, y en las transacciones organizacionales internas que apoyan estas actividades.[49]

Una amplia gama de tecnologías y procesos de negocios están actualmente relacionados con el comercio electrónico, por ejemplo: portales, transferencia electrónica de fondos, banca en línea, gestión de la cadena de suministro, marketing, compras en línea, comercio móvil, gestión de inventario, etcétera.

Áreas de Auditoría

Hay varios aspectos que son decisivos para un sistema de comercio electrónico. Algunos de ellos deberían tenerse en cuenta a la hora de decidir los objetivos de la auditoría, por ejemplo:

- Disponibilidad,
- Seguridad de las transacciones,
- Escalabilidad de la solución,
- Experiencia del usuario y, lo más importante,
- El proceso de negocio llevado a cabo por la estrategia de comercio electrónico.

Los procesos del negocio llevados a cabo a través de estrategias de comercio electrónico requieren de mecanismos de seguridad sólidos para proporcionar, principalmente, integridad, confidencialidad, irrefutabilidad y autenticidad de las transacciones en línea. Por lo tanto, un conjunto de procesos y tecnologías llamado Infraestructura de Clave Pública (PKI) se pone en práctica.

La PKI comprende un conjunto de algoritmos criptográficos estándar y técnicas que permiten a los usuarios comunicarse de forma segura a través de redes públicas no seguras para garantizar que la

[49] E-Commerce. Enciclopedia Británica. http://www.britannica.com/EBchecked/topic/183748/e-commerce.

información sea transmitida al destinatario deseado. Sin esta tecnología, el comercio electrónico como lo conocemos sería imposible.[50]

Con el fin de auditar los sistemas de comercio electrónico, con mucha frecuencia, el auditor debe conocer los principales componentes de una infraestructura de PKI:

- claves públicas y privadas,
- mecanismos de firma digital,
- certificados digitales,
- autoridades de certificación y registro,
- algoritmos criptográficos.

Si bien el auditor no necesita ser un experto en estas áreas, debe tener conocimiento de las normas ampliamente aceptadas y saber si la organización las ha adoptado.

Referencias/Lecturas adicionales:

1. Comercio Electrónico. Enciclopedia Británica. http://www.britannica.com/EBchecked/topic/183748/e-commerce
2. Comercio Electrónico y Auditoría de la Infraestructura de Clave Pública /Programa de Aseguramiento. Isaca. http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/E-commerce-and-Public-Key-Infrastructure-PKI-Audit-Assurance-Program.aspx
3. Pistas de Auditoría en un Entorno de Comercio Electrónico. http://www.isaca.org/Journal/Past-Issues/2002/Volume-5/Pages/Audit-Trails-in-an-E-commerce-Environment.aspx

[50] E-Commerce y Auditoría de Infraestructura Pública Clave/Programa de Aseguramiento. Isaca. 2012.

ANEXO I
LISTA DE VERIFICACIÓN GENÉRICA PARA LA EVALUACIÓN DE LA CRITICIDAD

Claves para la lista de verificación:

La EFS debe asignar un grado de importancia a las preguntas referidas a estándares. En caso de ser necesario, puede asignar el grado de importancia en conjunto con la entidad auditada. En caso de no asignarse ninguna importancia, la EFS puede dar la misma importancia a todas las preguntas, es decir, 1.

Las cifras entre paréntesis son puntuaciones indicativas para las respuestas. Las puntuaciones se ubican entre 1 y 5, siendo 1 indicativo de menor riesgo y 5 de mayor riesgo. Las EFS podrán adoptar escalas diferentes para ajustarlas a su realidad.

Las preguntas no son exhaustivas. Las EFS pueden seleccionar preguntas del cuadro que se presenta a continuación, o bien elaborar otras según sus propias necesidades.

La información incluida en la lista de verificación se debe recolectar para todas las organizaciones a ser auditadas por las EFS. Las EFS pueden procurar recolectar tanta información como sea posible a fin de que la puntuación y las comparaciones sean relevantes.

La EFS puede decidir mantener las puntuaciones y la calificación de manera confidencial, o bien compartirlas con los interesados de conformidad con su política.

I. NOMBRE DE LOS SISTEMAS DE TI Y DE LA ORGANIZACIÓN

	CRITERIOS	PESO	PUNTAJE
	Gobernanza de TI		
1	**Estado general de informatización de la entidad. La entidad ha informatizado:**		
	Todos los procesos del negocio (5)		
	La mayoría de los procesos del negocio (4)		
	Solo unos pocos procesos (3)		
	Ningún proceso del negocio (1)		
2	**La entidad posee una política de TI y políticas conexas**		
	Sí (1)		
	Parcialmente (3)		
	No (5)		
3	**La entidad posee:**		
	Un área de TI independiente (2)		
	Subcontrató algunas funciones de TI (5)		
	Subcontrató instalaciones de TI (5)		
4	**La entidad posee:**		
	Una gerencia de Tecnología o Sistemas (CIO) a cargo de las actividades		

	Un funcionario suficientemente calificado a cargo de las actividades relacionadas con TI, además de sus propias responsabilidades (3)		
	Un funcionario de menor ranto a cargo de actividades relacionadas con TI		
	La entidad no ha designado a ningún empleado para ocuparse de las		
	Desarrollo, Adquisición y Subcontratación		
5	**El sistema fue desarrollado:**		
	Internamente con suficiente capacidad interna (1)		
	Internamente con capacidad interna insuficiente (5)		
	Por parte de un contratista/ otro organismo de gobierno (4)		
	Una combinación de desarrollo interno y subcontratación (5)		
6	**La adquisición fue realizada:**		
	Por la entidad misma con suficiente capacidad para realizar adquisiciones		
	Por la entidad misma con insuficiente capacidad para realizar		
	Utilizando servicios de un consultor (4)		
7	**La documentación del sistema está:**		
	Disponible (1)		
	Parcialmente disponible (3)		
	No disponible (5)		
8	**¿Con qué frecuencia se efectúan/justifican cambios a las**		
	Más de cinco veces al año (5)		
	Menos de cinco veces al año y más de dos veces al año (3)		
	Menos de dos veces al año (2)		
	Ni una vez al año (1)		
	Operaciones de TI y Seguridad de SI		
9	**Cantidad de puntos de acceso/ubicaciones de la transacción/usuarios**		
	Más que Y (5)		
	Más que X, menos que Y y más que esos niveles, si es necesario (3)		
	Menos que X (1)		
	(Los números de X e Y serán decididos por la EFS)		
10	**Red**		
	Ninguna red (1)		
	Red de Área Local (LAN) (3)		
	Red de Amplio Alcance (WAN) (4)		
	A través de Internet (5)		
11	**Número de ubicaciones** *(Límite, números para ubicaciones como X e Y a ser decididos por la EFS)*		
	Solo una ubicación (1)		
	Más de una ubicación, menos de X ubicaciones (3)		
	Más de X ubicaciones (5)		
12	**¿Hace el sistema uso de enlaces directos con terceros, por ejemplo,**		
	Sí (5)		
	No (1)		
13	**Número de usuarios finales del sistema**		
	Menos de X (1)		
	Más de X, menos de Y y más de dichos niveles si es necesario (3)		
	Más de Y (5)		
14	**La entidad mantiene los datos y la aplicación:**		
	Internamente (1)		
	Parcialmente en forma interna y en instalaciones subcontratadas (3)		
	Alojado en instalaciones subcontratadas (5)		
15	**El sistema ha estado operando durante :**		
	Más de diez años (1)		
	Entre cinco y diez años		
	Entre dos y cinco años		
	Menos de dos años (5)		
16	**El volumen de datos en el sistema de aproximadamente (incluidos los**		

	Más de diez GB (5)		
	Entre dos GB y diez GB		
	Menos de dos GB (1)		
	Compromiso Financiero		
17	**Inversión efectuada en el sistema** *(Límite/monto niveles de $X y $Y a ser decididos por las EFS)*		
	Superior a $Y (5)		
	Superior a $X, menor a $Y (y superior a dichos niveles, de ser necesario)		
	Inferior a $X (1)		
18	**Modo de financiamiento del sistema**		
	A partir de recursos internos (3)		
	A partir de empréstitos (4)		
	A partir de préstamos de organismos internacionales (5)		
19	**Gastos fijos del sistema** *(Límite/ niveles de monto $X y $Y a ser decididos por las EFS)*		
	Superior a $Y (5)		
	Superior a $X, inferior a $Y (y mayor a dichos niveles, si es necesario) (3)		
	Inferior a $X (1)		
	Riesgo Funcional/ Usabilidad del Sistema		
20	**El sistema es utilizado para:**		
	Procesos internos solamente (3)		
	Procesos externos solamente (4)		
	Procesos internos y externos (5)		
21	**¿Proporcional el sistema servicios a los ciudadanos?**		
	Sí (5)		
	No (3)		
	Control Interno y Auditorías		
22	**¿Se ha realizado una certificación del sistema por parte de terceros?**		
	Sí (1)		
	No (5)		
23	**¿Ha sido el sistema auditado por auditores de TI de la EFS?**		
	Hace tres años (2)		
	Hace cinco años (4)		
	Nunca (5)		
24	**¿Se han realizado otras observaciones de auditoría (financiera/de cumplimiento/de desempeño) en auditorías anteriores?**		
	Varias observaciones de auditoría recurrentes (5)		
	Pocas observaciones de auditoría recurrentes (3)		
	Ninguna observación de auditoría recurrente (1)		
La lista no es completa. Las EFS pueden definir sus propios criterios además de los criterios presentados en esta lista.			
	Puntaje total:		

II. CALIFICACIÓN DE LOS SISTEMAS DE TI

Una vez completada la Lista de Verificación antes descripta, el auditor de TI puede utilizar el cuadro que se presenta a continuación para resumir su evaluación de los sistemas de TI dentro del organismo de auditoría. Esto se puede realizar utilizando las puntuaciones totales generadas por la lista de verificación y obteniendo una categoría de riesgo (según la sección III que se presenta a continuación), como también la correspondiente calificación.

Nombre del Sistema de TI	Puntuación total	Categoría del Riesgo	Calificación

III. CATEGORÍA DEL RIESGO

Prioridad del Sistema de TI	Rango* de Puntuación Total
A	L1-L2
B	>L2 y <L3
C	>L3 y <L4
D	> L4

***L1, L2, L3, L4 son rangos de puntuación a ser decididos por la EFS para categorizar los sistemas de TI.**

Por lo tanto, el marco anterior contempla la categorización de los sistemas de TI y también los clasifica para priorizarlos en las auditorías. La categoría "A" es la categoría de menor riesgo y la categoría "D" es la categoría de mayor riesgo.

ANEXO II:
MATRIZ SUGERIDA PARA LA AUDITORÍA DE GOBERNANZA DE TI

<table>
<tr><th colspan="2">Identificación, Dirección y Monitoreo de las Necesidades de la Organización</th></tr>
<tr><td colspan="2">Objetivo de auditoría: Evaluar si la Dirección de la organización conduce, evalúa y monitorea efectivamente el uso de TI para el cumplimiento de la misión institucional.</td></tr>
<tr><td colspan="2">Tema 1 de auditoría: Definir los requerimientos de TI
¿De qué manera la organización identifica y aprueba los requerimientos del negocio y de TI?</td></tr>
<tr><td colspan="2">Criterios:
La organización cuenta con un plan sobre cómo identificar los negocios emergentes o las necesidades de TI, y el Comité Directivo tiene suficiente información para tomar sus decisiones y aprobar los requerimientos.</td></tr>
<tr><td>Información Requerida</td><td>Método(s) de Análisis</td></tr>
<tr><td>Proceso de gestión de requerimientos

Actas del Comité Directivo y principios de operatividad, incluido el límite de aprobación y rechazo

Lista de requerimientos aprobados y rechazados</td><td>Revisión de los documentos para garantizar que los requerimientos de los nuevos negocios sean identificados y analizados de acuerdo con el proceso de gestión de requerimientos de la organización.

Revisión de los requerimientos aprobados o rechazados para garantizar que éstos se ajusten a los principios de operación aceptados.

Entrevista con la gerencia u otros responsables de la aprobación de proyectos para garantizar que se tomen en cuenta las capacidades, habilidades, recursos y capacitación del área de TI y la habilidad de los usuarios para utilizar nuevas herramientas y métodos o procedimientos.</td></tr>
<tr><td colspan="2">Tema 2 de auditoría : Liderazgo
¿De qué manera la Dirección conduce y supervisa el cumplimiento de los objetivos del negocio y el desempeño de TI de forma periódica?</td></tr>
<tr><td colspan="2">Criterios:
Se establecen las medidas de desempeño y el consejo o comité superior o equivalente realiza revisiones periódicas y reuniones, y toma las medidas apropiadas, o existe un sistema de reportes a la gerencia que le comunica el nivel de desempeño.</td></tr>
<tr><td>Información Requerida</td><td>Método(s) de Análisis</td></tr>
<tr><td>Medidas de desempeño para el negocio y TI

Informes periódicos sobre el estado del proyecto

Actas de revisiones periódicas

Lista de medidas a tomar y su estado, etc.</td><td>Revisión de una muestra de decisiones o memos de la gerencia para garantizar que sean claros y bien fundamentados, e inequívocos.

Revisión de las medidas de desempeño para garantizar que cubran el negocio y los sistemas de TI.

Revisión de los informes de estado del proyecto [u otra documentación que contenga el estado del proyecto (actas de las reuniones, correos electrónicos, etc.)] para garantizar que incluyan los indicadores de costo, cronograma e indicadores de desempeño y variaciones respecto al plan.

Revisión de las medidas a tomar de la gerencia para garantizar que son asignadas y se haga un seguimiento hasta el cierre e incluyan las lecciones aprendidas.</td></tr>
</table>

Tema 3 de auditoría: Inversiones de TI **¿De qué manera la organización gestiona las inversiones de TI?**	
Información Requerida	**Método(s) de Análisis**
Procedimientos y plan para la gestión de la inversión	Entrevista a la gerencia para determinar los procedimientos de gestión de inversiones de la organización.
Cartera de proyectos de TI	Revisión de la cartera para evaluar si los proyectos han sido priorizados de acuerdo con los criterios aprobados.
Informes de los análisis de muestra de costo- beneficio	Revisión de los informes de estado para verificar que proporcionan seguimiento de costos y cronograma.
Lista de proyectos aprobados y rechazados o aplazados	Revisión de los informes de análisis de costo-beneficio para evaluar que estén completos, que reflejen las condiciones reales y que no exageren los beneficios o subestimen el costo o cronograma (utilizar los servicios especializados de economistas o expertos en costos, si es necesario).
Informes del estado de los proyectos aprobados	En el caso de dificultades en los proyectos, determinar si su metodología fue la apropiada para el tipo de proyecto y fue adecuadamente aplicada, y si el aseguramiento de la calidad ha estado involucrado durante el ciclo de vida.
Informes de evaluación de las muestras pos proyectos	Entrevista con la gerencia para determinar si algún proyecto ha sido cancelado debido al bajo nivel de beneficios o desempeño.
	Entrevista con la gerencia para determinar de qué manera la organización toma las decisiones sobre las soluciones de desarrollo vs. adquisición (compra) (por ejemplo, en base a la capacidad, habilidades, costo, riesgo, etc.).
Conclusión de la Auditoría: Para ser completado por el auditor	

Estrategia de TI	
Objetivo de auditoría: Confirmar si existe una estrategia de TI, incluido el plan de TI y los procesos para el desarrollo de la estrategia, aprobación, implementación y mantenimiento, que se adapte a las estrategias y objetivos de la organización. Verificar que, mientras se da cumplimento a los objetivos de TI, los riesgos y recursos son gestionados con eficacia.	
Tema 4 de auditoría: Calidad de la estrategia de TI **¿Cuenta la organización con una estrategia de TI que sirva para guiar sus funciones de TI?**	
Criterios: Existe un plan estratégico de TI a nivel de la organización, que traduce los objetivos del negocio en metas y requerimientos de TI, aborda los recursos necesarios de TI para apoyar el negocio, y es revisado y actualizado periódicamente.	
Información requerida	**Método(s) de Análisis**
Plan Estratégico de TI, o documento equivalente	Revisión del documento
Actas de reunión de TI y reuniones del Comité Directivo de la Organización	Entrevista al directorio de la organización para determinar si sus necesidades son satisfechas por el área de TI.
	Revisión de las actas de las reuniones periódicas del Comité de TI y Comités Directivos de la Organización para garantizar que la alta dirección esté representada y que las decisiones estratégicas de TI se tomen a nivel del Comité Directivo.
	Revisión de la Estrategia de TI o entrevista con la gerencia para determinar los requerimientos de recursos y de qué manera se determinan y aprueban, quién aprueba la adquisición adecuada de herramientas y otros recursos (personal, contratantes, habilidades por medio de capacitación, etc.).

Tema 5 de auditoría: Gestión de Riesgo **¿De qué manera gestiona la organización sus riesgos?**	
Criterios: La organización cuenta con una política y plan de gestión de riesgos, y ha asignado recursos suficientes para identificarlos y gestionarlos.	
Información Requerida	**Método(s) de Análisis**
Plan de Gestión de Riesgos Lista de riesgos (incluida TI) y estrategias de mitigación. Actas de la evaluación periódica de riesgos u otras reuniones, si están disponibles.	Revisión del plan de gestión de riesgos u otro documento para garantizar que las responsabilidades de gestión de riesgos sean clara e inequívocamente asignadas. Revisión de documentos para determinar si los riesgos de TI son parte del marco general de gobernanza del riesgo y cumplimiento (GRC) Revisión de las actas de la reunión para garantizar que los nuevos riesgos sean incorporados y analizados según corresponda. Entrevista al personal responsable de la gestión de riesgos para determinar si los riesgos a ser mitigados cuentan con estimaciones de costos apropiadas y si los recursos son asignados. Entrevista con la gerencia o revisión de actas de la reunión para determinar si la dirección tiene conocimiento de los riesgos de TI y otros riesgos, y controla su estado de forma periódica.
Conclusión de la auditoría: Para ser completado por el auditor	

Estructuras, Políticas y Procedimientos de la organización

Objetivo de auditoría: garantizar que existan estructuras, políticas y procedimientos que permitan a la organización cumplir su mandato.	
Tema 6 de auditoría: **¿Es apropiada la estructura del área de TI de la organización para que ésta cumpla los objetivos de TI y satisfaga las necesidades del negocio?**	
Criterios: El área de TI se sitúa en un nivel suficientemente alto dentro de la organización, y sus funciones y responsabilidades se definen claramente, incluidas las del Gerente de Tecnología o Sistemas (CIO) o su equivalente.	
Información Requerida	**Método(s) de Análisis**
Organigrama general Organigrama de TI	Revisar los organigramas para determinar que el área de TI esté posicionada a nivel estratégico (por ejemplo, hay un CIO que depende o es miembro del Comité Directivo) Revisar el organigrama de TI para determinar que esté alineado con el negocio (tiene asistencia técnica, administradores de bases de datos, personal de mantenimiento o contratistas que prestan ayuda y facilitan las operaciones de TI).
Tema 7 de auditoría: Política y Procedimientos **¿Ha aprobado la organización y está utilizando políticas y procedimientos apropiados para guiar sus negocios y operaciones de TI?**	
Criterios: La organización documenta, aprueba y comunica las políticas y los procedimientos adecuados para guiar los negocios y las operaciones de TI con el fin de cumplir con su mandato.	
Información Requerida	**Método(s) de Análisis**
Políticas organizacionales respecto de: Recursos Humanos	Revisar las políticas para garantizar que están aprobadas y en curso. Por ejemplo, revisar la política de Recursos Humanos para determinar que los requerimientos de habilidad estén definidos y la capacitación esté identificada

incluida la contratación y terminación de la seguridad, retención de documentos, contratación y/o subcontratación, desarrollo y/o adquisición de software, etc. Procedimientos para áreas de políticas seleccionadas Correos electrónicos u otras formas para comunicar las políticas a los usuarios y partes interesadas adecuadas Informes de aseguramiento de la calidad a la gerencia que comuniquen el cumplimiento periódico de procedimientos y políticas y otras cuestiones Solicitar cambios en las políticas y/o revisiones periódicas y resultados	para el personal nuevo y otros. Revisar los materiales de capacitación inicial y de actualización u otros procesos internos mediante los cuales estas políticas y procedimientos son comunicados dentro de la organización. Entrevistar a los miembros del área de aseguramiento de la calidad u otro grupo responsable de aplicar la política para verificar qué hacen para garantizar el cumplimiento. Entrevistar al personal de aseguramiento de calidad o al personal a cargo del cumplimiento de las normas para determinar cómo y cuándo informa sus resultados a la gerencia senior. Entrevistar al personal responsable del cumplimiento de las políticas y procedimientos para determinar con qué frecuencia informa los resultados a la gerencia senior, y la forma en la que solicita opiniones sobre el incumplimiento de manera anónima e independiente. Entrevistar a gerentes y usuarios para comprender su percepción y actitud respecto de las políticas y los procedimientos analizados. En el caso de opiniones frecuentes: “Los procedimientos son complejos” preguntar cuáles y de qué manera se podrían simplificar. Revisar los antecedentes de la política de control de cambio para verificar que las políticas se actualizan periódicamente o cuando es necesario. Revisar los informes de aseguramiento de la calidad para garantizar que contengan temas relacionados con el cumplimiento de políticas o procedimientos según corresponda. Revisar correos electrónicos u otros mecanismos (correo físico, capacitación, etc.) para garantizar que las políticas sean distribuidas a los usuarios adecuados e interesados cuando se actualicen o sea necesario. Revisar las políticas para verificar su adecuación mediante la búsqueda de (por ejemplo): • Alcance de la política y el mandato • Definición de los roles y las responsabilidades • Recursos y herramientas requeridas • Relación con los procedimientos • Reglas para hacer frente al incumplimiento
Conclusión de la Auditoría: Para ser completado por el Auditor	

Recursos Humanos y materiales	
Objetivo de auditoría: Evaluar si se cuenta con suficiente personal calificado / capacitado con acceso a recursos adecuados como para permitir a la organización cumplir con sus objetivos.	
Tema 8 de auditoría: Recursos Humanos y logística **¿Cómo hace la organización para satisfacer las necesidades actuales y futuras de recursos humanos y materiales?**	
Criterios: La organización debe contar con un plan para satisfacer sus requerimientos actuales y futuros, para cumplir con las necesidades de la organización.	
Información Requerida	**Método(s) de Análisis**
Políticas organizacionales	Revisión de las políticas para garantizar que están aprobadas y vigentes.

respecto de: Recursos Humanos y Capacitación Estrategia de TI o Plan Estratégico Planes de Contratación y Capacitación	Revisión de las políticas para garantizar que requieren varios grupos (TI, aseguramiento de la calidad (QA), usuarios del negocio) para identificar sus necesidades actuales y futuras de personal y recursos. Revisión de los planes de contratación y capacitación para garantizar que reflejen las necesidades identificadas. Por ejemplo, revisar la política de Recursos Humanos para determinar que los requerimientos relativos a las capacidades se definan y la capacitación sea identificada para el personal nuevo y otros miembros del personal. Entrevista a gerentes de Recursos Humanos o de Negocios para evaluar de qué manera ellos garantizan la ocupación de puestos claves en caso de contingencias o ausencias prolongadas. Revisión de materiales de capacitación inicial y actualización u otro proceso interno mediante el cual estas políticas y procedimientos se comunican dentro de la organización. Revisión del plan estratégico de TI para garantizar que incluya el personal y los recursos necesarios para las necesidades actuales y futuras.
Conclusión de la Auditoría: Para ser completado por el Auditor	

Evaluación de Riesgos y mecanismos de cumplimiento

Tema 9 de auditoría: Mecanismo
¿Cómo se asegura la organización de que cuenta con mecanismos vigentes y adecuados para garantizar el cumplimiento de las políticas y los procedimientos?

Criterios:
La organización cuenta con un mecanismo (a través de un grupo de aseguramiento de la calidad, auditoría interna, o verificación al azar, etc.) para garantizar el cumplimiento de todas las políticas y procedimientos.

Información Requerida	**Método(s) de Análisis**
Políticas y procedimientos de la organización (Seguridad, SDLC, Capacitación, etc.) Organigrama Plan de aseguramiento de la calidad Informes de los equipos o grupos del área de cumplimiento Actas del Comité Directivo	Selección de una muestra de las políticas y procedimientos de la organización para evaluar el cumplimiento. Entrevista a la gerencia para determinar quién es responsable de garantizar el cumplimiento de las políticas y procedimientos conexos (auditoría seleccionada). Entrevista al equipo o grupo responsable del cumplimiento de lo anterior para determinar la forma en que cumplen con sus obligaciones. Revisión de los informes de varios grupos del área de cumplimiento para verificar lo que han hallado, qué medidas han tomado y comunicado a la gerencia. Revisión de las actas del comité directivo para verificar si las cuestiones relacionadas con un nivel elevado de cumplimiento se discuten en esta u otras reuniones. Entrevista al autor(es) para determinar la razón para la actualización de las políticas o procedimientos existentes. Revisión de los últimos temas y resoluciones relativos al incumplimiento. Revisión de la capacitación u otros mecanismos de difusión (correo electrónico, memorando, notificación) para verificar si se abordaron cuestiones relativas al incumplimiento.

Conclusión de la auditoría: Para ser completado por el Auditor
Ver el Anexo III y el Anexo IV respectivamente para las matrices de auditoría sobre Desarrollo y Adquisición y Operaciones de TI.

ANEXO III

MATRIZ SUGERIDA PARA LA AUDITORÍA DE DESARROLLO Y ADQUISICIÓN

<table>
<tr><th colspan="2">Requerimientos para el Desarrollo y Gestión</th></tr>
<tr><td colspan="2">Objetivo de auditoría: Evaluar de qué manera la organización identifica, prioriza y gestiona sus requerimientos de TI.</td></tr>
<tr><td colspan="2">Tema 1 de auditoría:
¿Cómo identifica la organización las necesidades de los usuarios de los servicios de TI?</td></tr>
<tr><td colspan="2">Criterios:
La organización cuenta con un plan o procedimientos sobre la forma de recopilar, revisar y enumerar los requerimientos para una funcionalidad nueva o adicional.</td></tr>
<tr><td>Información Requerida

Plan o procedimiento de gestión de requerimientos

Requerimientos de muestras presentados por los usuarios

Revisión inicial de la muestra</td><td>Método(s) de Análisis

Revisión del plan o procedimientos de gestión de requerimientos para garantizar que los usuarios, interesados u otros usuarios pertinentes participen en la identificación de los requerimientos.

En un importante desarrollo para el mejoramiento de la funcionalidad, la consulta de los usuarios y el desarrollo de prototipos pueden ser implementados paralelamente. El intercambio de información entre los titulares de los procesos del negocio y proveedores/organización de TI debe ser examinado.

Revisión de requerimientos de muestra para garantizar que existe una revisión inicial y que requerimientos similares o duplicados estén clasificados.</td></tr>
<tr><td colspan="2">Tema 2 de auditoría:
¿De qué manera la organización analiza, prioriza y gestiona los requerimientos del usuario?</td></tr>
<tr><td colspan="2">Criterios:
La organización analiza, prioriza y gestiona los requerimientos para garantizar que las necesidades del usuario se cumplan de manera óptima y rentable.</td></tr>
<tr><td>Información Requerida

Lista de requerimientos

Análisis de muestra de los requerimientos

Matriz de trazabilidad de requerimientos

Criterios para la priorización de requerimientos</td><td>Método(s) de Análisis

Revisión de los requerimientos para verificar que incluyan autor, fecha, prioridad, costo, riesgo y otros elementos.

Revisión del análisis de los requerimientos o comentarios sobre los requerimientos por parte de la alta dirección o interesados a fin de determinar que todas las opiniones se solicitan y resumen para el análisis correspondiente (aceptar, aplazar, rechazar, etc.).

Revisión de la matriz de trazabilidad para determinar que los requerimientos aprobados se asignen tanto al desarrollo como a la adquisición de proyectos y se realice un seguimiento de los mismos hasta el cierre cuando se implementen.

Revisión de los criterios de prioridad de los requerimientos para evaluar si incluyen elementos tales como el costo, las necesidades del negocio, los</td></tr>
</table>

	asuntos de emergencia y los nuevos mandatos.
Conclusión de la auditoría : Para ser completado por el Auditor	

Gestión y control de proyectos	
Objetivo de auditoría: Evaluar de qué manera la organización gestiona y controla el desarrollo o la adquisición de proyectos de TI aprobados.	
Tema 3 de auditoría: **¿Cómo planifica la organización el desarrollo o la adquisición de proyectos de TI?**	
Criterios: La organización cuenta con un plan de gestión de proyectos o equivalente para cada proyecto aprobado que guía su ejecución.	
Información Requerida	**Método(s) de Análisis**
Plan de gestión de proyectos o equivalente	Revisión del plan de gestión de requerimientos o equivalente para garantizar que contenga la descripción del proyecto, alcance, costo, cronograma, riesgos, estructura de la gestión y que identifique a las partes interesadas (internas o externas). Revisión del plan para garantizar que ha sido aprobado por la gerencia senior y que incorpora comentarios de las partes interesadas. Revisión del organigrama del proyecto para determinar las funciones de los individuos responsables del aseguramiento de la calidad o pruebas, desarrollo e instalación del sistema en la infraestructura tecnológica de las organizaciones, grupo de soporte, etc. Para los proyectos de adquisición, garantizar la existencia de un plan o lista equivalente de quienes estarán a cargo de la supervisión del contratista y revisión de las aprobaciones otorgadas por las personas responsables. Entrevista a los gerentes de proyecto para determinar qué método de SDLC ha sido utilizado para el desarrollo del proyecto. Tema 4 de AUDITORIA: ¿Cómo controla la organización los proyectos de TI?
Tema 4 de auditoría: **¿Cómo controla la organización los proyectos de TI?**	
Criterios: La organización controla y hace un seguimiento de los proyectos para garantizar que cumplan con su costo, cronograma y requerimientos de desempeño.	
Información Requerida	**Método(s) de Análisis**
Referencias de costo del proyecto y cronograma Informes del estado del proyecto	Comparación de las referencias de costo del proyecto y cronograma con los informes de estado del proyecto para evaluar desviaciones. Entrevista al gerente de proyectos/revisión de los informes para determinar si se han tomado medidas correctivas adecuadas en caso de desviaciones importantes.

Aseguramiento de la Calidad y Prueba

Objetivo de auditoría: Evaluar de qué manera la organización garantiza que los proyectos de desarrollo o adquisición de TI cumplen con los objetivos de calidad.

Tema 5 de auditoría:
¿Cuenta la organización con una estructura de aseguramiento de la calidad y están definidas sus funciones y responsabilidades?

Criterios:
Un procedimiento establecido para la conducción de actividades de aseguramiento de la calidad

Información requerida	**Método(s) de Análisis**
Política o plan de aseguramiento de la calidad	Revisión de la política o plan de aseguramiento de la calidad para determinar qué grupo o individuos se encargan de llevar a cabo las actividades de aseguramiento de la calidad para el proyecto (por ejemplo, el grupo de Aseguramiento de la Calidad debe revisar los documentos para garantizar que reflejen con precisión los requerimientos, debe revisar los manuales del usuario para garantizar que son legibles y no existen elementos o etapas faltantes).
Procedimientos de aseguramiento de la calidad	
Roles y Responsabilidades del grupo o individuo(s) a cargo del Aseguramiento de la Calidad	Revisión de los procedimientos de aseguramiento de la calidad o entrevistas con personal a cargo de esta área para determinar qué actividades llevan a cabo (cumplir con las revisiones entre pares, estar presente en las revisiones de diseño u otras revisiones, etc.).
Informes de aseguramiento de la calidad	Revisión de los informes del aseguramiento de la calidad de la organización para determinar qué observaron (si el equipo del proyecto está cumpliendo con su plan de gestión de proyectos y el SDLC adoptado, y las revisiones conexas, etc.) y a quienes se reportan los problemas.
SDLC adoptado por el Proyecto	

Tema 6 de auditoría:
¿De qué manera la organización planifica y conduce las pruebas de los sistemas?

Criterios:
La organización lleva a cabo pruebas en los sistemas y, en base a los resultados, lo acepta o rechaza.

Información requerida	**Método(s) de Análisis**
Plan de pruebas	Revisión de los planes de prueba.
Cronograma de pruebas	Comparación del costo del proyecto y cronograma de referencia con los informes de estado del proyecto para evaluar desviaciones, si las hubiera.
Resultados de las pruebas	Entrevista al gerente de proyecto o revisión de informes para determinar si se tomaron las medidas correctivas apropiadas en caso de desviaciones importantes.
Aceptar o rechazar criterios	Entrevista al equipo de gestión del proyecto y revisión de las actas de las reuniones con el contratista para evaluar la frecuencia y eficacia de la supervisión de las actividades de los proyectos subcontratados.
	Revisión del SLA del contratista o del contrato para garantizar que cumplen con los términos del contrato, por ejemplo, verificar que los contratistas realicen revisiones periódicas, proporcionen informes del estado, realicen un seguimiento de las medidas a tomar, conduzcan actividades de gestión de riesgos de conformidad con el contrato. Entrevista al contratista en la organización para determinar la forma en que ésta dirige al contratista si el SLA no está disponible.

Conclusión de la auditoría:
Para ser completado por el auditor

Solicitud

Objetivo de auditoría: Evaluar de qué manera la organización garantiza que las actividades relacionadas con la solicitud (conjunto de tareas tales como la confirmación del documento de las necesidades, encuadre del RFP, evaluación de las propuestas, realización de aclaraciones a la oferta preliminar, diseño y presentación de la oferta, evaluación, etc. conducentes a la adjudicación del contrato) son llevadas a cabo de acuerdo con el plan de requerimientos o el procedimiento adoptado.

Tema 7 de auditoría:
¿Cuál es el plan o procedimiento para la atención de solicitudes?

Criterios:
Las actividades de solicitud, incluida la selección de proveedores, se realizan de acuerdo con el plan de solicitud de la organización.

Información requerida	**Método(s) de Análisis**
Plan o procedimiento de solicitud Paquete de solicitud Revisión de requerimientos por parte del usuario Revisión del paquete de solicitud por parte del usuario Leyes aplicables que rigen la conducta de la solicitud	Revisión del plan de solicitud para garantizar que cubre áreas tales como la participación de los usuarios, obtención de ofertas sobre una base competitiva, realización de estudios de mercado previos al contrato en las áreas que correspondan y que la selección de proveedores se base en criterios objetivos. Entrevista al personal contratante clave para evaluar de qué manera garantiza que el paquete de solicitud esté completo (por ejemplo, haciendo que lo revisen los usuarios, grupos de interés, expertos, según corresponda). Entrevista a los usuarios o alta dirección para garantizar que hayan sido consultados durante la generación de los requerimientos o hayan aprobado los requerimientos técnicos de la solicitud y/o el paquete de oferta final. Entrevista a él/los funcionario(s) de contratación para evaluar la forma en la que garantizan que el proceso de solicitud cumple con las leyes y reglamentos aplicables.

Tema 8 de auditoría:
¿Qué criterios utiliza la organización para la selección de un proveedor?

Criterios:
La organización utiliza criterios objetivos y publicados para la selección de cada proveedor.

Información Requerida	**Método(s) de Análisis**
Criterios de selección de proveedores Matriz de puntuación de proveedores o equivalente	Revisión de los criterios de selección de proveedores para garantizar que reflejan la intención de la solicitud (por ejemplo, en un contrato de software, la selección del proveedor no debería incluir parámetros no esenciales para la organización). Entrevista a las partes interesadas clave para evaluar si están de acuerdo con los criterios de selección. Revisión de la matriz de puntuación del proveedor o equivalente para confirmar que sea compatible con los criterios de selección.

Conclusión de la Auditoría:
Para ser completado por el auditor

Gestión de la Configuración

Objetivo de auditoría: Evaluar de qué manera la organización gestiona la configuración de los productos relacionados con el desarrollo y la adquisición.

Tema 9 de auditoría:
¿Qué política utiliza la organización para la gestión de la configuración?

Criterios:
Las actividades de gestión de configuración se realizan de acuerdo con la política o procedimiento de la organización

Información Requerida	**Método(s) de Análisis**
Política o procedimientos de gestión de la configuración o equivalente	Revisión de la política de gestión de configuración en cuanto a su adecuación mediante la búsqueda de (por ejemplo): Alcance de la política y mandato. Definición de funciones y responsabilidades. Recursos y herramientas requeridas. Relación con los procedimientos. Reglas para enfrentar el incumplimiento. Entrevista al personal responsable de la gestión de configuración, si no existe una política, para evaluar de qué manera garantiza que sus funciones se llevan a cabo de manera uniforme para la organización.

Tema 10 de auditoría:
¿Qué grupo o individuo(s) son responsables de la autorización de los cambios y de la instalación final en el entorno de producción?

Criterios:
Sólo los cambios autorizados y aprobados deben ser introducidos en el entorno de producción.

Información requerida	**Método(s) de Análisis**
Grupos o individuos responsables de autorizar los cambios Proceso de aprobación e introducción de los cambios aprobados y probados en el entorno de producción	Garantizar que exista un grupo que autorice cambios en los productos. El grupo podría ser el equipo de control de cambios o equivalente que revisa y aprueba los cambios. Entrevista al personal responsable de autorizar la introducción de un nuevo software al entorno de producción a fin de garantizar que el software ha sido probado (incluidas pruebas de regresión con otros sistemas, si es necesario), cumple con los criterios de aceptación, cuenta con la documentación apropiada, e incluye la capacitación de usuarios (si corresponde) antes de ser introducido al negocio. Entrevista al personal responsable de autorizar los cambios en el sistema de producción para determinar de qué manera controlan y previenen cambios no autorizados en el sistema (por ejemplo, mediante el control del acceso al sistema de producción, la separación de los entornos de producción y desarrollo, etc.).

Conclusión de la Auditoría:
Para ser completado por el auditor

ANEXO IV
MATRIZ SUGERIDA PARA LA AUDITORÍA DE LAS OPERACIONES DE TI

<table>
<tr><th colspan="2">Gestión del Servicio</th></tr>
<tr><td colspan="2">Objetivo de auditoría: Evaluar si el área de TI monitorea activamente las operaciones de TI de conformidad con el Acuerdo de Nivel de Servicio interno o el contrato suscripto.</td></tr>
<tr><td colspan="2">Tema 1 de auditoría: Parámetros clave
¿Qué criterios básicos de medición de servicios están cubiertos por el SLA interno entre la organización y el área de TI?</td></tr>
<tr><td colspan="2">Criterios:
Buenas prácticas de SLA – asignación de responsabilidades entre los responsables de los procesos del negocio y el área de TI, objetivos documentados de la organización para la gestión de la red, ofertas de servicios y parámetros, definición por tipo de problemas, responsabilidades del centro de atención.</td></tr>
<tr><td>Información Requerida

SLA interno de la entidad entre el directorio y el área de TI

• Responsabilidades del servicio de atención

• Informes de servicio generados

• Usuario/tiempo de respuesta de la aplicación</td><td>Métodos de Análisis

Revisión del SLA para determinar si contiene elementos apropiados – objetivos de nivel de servicio detallados y mensurables, sistemas y servicios cubiertos, calidad del servicio (QoS), servicios no cubiertos, soporte y resolución de problemas al nivel de la aplicación, disponibilidad del sistema, horario de centro de atención, tiempo de respuesta y resolución dependiendo de la clasificación de la gravedad de un problema, rendimiento, cronograma de mantenimiento, etc.

Verificar si la copia de seguridad de datos y las prácticas de recuperación son compatibles con las normas BCP de la entidad.

Verificar si los responsables de los procesos de negocios han firmado el acuerdo.

Entrevista a una muestra de usuarios para verificar el grado de concientización.</td></tr>
<tr><td colspan="2">Tema 2 de auditoría: Cumplimiento
¿Qué mecanismos existen para garantizar que el SLA se cumpla sistemáticamente?</td></tr>
<tr><td colspan="2">Criterios:
Implementación, monitoreo y modificación del SLA, de ser necesario.</td></tr>
<tr><td>Información Requerida

Parámetros del SLA

Informes de plazos

Diagramas o gráficos que muestran el éxito o fracaso de cómo se cumplen estos acuerdos a lo largo del tiempo

Documentos de las reuniones periódicas que revisan el análisis de las bases de referencia y las tendencias</td><td>Métodos de Análisis

Revisión de los informes que el área de TI genera diariamente o en cualquier otro intervalo de tiempo. Verificar si todos los indicadores acordados están siendo monitoreados por medio de informes/gráficos de tendencias, etc.

Revisión de los informes para examinar qué parámetros se miden y se reportan a la gerencia periódicamente.

Revisión de los documentos para verificar que los informes de las actividades del centro de atención sean considerados por la gerencia y comparados con las solicitudes de resolución, y que los temas esenciales sean considerados para las decisiones de compra y para la revisión periódica del SLA.</td></tr>
</table>

Parámetros operacionales - tasas de defectos, Consultas al centro de atención, otros caminos de comunicación, tiempo de respuesta, tiempo para implementar nuevas funciones , documentación de los cambios, ubicación del servicio, incentivos y cláusulas penales (especialmente importantes si los servicios de soporte de TI son subcontratados)	Entrevista al personal de el área de TI y análisis de la naturaleza de la supervisión del personal del centro de atención, las herramientas de monitoreo utilizadas, la priorización de tareas de soporte, recolección de bases de referencia para la red y la aplicación, datos sobre el tiempo de respuesta, la frecuencia de las copias de seguridad, la comprobación de los datos de las copia de seguridad para verificar el cumplimiento con los requerimientos del SLA. Verificar qué medidas toma la unidad de TI o, en caso de un grupo de soporte de TI subcontratado - por la dirección de la organización - si los parámetros operacionales no se corresponden con los requerimientos del SLA.
Tema 3 de auditoría: Eficacia ¿La gestión de servicios de TI garantiza la satisfacción de los usuarios y ayuda a cumplir los objetivos del negocio de la organización?	
Criterios: Consecución de los parámetros de desempeño que se ajustan a las necesidades y a los objetivos del negocio.	
Información Requerida	**Métodos de Análisis**
Informes del centro de atención al cliente, actas de las reuniones entre las partes interesadas del negocio y el área de TI Temas de agenda para los ciclos de revisión del SLA	Entrevista a una muestra de usuarios del negocio (a distintos niveles) o realización de una encuesta de satisfacción sobre la calidad de los servicios por parte del centro de atención al cliente y del grupo de soporte de TI. Revisión de los informes del centro de atención para comprobar si se previno una proporción significativa de temas críticos relativos al servicio antes de ser informados por los usuarios. Verificar si el tiempo de resolución de problemas reportados fue inferior al de los parámetros establecidos en el SLA. Verificar si los parámetros del SLA estaban siendo revisados periódicamente por la gerencia y revisión de las cuestiones relacionadas con la calidad del servicio.
Conclusión de la auditoría: Para ser completado por el auditor	

Gestión de la Capacidad

Objetivo de auditoría: Evaluar si el área de TI garantiza que la capacidad y el desempeño del sistema satisfacen las necesidades actuales y futuras del negocio.	
Tema 4 de auditoría: Acuerdo en relación con los parámetros ¿Existe un acuerdo documentado entre la entidad y el área de TI que se utilice como base para la selección de parámetros de funcionamiento de las operaciones de TI?	
Criterios: Gobernanza de TI: hacer un seguimiento y monitorear la implementación de la estrategia en términos de parámetros mensurables.	
Información requerida	**Métodos de Análisis**
SLA interno, o cualquier otra forma de acuerdo Parámetros de funcionamiento de TI: disponibilidad de recursos de procesamiento, tiempo promedio de inicio de sesión en el sistema,	Revisión del acuerdo o la guía de funcionamiento que el grupo de TI está utilizando. Garantizar que ha sido revisado y firmado por los usuarios del negocio pertinentes o por la dirección ejecutiva. Comparación de los parámetros de desempeño de referencia (a saber, disponibilidad de la red, el tiempo de respuesta del servidor central) establecidos por el área de TI con la guía de funcionamiento dispuesta por

porcentaje de tiempo de inactividad, tiempo promedio de respuesta del sistema, etc.	los responsables de los procesos del negocio para verificar que el área de TI cumple con la guía de funcionamiento.
Tema 5 de auditoría: Monitoreo ¿El área de TI recopila o revisa en tiempo real o periódicamente los datos de desempeño del sistema para mejorar su alineamientos con las necesidades del negocio?	
Criterios: Buenas prácticas de los administradores de los sistemas o las redes incluida la base de referencia para el desempeño, recolección de información relacionada con el tráfico y la configuración, disponibilidad de recursos del sistema, observación de estadísticas y tendencias del tráfico, análisis hipotéticos y utilización de herramientas para identificar las causas del deterioro del desempeño.	
Información Requerida Informes, medidas a tomar, tiempo de respuesta del centro de atención al cliente, y otros parámetros.	**Métodos de Análisis** Utilizar el tema de cumplimiento en la matriz de SLA. Prestar especial atención a todos los elementos que tienen impacto en la capacidad, es decir, comparar los parámetros reales de capacidad con los requerimientos del SLA, etc.
Tema 6 de auditoría: Análisis de los datos de desempeño ¿Se analizan y ajustan los datos de desempeño para mejorar la eficiencia y evitar limitaciones en la capacidad? Si fuese necesario, ¿ha planificado y adquirido el área de TI recursos adicionales para satisfacer las necesidades del negocio? ¿El área de TI emplea, capacita o contrata personal conforme cambian las necesidades de la organización?	
Criterios: Parámetros establecidos en el acuerdo o guía de operaciones, buenas prácticas para la optimización del desempeño (memoria, optimización del tiempo de respuesta de la red, sistema operativo, I/O, diseño eficiente del esquema de la base de datos, programación de tareas según la prioridad y el requerimiento de recursos, procedimientos de actualización o ajuste establecidos para manejar los problemas de capacidad tanto sobre una base reactiva como a largo plazo).	
Información requerida Informes, acciones, informes del estado, gráficos de parámetros de desempeño Actas de las reuniones en el máximo nivel de el área de TI	**Métodos de Análisis** Revisión de los informes que el área de TI genera diariamente o en otro período de tiempo elegido, verificar si genera y analiza datos sobre tendencias, identifica los impedimentos para tomar medidas, informes de excepción para los problemas de capacidad. Comparación con los requerimientos del SLA. Comparación de informes y patrones de tendencia para verificar las medidas procesales adoptadas en respuesta a los informes. Revisión de las actas de las reuniones y verificación sobre si las cuestiones relacionadas a la dotación del personal de TI, los problemas de capacidad y cualquier necesidad adicional de recursos se discuten y destacan en el momento adecuado.
Conclusión de la auditoría: Para ser completado por el auditor	

Gestión de problemas e incidentes
Objetivo de auditoría: Evaluar la eficacia de las políticas y procedimientos para la gestión de problemas e incidentes de la organización.
Tema 7 de auditoría: Política de Concientización ¿Existe una política documentada de respuesta a incidentes y están los usuarios del negocio en conocimiento de ella?
Criterios: Buenas prácticas en respuesta a incidentes.

Información Requerida	Métodos de Análisis
Política de respuesta a los incidentes de la entidad Directrices para la comunicación con terceros externos en relación con los incidentes	Revisión de la política para verificar si contiene las etapas adecuadas: preparación, detección y análisis, contención y erradicación, medidas post-incidente. ¿Depende el tipo de actividad de la alta incidencia o nivel de incidentes? Verificar si la política asigna requerimientos de responsabilidad, alcance e información. Revisión de los procedimientos reales mediante los cuales los usuarios del negocio tienen conocimiento de la política, y la naturaleza de la comunicación entre el equipo de respuesta a incidentes (mesa de ayuda) y las partes interesadas del negocio. Entrevista con una muestra de usuarios del negocio en toda la organización para obtener una garantía sobre la concientización del plan de respuesta a incidentes.
Tema 8 de auditoría: Conjunto de habilidades y recursos ¿Existe un equipo de respuesta a incidentes adecuadamente calificado que posea las herramientas adecuadas, los recursos y el respaldo de la gerencia senior para gestionar los incidentes?	
Criterios: Buenas prácticas para la respuesta a incidentes, directrices NIST, como lo establece el SLA.	
Información Requerida	**Métodos de Análisis**
Política y plan de respuesta a incidentes Acta del equipo de respuesta a incidentes, composición y experiencia SLA Capacitación para la concientización de respuesta a incidentes, estrategia de actualización de las habilidades requeridas del personal de IRT Lista de herramientas de registro y aplicaciones utilizadas para el monitoreo y uso de la red	Verificar si el equipo cuenta con un acta para investigar los incidentes. Recurrir a la experiencia en redes, sistemas operativos y de seguridad en los miembros del equipo y a la forma en que llevan a cabo su trabajo. Revisar los procedimientos del centro de asistencia para comprobar si se han establecido los procedimientos de escalada para incidentes que no se pueden resolver de inmediato, de acuerdo a las categorías de riesgo definidas en el SLA. Revisar qué medidas se han tomado en respuesta a incidentes pasados. Revisar los informes de los casos para comprobar si el personal apropiado estuvo involucrado en el análisis de incidentes. Verificar qué herramientas de gestión de incidentes han sido utilizadas: ¿son pertinentes para las necesidades de la organización? Verificar si la organización ha establecido normas y procedimientos de registro para garantizar que la información adecuada sea recopilada mediante registros y software de seguridad, y que los datos sean revisados de forma regular.
Tema 9 de auditoría: Eficacia de la respuesta ¿La estrategia de respuesta a incidentes resulta efectiva?	
Criterios: Buenas prácticas de respuesta a incidentes (COBIT 5 DSS dominio, ITIL sobre Soportes de Servicio)	
Información requerida	**Métodos de Análisis**
Medidas a tomar para la respuesta a incidentes, registros de formularios,	Verificar si se ha asignado a cada bien o servicio una prioridad de respuesta o tratamiento de incidentes.

etc. Capacitación periódica sobre concientización de la seguridad Procedimientos de manejo de incidentes: directrices para la priorización de incidentes Informes de casos y medidas adoptadas	Verificar si los procedimientos prevén la captura y el análisis de datos volátiles[51] y estáticos en el momento oportuno. Verificar si el equipo de respuesta concientiza periódicamente a los usuarios sobre las políticas y los procedimientos en cuanto al uso adecuado de redes, sistemas, soportes externos y aplicaciones. Revisar los documentos para verificar si las actividades posteriores a los incidentes, como cursos de actualización, se han brindado a los grupos de usuarios para evitar la costosa repetición de incidentes significativos. Verificar si se identificó la fuente del incidente. Verificar las medidas adoptadas (procedimiento de cambio, amonestación, capacitación, etc.). Verificar si el equipo de respuesta a incidentes registra todos los incidentes resueltos en detalle y revisar la información por posibles actualizaciones de la base de conocimientos.
Conclusión de la auditoría: Para ser completado por el auditor	

Gestión del Cambio	
Objetivo de auditoría: Evaluar si la entidad ha implementado un procedimiento estandarizado para el control de cambios en los sistemas y aplicaciones claves de TI.	
Tema 10 de auditoría: Política ¿Cuenta la organización con una política aprobada de gestión de cambios que contenga los controles apropiados en todo el ciclo?	
Criterios: Buenas prácticas en los controles de cambios: Solicitud de cambio- autenticación- aceptación- priorización- diseño de cambio- prueba de cambio- implementación- documentación.	
Información requerida	**Métodos de Análisis**
Política y procedimientos de la gestión de cambios, diagrama de flujo de procesos Estatuto del consejo para el control de cambio Plazo de revisión de la política Documentación para el cambio: solicitud de cambio, procedimientos de pruebas de control de cambio, plan de aseguramiento de calidad, plan y procedimientos de pruebas Informes y registros del software para la gestión del cambio Actas de la reunión del consejo de control de cambios Informes breves de gestión de cambio considerados por la gerencia	Referirse a los requerimientos generales para las políticas y los procedimientos en la sección *Gobernanza de TI*. Revisión del documento de política de gestión de cambio para verificar si se han establecido los procedimientos para la iniciación, revisión y aprobación de los cambios junto con la planificación de la responsabilidad de estas tareas. Revisión de los estatutos del consejo para el control de cambios a fin de identificar la asignación de responsabilidades y los niveles de responsabilidad. Entrevista al personal, observar las prácticas reales y revisar los documentos para garantizar que se cumpla con los procedimientos de gestión del cambio: consulta para verificar el cambio, rastrear el cambio hasta el entorno operativo, verificar el cumplimiento de los procedimientos de solicitud, por ejemplo, revisión y priorización realizada por la gerencia, y verificar la existencia de la aprobación y la documentación. Verificar si el equipo de aseguramiento de la calidad (QA) interno ha efectuado una auditoría. Verificar si la revisión adecuada de los registros e informes fue realizada por la gerencia, donde se utiliza un software de gestión del cambio.

[51] Los datos volátiles son datos que han sido sobrescritos o cambiados en el tiempo, donde una instantánea no puede ser obtenida sin capturar de forma interactiva la información o mediante extractos de datos regularmente programados.

	Garantizar que el acceso a la biblioteca fuente de producción (por ejemplo: código fuente, configuraciones) esté limitado al personal de CM, y que el área de TI evite cambios no autorizados en el entorno operativo. Revisión de documentos, observar las prácticas para garantizar que los usuarios de la organización estén vinculados durante la prueba de los cambios para garantizar la exactitud. Garantizar que los cambios en el programa tengan un adecuado cierre de sesión por las partes pertinentes de la organización antes de ingresar a producción.
Tema 11 de auditoría: Procedimientos Auxiliares ¿De qué manera el área de TI garantiza que la organización puede volver a una versión anterior si es necesario?	
Criterios: Buenas prácticas de gestión del cambio: documentación sobre procedimientos y responsabilidades para la recuperación de áreas afectadas debido al impacto no deseado de los cambios.	
Información Requerida Procedimientos de gestión de cambio Documentación sobre pruebas e implementación de cambios Registros de cambios de configuración y recuperación de documentación Copia de seguridad y procedimientos de recuperación	**Métodos de Análisis** Revisión de la documentación, entrevista a los usuarios del negocio para verificar si los impactos imprevistos de los cambios o mejoras en la funcionalidad se han abordado como prioridad, de conformidad con los intereses de la organización.
Tema 12 de auditoría: Cambios de emergencia ¿Están controlados adecuadamente los cambios de emergencia cuando los procedimientos establecidos para definir, autorizar, probar y documentar los cambios no se puedan cumplir?	
Información Requerida Procedimientos de control de cambios de emergencia Documentación de cambios de emergencia que se han realizado durante el período auditado	**Métodos de Análisis** Revisión de los procedimientos de gestión de cambio para determinar si contienen una sección específica y un conjunto de procedimientos para controlar cambios de emergencia en el sistema. Solicitar un ejemplo de cambio de emergencia. Comparación con un procedimiento documentado. Verificar qué pruebas se han realizado, previo a la introducción en el entorno de producción. En caso de no existir un procedimiento documentado, preguntar cómo saben qué hacer y quién aprueba tales cambios. Examinar si los cambios de emergencia son aprobados por un miembro adecuado de la gerencia antes de pasar a producción.
Tema 13 de auditoría: Cambiar el cierre y la documentación ¿Se cumple con los procedimientos adecuados para la actualización de los sistemas asociados y la documentación de usuario con posterioridad a la implementación de un cambio?	
Criterios: Buenas prácticas de gestión de cambio (por ejemplo, COBIT 5-BAI dominio, ITIL sobre Soporte del Servicio)	

Información Requerida	**Métodos de Análisis**
Documentación del proceso de funcionalidades afectadas por el cambio Procedimientos establecidos para la documentación	Revisión de los documentos para garantizar la integridad y la coherencia de los cambios implementados. ¿Cumplieron los procedimientos operativos, información de configuración, documentación de aplicaciones, pantallas de ayuda y materiales de capacitación con el mismo procedimiento de gestión de cambio y fueron considerados como parte integral del cambio? Verificar si existe un período adecuado de conservación para la documentación de los cambios, para el sistema de cambio previo y posterior, y para la documentación del usuario. Verificar qué mecanismos existen para actualizar los procesos del negocio para cambios en el hardware o el software a fin de garantizar que se utiliza una funcionalidad nueva o mejorada.
Conclusión de la auditoría: Para ser completado por el auditor	

ANEXO V

MATRIZ SUGERIDA PARA LA AUDITORÍA DE SUBCONTRATACIÓN

<table>
<tr><th colspan="2">Política de subcontratación</th></tr>
<tr><td colspan="2">Objetivo de auditoría: Evaluar si la entidad cuenta con una política adecuada para la subcontratación.</td></tr>
<tr><td colspan="2">Tema 1 de auditoría: Elementos claves de la Política de Subcontratación
¿Cuenta la organización con una política de subcontratación?</td></tr>
<tr><td colspan="2">Criterios:
Política Organizacional sobre subcontratación.</td></tr>
<tr><td>Información Requerida

Documento de la Política

Proceso de aprobación para la subcontratación de una función/servicio

Lista de las funciones/servicios subcontratados

Lista de las funciones/servicios subcontratados con subcontratación parcial

Modalidad de servicio por parte del proveedor de servicios

Análisis de costos y beneficios de la subcontratación de una función/servicio

Lista de proveedores de servicios subcontratados con sus ubicaciones

Documentos relativos a la aprobación de funciones/servicios subcontratados

Estrategia para garantizar la continuidad en el caso que otra organización asuma el control del proveedor de servicios

Información sobre cualquier adquisición del proveedor de servicios

Documentos/informes de seguimiento</td><td>Método(s) de Análisis

Revisión de la política para garantizar que esté aprobada.

Revisión de la política para verificar (por ejemplo) que contenga información sobre los activos de la organización que pueden o no ser subcontratados y determine la lista de servicios/funciones que ésta puede subcontratar.

Revisión de los documentos de aprobación de la adquisición o de la subcontratación para garantizar que la gerencia senior esté involucrada en la aprobación.

Revisión de los documentos para evaluar que la organización haya identificado los riesgos conexos en relación con las diferentes modalidades de subcontratación y la ubicación del proveedor de los servicios subcontratados.

Revisión de la documentación para verificar si la organización está en conocimiento de los riesgos asociados con la posibilidad de la adquisición del proveedor de servicios.

Revisión de la documentación para verificar si la organización ha garantizado que la continuidad del negocio, los derechos a los datos, seguridad, titularidad y costo estén incluidos en el contrato de servicios que cubre el caso de la adquisición.

Revisión de la documentación para evaluar que la política incluya la identificación de los parámetros de monitoreo para las funciones subcontratadas y que requiera que éstos sean incluidos en el acuerdo de subcontratación.</td></tr>
<tr><td colspan="2">Conclusión de la auditoría:
Para ser completado por el auditor</td></tr>
</table>

Solicitud

Objetivo de auditoría: Evaluar si la entidad cuenta con una política sobre cómo gestionar una solicitud.

Tema 2 de auditoría: Política y Proceso de solicitud

- ¿Cuenta la organización con una política de adquisiciones?
- ¿Cuenta la organización con un proceso definido para la identificación y la selección del proveedor de servicios?
- ¿Cuenta la organización con un proceso para garantizar la inclusión de las necesidades de los usuarios en los Requerimientos de Nivel de Servicio/requerimientos contractuales?
- ¿Se toman las decisiones pertinentes en los niveles adecuados?

Criterios:

Disposiciones de la política de la organización sobre subcontratación y política en materia de contratación de servicios de TI que se ocupan de la solicitud y la adquisición.

Información Requerida	**Método(s) de Análisis**
Política de adquisición o equivalente	Revisión del documento para evaluar si la organización cuenta con una política de solicitud o adquisición.
Lista de leyes que regulan la adquisición y subcontratación	Revisión de la política para garantizar que ésta contenga disposiciones para la solicitud de datos de los subcontratistas si el contratista principal ha incluido subcontratistas como parte de la propuesta.
Proceso de selección para la identificación y selección de un proveedor de servicios	Revisión de la documentación para evaluar si la política sobre solicitud y adquisición cumple con las leyes sobre subcontratación y adquisición (verificar que haga referencia a las leyes y reglamentaciones vigentes).
Lista de funciones/servicios subcontratados y del proveedor de servicios	Revisión del proceso de selección para verificar el cumplimiento con la política de cada muestra de contratos o servicios subcontratados (revisar que el proceso de selección sea transparente, tenga criterios objetivos, que el equipo de selección esté constituido por personal que comprenda las necesidades, esté representado por personal contratado y legal, y consultar con los usuarios en caso de una aclaración, de ser necesario).
Requisitos del usuario para el servicio contratado o subcontratado	Garantizar que los requerimientos contractuales hayan sido aprobados por los usuarios e interesados pertinentes.
Contrato/Acuerdo de Nivel de Servicio	Reunión con la oficina de contrataciones para garantizar que el nivel apropiado de la administración haya aprobado la solicitud y el contrato.
Documentos de aprobación para la selección del proveedor de servicios	

Conclusión de la Auditoría:
Para ser completado por el auditor

Monitoreo del proveedor o contratista

Objetivo de auditoría: Evaluar si la organización está dirigiendo al contratista o al proveedor, y si toma las medidas apropiadas cuando el desempeño o la calidad no cumplen con lo establecido.

Tema 3 de auditoría: Dirección del contratista

- ¿Existe un contrato con el proveedor de servicios?
- ¿Se identifican y acuerdan los Niveles de Servicio por medio de un Acuerdo de Nivel de Servicio?
- ¿Existe un mecanismo de seguimiento de los servicios provistos?
- ¿Están los niveles de servicio garantizados por medio de este acuerdo?
- ¿Se toman las medidas adecuadas cuando no se cumplen las disposiciones del acuerdo de nivel de servicio?

Criterios:

Disposiciones/parámetros definidos en el Acuerdo de Nivel de Servicio y las medidas de seguimiento de la organización.

Información Requerida	Método(s) de Análisis
Contrato/Acuerdo de Nivel de Servicio Cronogramas aprobados, referencias, costos y otros parámetros técnicos que definen el producto o servicio adquirido o subcontratado Documentos/informes de seguimiento/actas de reuniones de las revisiones realizadas, medidas a tomar, indicaciones al proveedor (órdenes de trabajo, descripción de las tareas, etc.) Evaluación del impacto de las desviaciones Medidas a tomar o indicaciones al proveedor Informes de Acciones tomadas sobre las desviaciones de los niveles de servicio	Revisión de la documentación para evaluar si se ha establecido un acuerdo de nivel de servicio. Revisión de los informes de seguimiento presentados por el contratista para garantizar que contengan elementos que están incluidos en el contrato o en el SLA (costo, cronograma, desempeño, riesgo, estado, problemas y estado de las medidas tomadas con anterioridad o tareas realizadas). Revisión de los informes de seguimiento para identificar la deficiencia /desviación del servicio y evaluación del impacto debido a las deficiencias/desviaciones. Revisión de las notificaciones e informes sobre las medidas tomadas para verificar que éstas se adecuen al impacto en las disposiciones del negocio y contractuales.
Conclusión de la auditoría: Para ser completado por el auditor	

Derechos sobre los Datos

Objetivo de auditoría: Evaluar si los requerimientos de protección de datos de la organización están identificados y son parte de los requerimientos contractuales.

Tema 4 de auditoría: Protección de datos y gestión de datos

- ¿Están los derechos de protección de datos y acceso incorporados al contrato de servicio?
- ¿Están los datos apropiadamente definidos como para cubrir los datos productivos, así como los programas/software que los procesan, según corresponda?
- ¿Existe un mecanismo para garantizar que el proveedor de servicios adopta e implementa los requerimientos en cuanto a la protección de datos y la seguridad, de conformidad con el Acuerdo de Nivel de Servicio?

Criterios
Los requerimientos respecto de los derechos de acceso y protección de datos de la organización, de corresponder se aplican al contratista.

Información Requerida	Método(s) de Análisis
Requerimientos respecto de los derechos de acceso y Protección de Datos de la Organización Definición de los datos (para protección y derechos de acceso) Contrato con el proveedor de servicios Lista de los registros de acceso de datos del proveedor de servicios Informes de auditorías de terceros o propias con recomendaciones y seguimiento de las mismas Informes del monitoreo Correspondencia con el proveedor de servicios sobre el tema Informes de gestión de incidentes	Revisión de la documentación sobre la adecuación de los requerimientos para la protección de datos y derechos de acceso/definición de datos. Revisión de la documentación del contrato con el proveedor de servicios para verificar la incorporación de los requerimientos sobre protección de datos y derechos de acceso. Revisión de la documentación de los informes de auditoría de terceros/propias. Revisión de la documentación de los informes de la supervisión, correspondencia e informes de gestión de incidentes para evaluar las actividades de seguimiento de la organización. Revisión del acuerdo de no divulgación para verificar que toda la información relevante sea cubierta. Verificar si la divulgación de la información por parte de la entidad subcontratada ha sido autorizada.

Acuerdo de no divulgación con la entidad subcontratada Lista de la información divulgada por la entidad subcontratada a terceros, parte(s) no vinculada(s)	
Conclusión de la auditoría: Para ser completado por el auditor	

Proveedor de Servicios en el Exterior	
Objetivo de auditoría: Determinar si la organización cuenta con una estrategia de contratación de servicios a proveedores en el exterior.	
Tema 5 de auditoría: Gestión de Proveedores en el Exterior ¿Tiene la Organización conocimiento de la problemática relacionada con la subcontratación de entidades en el exterior al momento de hacerlo?	
Criterios: Disposiciones de la política de subcontratación relacionadas con la subcontratación de entidades en el exterior. Leyes del país que regulan las actividades del negocio con entidades en el exterior.	
Información Requerida	**Método(s) de Análisis**
Lista de leyes y reglamentos relacionados con la subcontratación de servicios Información sobre cualquier presencia en el país del proveedor de servicios Lista de oficinas de la organización ubicadas en el exterior Lista de leyes y reglamentos que regulan al proveedor de servicios en su país Acuerdo bilateral entre el país de la organización y el país del proveedor de servicios que facilite acuerdos de subcontratación Informes sobre el desempeño anterior del proveedor en cuanto a plazos de entrega y cuestiones de calidad Análisis de costos y beneficios del proveedor de servicios local y del exterior Contrato de subcontratación y Acuerdo de Nivel de Servicio Información sobre el monto del depósito/garantía financiera relacionada con el desempeño Lista de las desviaciones al Acuerdo del Nivel de Servicio y el contrato de subcontratación Informes de monitoreo y seguimiento de las medidas adoptadas por el proveedor de servicio respecto de las desviaciones	Revisión de la documentación para evaluar que la organización haya identificado los riesgos relacionados con la subcontratación de proveedores de servicios en el exterior. Revisión de la documentación para evaluar si el análisis del costo-beneficio abordó los riesgos relacionados con la subcontratación de proveedores de servicios en el exterior. Revisión de la documentación para evaluar que se ha llevado a cabo la verificación adecuada de antecedentes del proveedor de servicios. Revisión de la documentación para evaluar la existencia de un sistema sólido para garantizar el cumplimiento del Acuerdo de Nivel de Servicio y el contrato de subcontratación. Revisión de la documentación para evaluar que el seguimiento de cualquier desviación del Acuerdo de Nivel de Servicio y del contrato se realiza oportunamente, garantizando un tiempo de inactividad y pérdida mínimo para la organización.

Conclusión de la auditoría: Para ser completado por el auditor

Mantener el Conocimiento del Negocio/Titularidad de los procesos del negocio

Objetivo de auditoría: Evaluar si la entidad mantiene el conocimiento y la titularidad de los procesos del negocio.

Tema 6 de auditoría: Política sobre la titularidad del conocimiento y procesos del negocio.

- ¿Está bien delineada y documentada la titularidad de los procesos del negocio?
- ¿Se garantiza que no se producirá una pérdida de conocimiento del negocio debido a la subcontratación?
- ¿Existe capacidad para llevar a cabo internamente los servicios de subcontratación?
- ¿Se puede garantizar la continuidad del negocio si el proveedor no puede prestar los servicios en el futuro?

Criterios:

Las Organizaciones mantienen el conocimiento del negocio y son capaces de continuar con sus operaciones internamente para la función esencial de la misión, si los contratistas o proveedores son incapaces de prestar el servicio.

Conservar la titularidad de los procesos del negocio.

Mantener el conocimiento del negocio.

Desarrollo en relación con la continuidad del negocio ante la falta de prestación del servicio por parte del proveedor en cualquier momento.

Información Requerida	**Método(s) de Análisis**
Identificación de los procesos del negocio y habilidades esenciales que se deben mantener internamente. Documentación de los procesos del negocio. Documento detallado del diseño del sistema de servicios de subcontratación de la organización. Lista de capacitación del personal en los procesos del negocio, diseño de sistemas, datos, software de aplicación. Informes de incidentes/correspondencia relacionados con la interrupción del servicio/disputa con el proveedor de servicios, incluidas aquellas relacionadas con la titularidad del sistema /datos. Actas de las reuniones con el contratista.	Revisión de la documentación para evaluar si la organización mantiene la titularidad de los procesos, datos y software de aplicación por medio de disposiciones adecuadas contenidas en el contrato. Revisión de la documentación para evaluar que el conocimiento del negocio en términos de datos, software de aplicación, diseño de sistemas esté bien documentado y que el personal se mantenga actualizado respecto de estos temas periódicamente a través de la capacitación, etc. Revisión de la documentación para evaluar que la organización y su personal estén involucrados en las actualizaciones del sistema realizadas por la entidad subcontratada y que la documentación detallada sobre las actualizaciones al sistema sea proporcionada a la organización. Revisión de la documentación para evaluar que no existan incidentes o disputas con el proveedor de servicios con respecto a la titularidad del sistema y los datos. Revisión de las actas de la reunión con el contratista para garantizar que, si existe un riesgo de nivel elevado, se haga un seguimiento y se aborde el mismo en forma conjunta para garantizar la continuidad de las operaciones.

Conclusión de la auditoría: Para ser completado por el auditor

Control y gestión de costos

Objetivo de auditoría: Evaluar si la organización ha garantizado el criterio de economía durante la duración del contrato de subcontratación.

Tema 7 de auditoría: Evaluación costo-beneficio

- ¿Se identificaron todos los costos (incluidos los costos futuros) de la subcontratación?
- ¿Se ha realizado un análisis adecuado de costo-beneficio y se ha elegido la mejor opción?
- ¿Existen responsabilidades específicas en la organización respecto de la subcontratación y están incorporados los elementos de costos /impactos críticos?
- ¿Se cargarán a la entidad los costos adicionales o incremento de costos?

Criterios:
El análisis costo-beneficio es realista y constituye la base sobre la cual se gestiona y controla el programa.

Información Requerida	**Método(s) de Análisis**
Análisis de costo-beneficio inicial. Costo estimado del contrato de subcontratación. Proceso de selección del proveedor de servicios en relación con el componente costo. Documentos del proceso de aprobación relacionados con la selección. Situaciones de costos adicionales/incremento de los costos por parte del proveedor de servicios. Acuerdo de Nivel de Servicio y contrato Informes de seguimiento con respecto a la función/actividad específica para la cual se procura el incremento/costo adicional que se busca. Documentos de la actuación respecto de solicitudes de costos adicionales/incrementos de costos por parte del proveedor de servicios.	Revisión de la documentación para evaluar que todos los costos hayan sido identificados por la organización, revisados y aprobados por los interesados pertinentes. Revisión de la documentación del proceso de selección y aprobación. Revisión de la documentación para evaluar que todos los costos se reflejen en el contrato y que no haya costos ocultos, incluido cualquier costo futuro. Revisar que todos los costos estén sujetos al análisis de costo-beneficio previo al compromiso por parte de la organización. Revisión y comparación de los gastos estimados vs. los gastos reales en el contrato. Revisión del gasto en relación con el presupuesto disponible. Revisión del desempeño del proveedor de servicios sobre la actividad/funciones específicas para las que se solicita la modificación en el costo por medio de informes de seguimiento y evaluación de la necesidad de tal modificación. Revisión de las acciones de la organización respecto de los costos adicionales/incremento de los costos por parte del proveedor de servicios.

Conclusión de la auditoría:
Para ser completado por el auditor

Acuerdos de Nivel de Servicio

Objetivo de auditoría: Evaluar si la entidad ha elaborado el Acuerdo de Nivel de Servicio detallando todos sus requerimientos y está monitoreando activamente al proveedor en relación con el acuerdo.

Tema 8 de auditoría: Adecuación del Acuerdo de Nivel de Servicio

- ¿Es un acuerdo de nivel de servicio aceptado entre la organización y el proveedor de servicios?
- ¿Está suficientemente detallado el acuerdo de nivel de servicio para identificar todas las funciones y responsabilidades entre la organización y el proveedor de servicios?
- ¿Se ha implementado con rigurosidad el acuerdo de nivel de servicio?
- ¿Cuenta la organización con un mecanismo para monitorear la implementación del acuerdo de nivel de servicio?
- ¿Existe un mecanismo disponible para abordar las excepciones al acuerdo de nivel de servicio?

Criterios:
El acuerdo de nivel de servicio es la base para el seguimiento y control del contratista o proveedor en relación a los requerimientos técnicos y de otro tipo.

Información Requerida	**Método(s) de Análisis**
Acuerdo de nivel de servicio o contrato	Revisión de la documentación para evaluar que todos los requerimientos de los usuarios se traducen en requerimientos de nivel de servicios.
Requerimientos técnicos y de otro tipo (lista de servicios a ser realizados por el proveedor)	Revisión de la documentación para evaluar que las funciones y responsabilidades de la organización y del proveedor de servicio sean claramente identificadas y definidas.
Lista de las responsabilidades de la organización y del proveedor	
Referencia para los servicios que se medirán, período de medición, duración, ubicación y cronogramas de presentación de informes (índices de defectos, tiempo de respuesta, horario del personal de atención al cliente, etc.).	Revisión de la documentación para evaluar que los parámetros para los niveles de desempeño sean claramente identificados e incluidos en el acuerdo de nivel de servicio.
	Revisión de la documentación para evaluar que se ha establecido y acordado el mecanismo de monitoreo de nivel de servicio entre la organización y el proveedor de servicios.
Informes periódicos del estado de desempeño de los proveedores	Revisión de los informes de estado de los proveedores para evaluar que los parámetros en el SLA son informados por parte del contratista y revisados por personal pertinente dentro de la organización.
	Evaluación del cumplimiento de los parámetros técnicos y referencias del SLA.
	Verificación de las medidas adoptadas por la organización en relación a las desviaciones al acuerdo de nivel de servicio.

Conclusión de la auditoría:
Para ser completado por el auditor

Seguridad

Objetivo de auditoría: Evaluar si se abordan y cumplen los requisitos de seguridad en la subcontratación.

Tema 9 de auditoría: Respuesta a los requerimientos de Seguridad

- ¿Ha identificado la organización los requisitos de seguridad con respecto a la subcontratación?
- ¿Existe un mecanismo que garantice que los requisitos de seguridad de la organización son abordados por el proveedor de servicios?
- ¿Cuenta la organización con un mecanismo para monitorear el cumplimiento de los requisitos de seguridad por parte del proveedor de servicios?

Criterios:
Los requisitos de seguridad pertinentes a la organización se aplican al contratista según corresponda.

Información Requerida	Método(s) de Análisis
Política de seguridad de la organización. Contrato de subcontratación. Acuerdo del Nivel de Servicio. Inventario de datos, hardware y software de aplicación con el proveedor de servicios. Inventario de las copias de seguridad de archivos de datos y software de aplicación con el proveedor de servicios. Registros de control de acceso de los archivos de datos, software de aplicación, así como hardware en la ubicación subcontratada. Plan de seguridad para el sitio de copia de seguridad y para el sitio de recuperación ante desastres. Informes de seguimiento con respecto a problemas de seguridad. Correspondencia entre la organización y el proveedor de servicios con respecto a las cuestiones de seguridad.	Revisión de la documentación para evaluar que los requerimientos de seguridad han sido identificados por la organización e incorporados al contrato de subcontratación o SLA. Verificar si la organización cuenta con el inventario de los archivos de datos, software de aplicación. Verificar que la organización controle/ tenga conocimiento que el estado de los archivos de datos, software de aplicación y hardware se conserven durante el proceso de copia de seguridad y recuperación de datos llevado a cabo por la entidad subcontratada. Verificar si la organización cuenta con la garantía de autorización de cualquier cambio en los datos, software de aplicación y hardware de la entidad subcontratada. Verificar si la organización cuenta con una garantía en cuanto al acceso a los datos, aplicaciones de software y hardware en la ubicación subcontratada mediante un estudio de los registros de acceso (físico y lógico). Verificar si la organización cuenta con la garantía de mecanismos de seguridad establecidos por el proveedor de servicios. Verificar si la organización recibe regularmente informes y actas sobre la información en los reportes de monitoreo.
Conclusión de la Auditoría: Para ser completado por el auditor	

Copia de seguridad y recuperación ante desastres para los servicios subcontratados

Objetivo de auditoría: Evaluar si los servicios subcontratados cumplen contractualmente con los planes de continuidad del negocio y de recuperación ante desastres.

Tema 10 de auditoría: Procedimientos para la copia de seguridad y recuperación.
¿Cumple el proveedor con los requerimientos del contrato o SLA para BCP y DRP?

Criterios:
Acuerdo de nivel de servicio o contractual respecto del BCP y DRP con el proveedor.

Información Requerida	Método(s) de Análisis
Contrato o SLA. Auditoría Interna o certificación de terceros de la disponibilidad del BCP y DRP del proveedor. Informes periódicos de las pruebas o actualizaciones del BCP/DRP.	Revisión de un contrato o SLA para asegurar que el proveedor esté obligado a garantizar el BCP y DRP en los datos, aplicaciones y servicios subcontratados. Revisión del contrato o SLA para garantizar que el proveedor proporcione los informes de auditoría interna o independiente que confirman que las actividades de BCP/DRP se han implementado y que el proveedor prueba sus procedimientos periódicamente. Revisión de los informes presentados por el proveedor para garantizar que las pruebas se hayan realizado de acuerdo con las condiciones del contrato y/o SLA.

	Revisión de los informes periódicos para garantizar que los procedimientos hayan sido actualizados, si es necesario.
Conclusión de la auditoría: Para ser completado por el auditor	

ANEXO VI

MATRIZ SUGERIDA PARA LA AUDITORÍA DEL BCP/DRP

Política de Continuidad del Negocio	
Objetivo de auditoría: Evaluar si existe una política efectiva de continuidad del negocio en la organización.	
Tema 1 de auditoría: Política ¿Cuenta la organización con un plan de contingencia y una política de continuidad del negocio?	
Criterios: La organización cuenta con un plan de contingencia publicado, aprobado y adoptado, y una política que cubre de forma exhaustiva todas las áreas de operaciones de contingencia e identifica claramente los requerimientos de capacitación y cronogramas de prueba.	
Información Requerida	**Método(s) de Análisis**
Documento de Política de Continuidad del Negocio. Documento de Política de TI. Proceso de aprobación para el establecimiento de los objetivos de la política del negocio. Correspondencia y actas de las reuniones relacionadas con la continuidad del negocio.	Revisión de la documentación para evaluar que la política sea coherente con las políticas generales de TI de la organización. Revisión de la documentación para evaluar que la política aborda los requerimientos de continuidad del negocio mediante la definición de los objetivos de contingencia de la organización, el marco organizacional y las responsabilidades para la planificación de contingencias. Revisión o entrevista al personal para determinar con qué frecuencia se actualiza la política si se modifican las condiciones. Revisión de la política para determinar quién la aprobó y cuándo fue su última distribución/ Entrevista a una muestra de usuarios del negocio para evaluar si la política ha sido suficientemente difundida dentro de la organización.
Conclusión de la Auditoría: Para ser completado por el auditor	

Organización de la Función de Continuidad del Negocio	
Objetivo de auditoría: Evaluar si existe un equipo adecuado para resguardar la continuidad del negocio	
Tema 2 de auditoría: Función de Continuidad del Negocio ¿Existe un equipo de continuidad del negocio o una función equivalente?	
Criterios: Cobertura de todas las áreas críticas de la organización en el equipo. Requerimientos en cuanto a roles y responsabilidades para los miembros del equipo.	
Información Requerida	**Método(s) de Análisis**
Organigrama de la organización. Organigrama del equipo de continuidad del negocio. Descripción del rol/responsabilidades de los	Revisión de la documentación/entrevista al personal pertinente para evaluar que todas las áreas críticas de la organización estén representadas en el equipo de continuidad del negocio o su equivalente. Revisión de la documentación para evaluar si existe una titularidad y asignación adecuada de la responsabilidad de la continuidad del negocio a nivel de la gerencia senior. Por ejemplo, ¿ha identificado la gerencia el nivel

miembros del equipo de continuidad del negocio. Correspondencia/actas de las reuniones sobre los asuntos relacionados con la continuidad del negocio. Plan de Continuidad del Negocio.	y la urgencia de la recuperación, y se refleja esto en la política? Revisión de la documentación para evaluar que los principales departamentos hayan designado miembros del equipo de recuperación ante desastres y que sus funciones sean claramente establecidas. Entrevista a una muestra del personal del equipo de continuidad del negocio/equivalente para evaluar que está en conocimiento de sus roles para la continuidad del negocio en cada unidad/departamento de la organización.
Conclusión de la auditoría: Para ser completado por el auditor	

Evaluación del Impacto del Negocio	
Objetivo de auditoría: Verificar si la evaluación de impacto del negocio y la evaluación de riesgos se han completado, y si existe un sistema de gestión de riesgos.	
Tema 3 de auditoría: Evaluación de Riesgo ¿Se han llevado a cabo análisis de impacto del negocio y evaluaciones de riesgo, y se han identificado y priorizado datos críticos, software de aplicaciones, operaciones y recursos?	
Criterios: Marco de Gestión del Riesgo de la organización o equivalente. Política de Continuidad del Negocio o equivalente. Finalización de la evaluación del impacto del negocio e identificación de datos críticos, software de aplicación, operaciones y recursos.	
Información Requerida	**Método(s) de Análisis**
Informe(s) de Evaluación de Riesgo. Informe(s) de Evaluación del impacto del Negocio. Lista de datos críticos, software de aplicación, operaciones y recursos para cada función. Lista de riesgos residuales. Lista de interesados involucrados. Revisión de informe(s) sobre la evaluación de riesgo y el impacto en el negocio. Política/marco de la evaluación de riesgo de la organización. Actas de las reuniones sobre evaluación de riesgo y evaluación del impacto en el negocio.	Revisión de la documentación para evaluar que se ha llevado a cabo la evaluación de riesgo, y que se han identificado las posibles amenazas y sus impactos. Revisión de la documentación para evaluar que se han considerado todas las áreas funcionales en la evaluación de riesgo y la evaluación del impacto. Revisión de la documentación para evaluar que el análisis de impacto haya considerado el impacto provocado por cualquier interrupción en relación con el tiempo y otros recursos y sistemas conexos. Revisión de la documentación para evaluar que la decisión sobre los riesgos residuales se haya tomado en un nivel apropiado. Revisión de la documentación para evaluar que la organización haya determinado los RTO (objetivos de tiempos de recuperación) y RPO (Objetivos de puntos de recuperación) para cada aplicación crítica. Revisión de la documentación para evaluar que los RTO y RPO sean prácticos y razonables para cada aplicación y línea del negocio o función. Revisión de la documentación para evaluar la participación/aprobación de la gerencia senior. Revisión de la documentación para evaluar que los interesados pertinentes hayan estado involucrados en la identificación de riesgos y evaluación del impacto.
Conclusión de la auditoría: Para ser completado por el auditor	
Tema 4 de auditoría: Gestión de Riesgo	

¿Existe un proceso de gestión de riesgo (que incluya la mitigación y el seguimiento, etc.) y se han establecido prioridades en el procesamiento de emergencia?	
Criterios: Cobertura del Proceso de gestión de riesgo en relación con la evaluación de riesgo y evaluación de impacto en el negocio. Los riesgos y emergencias son abordados inmediatamente de acuerdo con los parámetros acordados por la organización.	
Información Requerida	**Método(s) de Análisis**
Documento del proceso de Gestión de Riesgo. Informe(s) de la Evaluación de Riesgo y Evaluación del Impacto en el Negocio. Lista de todo el personal pertinente, miembros del equipo de BCP que incluya funciones y responsabilidades. Lista de elementos prioritarios para el proceso de emergencia. Lista de los riesgos residuales identificados. Lista de las instancias del proceso de emergencia que ha sido alegado. Proceso de emergencia/informes de respuesta.	Revisión de la documentación para evaluar que el proceso de gestión de riesgo aborde todos los temas de máxima prioridad. Entrevista y revisión de la documentación para evaluar que todo el personal pertinente, incluida la gerencia senior tenga conocimiento de sus roles y responsabilidades, y las lleven a cabo. Revisión de la documentación para evaluar que los riesgos residuales no tengan impacto significativo en la organización. Revisión y observación de la documentación para evaluar que los casos de emergencia se gestionen adecuadamente. Revisión de la documentación para evaluar el impacto de la emergencia. Revisión de las actas de las reuniones o lista de los riesgos para determinar que éstos hayan sido identificados, las actividades de mitigación hayan sido definidas, y que los riesgos se han supervisado periódicamente y su estado actualizado.
Conclusión de la auditoría: Para ser completado por el auditor	

Plan de Recuperación ante Desastres	
Objetivo de auditoría: Evaluar si el Plan de Continuidad del Negocio incluye planes de recuperación y copias de seguridad para el hardware, datos, software de aplicación y centro de procesamiento de datos (recuperación) y si han sido implementados adecuadamente.	
Tema 5 de auditoría: Procedimiento de Copia de Seguridad ¿Se han diseñado e implementado efectivamente los procedimientos de copias de seguridad de programas y datos?	
Criterios: Se determine la criticidad de las aplicaciones y funciones de conformidad con la Evaluación de Impacto del Negocio de la organización. Se determine la periodicidad de las copias de seguridad. Se documenten los planes de recuperación y copia de seguridad.	
Información Requerida	**Método(s) de Análisis**
Planes de copia de seguridad y procedimientos para el hardware, datos, software de aplicación. Registros de copia de seguridad/ Registros de las versiones. Roles y responsabilidades en	Revisión de la documentación para evaluar que el plan de copia de seguridad incluya el hardware, datos, software de aplicación esenciales. Revisión de la documentación para evaluar que los procedimientos de copia de seguridad detallados hayan sido diseñados. Revisión de la documentación para evaluar que el plan de copia de seguridad sea implementado adecuadamente.

relación con la copia de seguridad. Lista de ubicaciones para almacenamiento y periodicidad. Cronograma de conservación. Disposiciones de seguridad para la ubicación de copia de seguridad. Registro de desastres. Roles y responsabilidades en relación con las actividades de recuperación. Registros de capacitación del personal responsable. Evaluación del impacto de los desastres. Informe sobre las actividades de recuperación ante desastres.	Análisis de los registros para evaluar que la copia de seguridad sea efectuada a intervalos determinados y conservada por un período de tiempo específico. Verificar que la versión correcta de copia de seguridad esté disponible. Revisión de la documentación para evaluar la pertinencia de la ubicación de las copias de seguridad y el modo de transporte de los archivos de respaldo, etcétera a la ubicación de la copia de seguridad. Verificar que la seguridad, lógica o física, sea la adecuada para la ubicación de la copia de seguridad. Verificar que los archivos de respaldo puedan ser utilizados para la recuperación. Revisión de la documentación para evaluar que los procedimientos de copia de seguridad sean implementados, minimizando la pérdida de tiempo y recursos. Revisión de la documentación para evaluar que el procedimiento detallado de recuperación haya sido diseñado e incluya un reajuste de los parámetros del sistema, instalación de parches, establecimiento de los ajustes de configuración, disponibilidad de la documentación del sistema y procedimientos operativos, reinstalación de la aplicación y del software del sistema, disponibilidad de la copia de seguridad más reciente y prueba del sistema. Revisión de la documentación para evaluar que los procedimientos de recuperación sean implementados, minimizando la pérdida de tiempo y recursos. Revisión de la documentación/entrevista al personal para evaluar que el personal pertinente haya sido capacitado en los procedimientos de copia de seguridad y recuperación.
Conclusión de la auditoría: Para ser completado por el auditor	

Control del entorno	
Objetivo de auditoría: Evaluar si la organización cuenta con un adecuado control del ambiente físico en el que se resguardan las copias de seguridad.	
Tema 6 de auditoría: Mecanismos de Control ¿Se ha diseñado y puesto en práctica un mecanismo de control del ambiente físico en el que se resguardan de las copias de seguridad?	
Criterios: Parámetros de control del ambiente físico definidos en el procedimiento de control del ambiente físico.	
Información Requerida Programa de control del entorno. Lista de posibles peligros en el entorno identificados durante la evaluación de riesgo, junto con las ubicaciones (documento de evaluación de riesgo).	**Método(s) de Análisis** Revisión de la documentación, observación y pasos a seguir de los procedimientos para evaluar que: • La fuente de alimentación ininterrumpida esté disponible. • El sistema adecuado de protección contra incendios se haya puesto en marcha. • La humedad, temperatura y tensión estén controladas dentro de los límites.

Lista de medidas de mitigación tomadas en el entorno.	• El sistema adecuado de protección contra inundaciones sea puesto en marcha. • Los controles del entorno cumplan con las regulaciones. • Las medidas de control del entorno sean transmitidas y cumplidas por todo el personal involucrado.
Conclusión de auditoría: Para ser completado por el auditor	

Documentación	
Objetivo de auditoría: El plan de continuidad del negocio está adecuadamente documentado para llevar a cabo actividades temporarias y efectivas del negocio y procedimientos de recuperación después de una interrupción de la actividad.	
Tema 7 de auditoría: Planes documentados para los procedimientos de copia de seguridad y recuperación, roles y responsabilidades. ¿Cuenta la organización con un plan de recuperación ante desastres documentado, rápidamente accesible para resguardar y restaurar?	
Criterios: Disponibilidad y vigencia del plan de continuidad del negocio y plan de recuperación ante desastres.	
Información requerida	**Método(s) de Análisis**
Plan de continuidad del negocio. Plan de recuperación ante desastres Versión/vigencia del plan de continuidad del negocio y el plan de recuperación ante desastres. Lista de distribución de los planes de continuidad del negocio y de recuperación ante desastres a todos los involucrados.	Revisión de la documentación para evaluar la vigencia del plan de continuidad del negocio. Revisión de la documentación para evaluar la vigencia del plan de recuperación ante desastres. Verificar si la última versión del plan de continuidad del negocio y el plan de recuperación ante desastres ha sido comunicada a todos los involucrados. Determinar si los documentos del plan de recuperación ante desastres y de continuidad del negocio se encuentran disponibles en la ubicación remota en caso de desastre. Verificar si las funciones y responsabilidades del equipo o personal conexo de recuperación ante desastres y copias de seguridad, están claramente enumeradas. Entrevista a una muestra de personal para evaluar si se conocen y comprenden los procedimientos de recuperación ante desastres.
Conclusión de la auditoría: Para ser completado por el auditor	

Prueba del BCP/DRP
Objetivo de auditoría: Evaluar si los procedimientos de recuperación ante desastres y de continuidad del negocio han sido examinados.
Tema 8 de auditoría: Pruebas ¿Ha examinado la organización sus procedimientos de BC y DR, y qué cambios (si los hubo) se han efectuado como resultado de la prueba?
Criterios: La organización debe examinar sus procedimientos documentados de BCP y DRP a través de ejercicios o maquetas para garantizar que operan en condiciones reales. El personal involucrado en garantizar la continuidad debe tener conocimiento de sus roles.

Información Requerida	Método(s) de Análisis
Procedimientos de BC y DR y procedimientos de prueba. Lista de elementos en base a los cuales se debe examinar el plan de continuidad del negocio/recuperación ante desastres. Frecuencia de las pruebas del plan de continuidad del negocio y plan de recuperación ante desastres. Lista de las pruebas llevadas a cabo. Lista de criterios de prueba como RTO y RPO, etc. Lista de los métodos de prueba empleados. Resultado de la prueba y medidas adoptadas o recomendaciones de la prueba. Medidas de seguimiento para los resultados de la prueba.	Revisión de la documentación para determinar si todos los elementos pertinentes están cubiertos para la prueba. Revisión de la documentación para determinar si las pruebas se llevan a cabo oportunamente a intervalos adecuados. Revisión de la documentación para determinar que las pruebas hayan sido llevadas a cabo en relación con los criterios identificados. Revisión de la documentación para determinar que las pruebas se hayan realizado utilizando métodos de prueba apropiados. Revisión de la documentación para determinar que las recomendaciones hayan sido transmitidas a las autoridades correspondientes para su seguimiento. Revisión de la documentación para determinar que las recomendaciones de las pruebas hayan sido debidamente cumplidas y el plan de continuidad del negocio o el plan de recuperación ante desastres hayan sido adecuadamente actualizados.
Conclusión de la auditoría: Para ser completado por el auditor	

Seguridad	
Objetivo de auditoría: Evaluar si el plan de continuidad del negocio o el plan de recuperación ante desastres garantiza la seguridad de los datos, las aplicaciones, el hardware y el centro de procesamiento de datos.	
Tema 9 de auditoría: Eficiencia de los Indicadores de Seguridad Determinar si los datos, software de aplicación, hardware y centros de procesamiento de datos están asegurados adecuadamente durante el procedimiento de copia de seguridad para la recuperación ante desastres.	
Criterios: Referencias de seguridad para la organización similares a los procedimientos establecidos en la política de seguridad de TI y los planes de recuperación ante desastres.	
Información Requerida	**Método(s) de Análisis**
Inventario de datos, hardware y software de aplicación. Inventario de archivos de datos de respaldo y software de aplicación. Registros de control de acceso a los archivos de datos, hardware y software de aplicación. Plan de seguridad para la ubicación de las copias de seguridad y de recuperación ante desastres.	Verificar si se conservan la cantidad y el estado de los archivos de datos, hardware y software de aplicación durante el proceso de copia de seguridad y de recuperación de datos. Verificar si los datos, hardware y software de aplicación han sufrido algún cambio durante el proceso de copia de seguridad o de recuperación ante desastres, a través del examen de los totales de los controles sobre el número de registros y el tamaño de los archivos relacionados con los datos y software de aplicación. Verificar si ha habido alguna violación a la seguridad a través del examen de los registros de control de acceso (físico y lógico).
Conclusión de la auditoría: Para ser completado por el auditor	

Copia de seguridad y recuperación ante desastres para los servicios subcontratados	
Objetivo de auditoría: Evaluar si los servicios subcontratados se ajustan a los planes de continuidad del negocio y de recuperación ante desastres.	
Tema 10 de auditoría: Determinar si el proveedor de los servicios subcontratados garantiza que se adopte el plan de continuidad del negocio y el plan de recuperación ante desastres de la organización.	
Criterios: Referencias de seguridad para la organización similares a los procedimientos establecidos en la política de seguridad de TI y el plan de recuperación ante desastres.	
Información Requerida	**Método(s) de Análisis**
Inventario de datos, software de aplicación y hardware de la organización con la entidad subcontratada. Inventario de archivos de datos de respaldo y software de aplicación de la organización con la entidad subcontratada. Registro de control de acceso de los archivos de datos, software de aplicación y hardware con la entidad subcontratada. Resultados de las pruebas del plan de copia de seguridad y del plan de recuperación ante desastres en la ubicación de la entidad subcontratada. Plan de seguridad para la ubicación de la copia de seguridad y ubicación de recuperación ante desastres en la entidad subcontratada. Plan de seguridad para el sitio de copia de seguridad y el sitio de recuperación ante desastres en la ubicación de la entidad subcontratada. Estrategia para garantizar la continuidad en caso que otra organización adquiera al proveedor de servicios. Información sobre cualquier adquisición del proveedor de servicios.	Verificar si la organización controla que la cantidad y el estado de los archivos de datos, software de aplicación y hardware se preservan durante los procesos de copia de seguridad y de recuperación de datos en la entidad subcontratada. Verificar si la organización controla si los datos, el software de aplicación y hardware han sufrido algún cambio durante los procesos de copia de seguridad o de recuperación ante desastres a través del examen de los totales de control sobre la cantidad de registros y el tamaño de los archivos relacionados con los datos y software de aplicación en la entidad subcontratada. Verificar si la organización controla si ha habido alguna violación de seguridad a través del examen de los registros de control de acceso (físico y lógico). Verificar si la organización controla si se garantiza la prueba de copia de seguridad y de la recuperación ante desastres en la entidad subcontratada. Verificar si la organización tiene conocimiento de los riesgos asociados con la posibilidad de adquisición del proveedor de servicios. Verificar si la organización ha garantizado que la Continuidad del Negocio está incorporada al acuerdo del servicio.
Conclusión de la auditoría: Para ser completado por el auditor	

ANEXO VII

MATRIZ SUGERIDA PARA LA AUDITORÍA SOBRE SEGURIDAD DE LA INFORMACIÓN

<table>
<tr><th colspan="2">Evaluación de Riesgos</th></tr>
<tr><td colspan="2">Objetivo de auditoría: Garantizar que todos los riesgos relativos a la seguridad de la información hayan sido identificados y que se haya implementado una estrategia adecuada de mitigación.</td></tr>
<tr><td colspan="2">Tema 1 de auditoría: Mecanismo de Evaluación
¿Cuenta la organización con un eficaz y bien documentado mecanismo de evaluación de riesgos respecto a la seguridad de la información?</td></tr>
<tr><td colspan="2">Criterios:
La política interna, los procedimientos o regulaciones muestran la disposición de la organización para enfrentar los riesgos críticos.</td></tr>
<tr><td>Información Requerida

Política de Seguridad de SI.

Procedimientos formales para la gestión de riesgo.

Documentación sobre la configuración del sistema</td><td>Método(s) de Análisis

Análisis de la política de gestión de riesgo, documentos de evaluación de riesgos y entrevista a la gerencia senior y a nivel operativo para:

• Comprender el verdadero papel de la organización en los procedimientos de evaluación de riesgo.
• Identificar quiénes participan en la evaluación de riesgo.
• Conocer los costos operativos del mecanismo.
• Verificar si se lleva a cabo y se documenta la evaluación de riesgo en forma periódica, o siempre que las condiciones se modifican.
• Verificar si la configuración actual del sistema está documentada, incluidos los enlaces a otros sistemas.
• Verificar si la documentación describe los riesgos clave para el sistema, el negocio y la infraestructura de la organización.

En caso de ausencia de procedimientos formales y de documentos sobre evaluación de riesgo, no desestimar controles que se encuentran incorporados a los procedimientos operativos de la organización –verificar si el mecanismo de control compensatorio que se encuentra incorporado a las operaciones es eficaz. Esto se puede observar mediante el análisis de una muestra de las operaciones, etcétera.</td></tr>
<tr><td colspan="2">Tema 2 de auditoría: Cobertura
¿Cubre la evaluación de riesgos los principales riesgos internos y externos? ¿Se evalúan los posibles efectos e impacto de las violaciones a la Seguridad de la Información?</td></tr>
<tr><td colspan="2">Criterios:
Todos los riesgos significativos se identifican y evalúan correctamente (buenas prácticas en la evaluación de riesgos).[52]</td></tr>
</table>

[52] ISO 27005 gestión de riesgo de seguridad de la información, ISACA Marco de Riesgo de TI, COSO Marco de Gestión de Riesgos de la Organización.

Información Requerida	Método(s) de Análisis
Evaluaciones de Riesgo documentadas. Registro de riesgos. Informes de manejo de incidentes.	Revisar los documentos para verificar si la evaluación de riesgo realizada por la organización auditada se basó en información suficientemente completa. Verificar si los datos e informes fueron obtenidos del sistema de gestión de incidentes de la organización. (Fundamente su análisis con resultados de los Métodos de Análisis de las operaciones de TI enfocados en el sistema de gestión de incidentes, especialmente, si el manejo del incidente de seguridad de la información se realiza en un sistema separado del sistema de gestión de incidentes generales). ***Prueba de Validación 1:*** pistas de auditoría de seguridad: Determinar si las pistas de auditoría de seguridad cubren la identificación del usuario (ID), el tipo de evento, datos y tiempo, indicador de éxito o fracaso, origen del evento, y la identidad o el nombre del elemento afectado. Entrevista al personal pertinente para verificar si se realiza una reevaluación estándar del riesgo cada vez que la organización planea lanzar nuevos sistemas de información, actualizaciones y nuevas versiones. Verificar que el diseño de la evaluación del riesgo sea completo, relevante, oportuno y cuantificable. Verificar si las consecuencias de inoperatividad de la infraestructura son tenidas en cuenta al asignar categorías de riesgo. Verificar los documentos para comprobar si se realiza un análisis de impacto en el negocio como consecuencia del hecho que la información crítica no esté disponible, se deteriore, se encuentre inapropiadamente afectada o se pierda. Revisar los informes de respuesta a incidentes y documentos/registros de riesgo anteriores para examinar si la metodología de evaluación de riesgo ha sido eficaz en el pasado.
Tema 3 de auditoría: Mitigación ¿Se mitigan los riesgos importantes de manera eficiente y eficaz?	
Criterios: Se han implementado prácticas adecuadas de mitigación de riesgo.	
Información Requerida	**Método(s) de Análisis**
Informes de manejo de problemas/incidentes. Informes de actividad periódicos.	Revisión de los informes de manejo de incidentes y verificar si se han implementado procedimientos apropiados para prevenir, detectar y controlar los riesgos de seguridad identificados en el documento de evaluación de riesgo. En organizaciones que no utilizan mecanismos de evaluación de riesgo bien definidos, identificar qué control de compensación existe. Analizar si ha ocurrido algún incidente de seguridad grave, que representa un riesgo que podría haberse mitigado de manera más adecuada utilizando un mecanismo de evaluación de riesgo que funcione correctamente, en comparación con los controles de compensación existentes. Tener en cuenta que, en algunos casos, los informes sobre problemas/incidentes pueden estar incompletos. Sin embargo, los incidentes relevantes pueden indicarse directamente o indirectamente en otros documentos, por ejemplo, en informes anuales de actividades y otros informes periódicos.
Conclusión de la auditoría: Para ser completado por el auditor	

Política de Seguridad de la Información

Objetivo de auditoría: Evaluar si existe orientación estratégica y respaldo adecuados respecto a la seguridad de la información en términos de una política de seguridad, su cobertura, la concientización y su cumplimiento por parte de toda la organización.

Tema 4 de auditoría: Política de Seguridad de la Información

¿Cuenta la organización con una Política de Seguridad de la Información? ¿Está correctamente implementada y documentada? ¿Conforma un plan de seguridad de TI coherente y sólido?

Criterios:

La política de seguridad de la información de la organización cubre todos los riesgos operativos y es capaz de proteger razonablemente los activos de información importantes del negocio contra pérdida, daño o abuso.[53]

Información Requerida	**Método(s) de Análisis**
Estrategia de TI Actos jurídicos que definen los requerimientos de la seguridad de la información. Política de seguridad de la información formal y por escrito. Estructura de la organización y descripción de puestos. Acuerdos contractuales con terceros. Plan de Seguridad de TI.	Verificar el documento para examinar si la estrategia de TI destaca adecuadamente el papel fundamental de la seguridad de la información. Consultar y utilizar la matriz de *Gobernanza de TI* para *la estrategia de TI.* Ante la falta de una estrategia de TI por escrito, entrevistar a la gerencia senior, a la gerencia de nivel intermedio y al personal para verificar cuál es su conocimiento sobre el papel estratégico de la seguridad de la información. Evaluar el cumplimiento de la *Política de Seguridad de la Información* y *Estrategia de TI* de la organización y los requerimientos de cumplimiento externos. Comparar los objetivos de política y los procedimientos de seguridad para determinar la efectividad de la incorporación de los requerimientos de seguridad de la información en el plan de seguridad de TI (estatutos, marco, manual, etc.). Verificar si los niveles de la administración adecuados evalúan lo antedicho con regularidad. Examinar la cobertura del plan de seguridad de TI y verificar si incluye los planes estratégicos de TI, clasificación de datos, normas relativas a la tecnología, políticas de seguridad y control, y gestión de riesgo. Verificar si el plan de seguridad de TI identifica: Roles y responsabilidades (comité, dirección ejecutiva, responsables inmediatos, personal y todos los usuarios de la infraestructura tecnológica de la organización), requerimientos del personal, concientización y capacitación en seguridad; prácticas de cumplimiento; y necesidad de inversiones en los recursos requeridos para la seguridad. Revisar y analizar los estatutos para verificar que éstos hacen referencia al perfil de riesgo de la organización con respecto a la seguridad de la información, y que los estatutos incluyen claramente el alcance y los objetivos de la función de gestión de seguridad. Revisión de los informes de incidentes de seguridad y los documentos de seguimiento para identificar cuáles son las medidas que la organización implementa cuando los individuos violan la política de seguridad. Revisión de los informes de incidentes para identificar la cantidad de violaciones a la Seguridad de la Información cometidas por los empleados o terceros en un periodo determinado a fin de evaluar la efectividad de la política.

Tema 5 de auditoría: Confidencialidad

¿Cuenta la organización con requerimientos de confidencialidad o acuerdos de no divulgación que reflejen adecuadamente la necesidad de proteger la información? ¿Las políticas aseguran la información en la relación de la organización con terceros?

[53] Véase la serie ISO 27000 sobre el Sistema de Gestión de Seguridad de la Información y otras políticas internas, procedimientos o regulaciones aplicables.

Criterios: La política de seguridad de la información de la organización es capaz de proteger toda la información confidencial relacionada con los interesados internos y con terceros.	
Información Requerida	**Método(s) de Análisis**
Regulaciones externas e internas relativas a la información confidencial y clasificada. Por ejemplo, cláusulas de no divulgación para los empleados. Acuerdos contractuales con terceros. Política de seguridad de la información. Plan de Seguridad de TI.	Verificar las medidas procedimentales adoptadas por la organización para cumplir con los requerimientos de confidencialidad. Cuando los casos de violación a la confidencialidad se limitan a procesos legales especiales y a entidades especiales únicamente, fundamente su opinión en base a sus informes y recomendaciones a la gerencia de la organización, en caso de estar disponibles. Revisar los acuerdos contractuales con terceros o contratistas. ¿Incluyen el otorgamiento o solicitud de acceso, procesamiento, comunicación o gestión de activos de información de la organización? Verificar si los términos y obligaciones contractuales definen las restricciones y obligaciones respecto de la seguridad que regulan de qué manera los contratistas utilizarán los activos de la organización y accederán a los sistemas de información y servicios. Verificar si los contratistas han cometido alguna violación a la seguridad de la información. Verificar las medidas tomadas por la gerencia respecto de tales violaciones.
Conclusión de la auditoría: Para ser completado por el auditor	

Organización de la Seguridad de TI

Objetivo de auditoría: Garantizar la operación segura de las instalaciones de procesamiento de TI.

Tema 6 de auditoría: Estructura

¿Cuenta la entidad auditada con una clara estructura de seguridad de TI? ¿Están definidos los roles y las responsabilidades relativas a la seguridad con respecto a la política de seguridad de la información?

Criterios: Roles y responsabilidades de TI claros y documentados referidos a la Política de Seguridad de la Información[54]	
Información Requerida	**Método(s) de Análisis**
Estructura de el área de TI. Regulaciones internas relativas a la seguridad de SI. Descripciones de las tareas Actas de reuniones de los órganos pertinentes.	Determinar si la responsabilidad de la seguridad de TI se estableció de forma correcta y con claridad. Verificar si existe un proceso para priorizar las iniciativas de seguridad propuestas, incluidos los niveles requeridos de políticas, normas y procedimientos. Verificar de qué manera la gerencia senior mantiene un nivel de interés adecuado en la seguridad de la información dentro de la organización.

Tema 7 de auditoría: Coordinación

¿De qué manera la organización coordina las actividades de seguridad de la información entre las diferentes áreas de la organización?

Criterios: Inexistencia de conflictos de responsabilidad, discordancia, vacíos de responsabilidad en las actividades de Seguridad de la Información.[55]

[54] Véase Serie ISO 27000.
[55] Véase Serie ISO 27000 sobre Sistema de Gestión de Seguridad de la Información.

Información Requerida	Método(s) de Análisis
Requerimientos legales respecto a la información clasificada. Estructura de la organización. Regulaciones Internas relativas a la seguridad de SI. Actas de la reunión del comité de seguridad de TI. Informes de fallas.	Verificar los documentos, observar las prácticas y entrevistar al personal para determinar si hay conflictos/superposiciones/disparidades inherentes entre los procedimientos de seguridad que cumplen los empleados en diferentes departamentos/ unidades. Verificar los procedimientos del flujo de trabajo operativo para identificar si cierta información es transmitida a terceros fuera del control de las unidades/empleados responsables. Verificar si los gerentes senior tienen conocimiento de los problemas de coordinación y si supervisan las inspecciones y actividades de coordinación. Revisar los procesos para verificar si existe algún procedimiento establecido para que la gerencia autorice nuevas instalaciones de procesamiento de información.
Conclusión de la auditoría Para ser completado por el auditor	

Gestión de Operaciones y Comunicaciones	
Objetivo de auditoría: Garantizar que la comunicación interna y externa sea segura.	
Tema 8 de auditoría: Política y procedimientos ¿Son las políticas y los procedimientos adecuados para una comunicación interna y externa segura y eficiente?	
Criterios: Las políticas y los procedimientos conforman un entorno de gestión seguro para la comunicación interna y externa.[56]	
Información Requerida	**Método(s) de Análisis**
Política oficial y por escrito relativa a las comunicaciones y operaciones de TI. Documentación relativa a los procedimientos operativos.	Verificar si las políticas y los procedimientos de la organización incluyen la comunicación con los ciudadanos, los medios de comunicación y las organizaciones externas. Verificar de qué manera la organización documenta sus procedimientos operativos y los pone a disposición de todos los usuarios. Entrevista a una muestra de usuarios en diferentes niveles para examinar si los procedimientos para el manejo de datos son reconocidos por los empleados. Verificar con qué frecuencia se revisan y actualizan los procedimientos de comunicación y manejo de datos.
Tema 9 de auditoría: Control de Red ¿De qué manera la organización gestiona y controla la información en la red?	
Criterios: Las operaciones de red son gestionadas y ejecutadas de forma segura y efectiva.[57]	
Información Requerida	**Método(s) de Análisis**
Política de Restricción de la Información. Registros de administrador de red. Resultados de los análisis de los registros. Informe de pruebas de	Verificar qué herramientas se utilizan para el seguimiento y análisis de la red. Verificar si los usuarios y los sistemas de TI de la entidad auditada están protegidos contra *spam*. Verificar si las configuraciones y los registros del Sistema de Detección de Intrusión son analizados por el personal adecuado para garantizar la seguridad de la información ante ataques de *hackers* e intrusiones de programas maliciosos. Verificar si los ataques (fallidos y concretados) son analizados e informados.

[56] Véanse las siguientes normas: ISO-27002, S15 Control-IT (Norma ISACA), marco de referencia de buenas prácticas de TI COBIT.
[57] Ibid.

admisión del usuario. Acuerdo(s) de Nivel de Servicio Información disponible al público o encontrada en las páginas web	Verificar las estadísticas de ataques de *spam, hackers* y programas maliciosos. Investigar de qué manera la organización proporciona una transmisión segura de las transacciones que se emiten a través de redes públicas. Por ejemplo, circulación/notificación de procedimientos operativos a los usuarios para transacciones de *e-commerce* y transacciones *on- line*. Revisar las políticas para verificar si la transmisión de datos fuera de la organización requiere un formato encriptado previo a la transmisión. Investigar si se han implementado políticas de seguridad de la información de conformidad con la clasificación de sensibilidad de los datos de la organización (por ejemplo, confidencial, sensible). Mediante consultas, determinar si el cliente utiliza el encriptado para el procesamiento de información sensible. En caso afirmativo, realizar una prueba de validación. **Procedimientos para las Pruebas de Validación de Control** **Prueba de Validación 1:** Efectividad operativa de los controles de encriptado : Determinar: • La existencia de procesos para el ciclo de vida de gestión de claves. • Destrucción de claves. • División de tareas de los encargados autorizados de las claves.
Tema 10 de auditoría: Gestión de la Configuración ¿Se encuentran las configuraciones de los recursos de TI bajo un adecuado control?	
Criterios: Sistema de configuración claro y bien gestionado, que respalde la Seguridad de la Información en la comunicación y las operaciones.	
Información Requerida	**Método(s) de Análisis**
Políticas y procedimientos relativos a cuestiones de configuración en el área de operaciones. Listas de configuración/ biblioteca	Revisar las matrices de los roles para determinar quién es responsable de la administración de la configuración y cuál es el alcance del control de la configuración en las operaciones. Verificar de qué manera se registra, controla y actualiza. Verificar si anteriormente se había producido algún problema debido a discrepancias en la configuración. En este caso, entrevistar a los administradores para verificar qué procedimientos se han implementado en los cambios de configuración.
Conclusión de la auditoría Para ser completado por el auditor	

Gestión de Activos
Objetivo de auditoría: Fomentar la adecuada protección de los activos de TI.
Tema 11 de auditoría: Gestión de Activos ¿Cuenta la organización con un sistema de gestión de activos adecuado, que respalde la seguridad de la información?
Criterios: Garantizar la adecuada protección de los activos de información [58]

[58] Serie ISO 2700 Sistema de Gestión de Seguridad de la Información, COBIT, y otras políticas, procedimientos y regulaciones internos aplicados).

Información Requerida	Método(s) de Análisis
Política de gestión de activos. Clasificación de Activos. Clasificación de información. Procedimientos de disposición de activos Informes de auditoría financiera (si se refieren a activos e inventarios).	Revisión de la política para verificar que exista una política de uso razonable para el hardware y el software de TI (por ejemplo, las computadoras portátiles se pueden utilizar para uso personal si no interfieren con el trabajo oficial). Verificar si la base de datos de activos está actualizada. Verificar los registros de inventario para corroborar si los activos se clasifican en función del valor, la sensibilidad, u otras categorías. Revisión de los procedimientos para la disposición de activos y el nivel de supervisión obligatoria. Verificar el requerimiento de autorización para cualquier disposición o reutilización de los equipos. Consultar a las personas y verificar las disposiciones que garantizan que los datos son eliminados antes de la remoción o reutilización de los equipos.
Conclusión de la auditoría	

Seguridad de los Recursos Humanos	
Objetivo de auditoría: Garantizar que todos los empleados (incluidos los contratistas y todo usuario de datos sensibles) estén calificados para manejar datos y comprendan sus funciones y responsabilidades, y que el acceso sea dado de baja una vez que el empleo/contrato haya concluido.	
Tema 12 de auditoría: Concientización y responsabilidad del personal ¿Están los empleados en conocimiento de sus roles, obligaciones y responsabilidades referidas a la seguridad de la información?	
Criterios: Personal capacitado profesionalmente en relación con la protección de la seguridad de la información.	
Información Requerida	**Método(s) de Análisis[59]**
Política y procedimientos de selección de RRHH. Política y procedimientos de seguridad de la información. Normas de competencia para personal de TI. Informes de evaluación individual. Informes de incidentes de seguridad (incluido el incumplimiento con el código de ética o código de conducta). Campaña de concientización sobre seguridad. Roles y responsabilidades de la administración del usuario.	Examinar la documentación de la contratación para una muestra representativa de los miembros del personal de TI a fin de evaluar si se ha completado y evaluado la verificación de los antecedentes. Verificar los criterios de selección para realizar los controles de antecedentes de acreditaciones de seguridad. El rol de cada posición debe ser claro. Se deben realizar actividades de supervisión para verificar el cumplimiento con las políticas y procedimientos de administración, el código de ética y las prácticas profesionales. Verificar si los roles claves para la seguridad de la información están claramente definidos y documentados. Los empleados y terceros a cargo de tales funciones deben conocer sus responsabilidades con respecto a la protección de los activos de información de la organización, incluidos los datos electrónicos, infraestructuras de SI y documentos. Verificar que las definiciones de funciones críticas sean adecuadas, para las cuales se requieren los controles de autorización de seguridad. Esto deber aplicarse a los empleados, contratistas y proveedores. Verificar que la División de Funciones entre la gestión de seguridad de TI y las Operaciones sea adecuada. Verificar si la política de ubicación, traslado y rotación del personal de TI, así

[59] Recursos humanos con respecto a la Seguridad de la Información es uno de los temas clave en otras secciones como *Gobernanza* de *TI*, y posiciones de esta Matriz de Auditoría, como *Política de Seguridad de la Información* (concientización, responsabilidad, flujo de información de arriba hacia abajo, sanciones) o *Control de Acceso* (derechos de usuarios individuales).

	como la terminación de los contratos de empleo es lo suficientemente clara para minimizar la dependencia de un individuo. Verificar qué mecanismos de transferencia de conocimientos se utilizan.
Tema 13 de auditoría: Capacitación ¿Es la capacitación un procedimiento efectivo para mejorar las habilidades profesionales del personal en materia de Seguridad de la Información?	
Criterios: Realización, alcance y frecuencia de la Capacitación en Seguridad de la Información de la Organización.	
Información Requerida Cronograma de capacitación. Resultados de las pruebas finales. Evaluación de la eficacia de la capacitación.	**Método(s) de Análisis** Evaluar el proceso de medición de la efectividad de la capacitación, en caso de que los haya, para corroborar que los requerimientos clave de la capacitación y la concientización en seguridad de TI estén incluidos. Revisión del contenido del programa de capacitación en seguridad de TI para verificar que sea completo y adecuado. Revisión de los mecanismos de transmisión para determinar si la información se transmite a todos los usuarios de recursos de TI, incluidos los consultores, contratistas y empleados temporarios y, si corresponde, clientes y proveedores. Revisión del contenido del programa de capacitación para determinar si están incluidos todos los marcos de control interno y los requerimientos de seguridad sobre la base de las políticas de seguridad y los controles internos de la organización (por ejemplo, el impacto del incumplimiento con los requerimientos de seguridad, el uso apropiado de los recursos e instalaciones de la organización, manejo de incidentes, responsabilidad de los empleados respecto de la seguridad de la información). Consultar y confirmar si los materiales y programas de capacitación han sido revisados periódicamente para verificar su adecuación. Revisión de la política para determinar los requerimientos de capacitación. Corroborar que la política de capacitación garantice que los requerimientos claves de la organización se reflejen en los programas de capacitación y concientización. Entrevista al personal para verificar si ha realizado capacitaciones llevadas a cabo por la organización y si ha comprendido claramente las responsabilidades en relación con el mantenimiento de la seguridad y confidencialidad de la información.
Conclusión de la Auditoría	

Seguridad Física	
Objetivo de auditoría: Prevenir el robo o daño de la infraestructura de TI, el acceso no autorizado, y la copia o visualización de información sensible.	
Tema 14 de auditoría: Seguridad de las instalaciones ¿Están asegurados los edificios y las áreas exteriores de la organización contra riesgos físicos y ambientales?	
Criterios: Asegurar que la seguridad física y ambiental cumple con los requerimientos de seguridad y clasificación de la sensibilidad de los activos de TI.	
Información Requerida Diagrama de red. Plan de Seguridad de las instalaciones. Informe periódico de las pruebas físicas. Informes de los servicios	**Método(s) de Análisis** Analizar cuáles son los principales controles de seguridad física de la organización auditada. Verificar si coinciden con el análisis de riesgo actualizado. Revisión de la ubicación y de las medidas de precaución físicas para los elementos clave de la infraestructura tecnológica. Verificar qué controles ambientales se han implementado (extintores, alarma, sistemas de energía,

pertinentes (Ejemplo, departamento de Bomberos).	etc.). Verificar si se han implementado las recomendaciones de los servicios pertinentes (especialmente, los bomberos, la inspección de la vivienda, la prevención de desastres). (Para planes de seguridad relativos a los desastres, consultar la sección sobre BCP y DRP del presente Manual).
Tema 15 de auditoría: Acceso físico ¿De qué manera garantiza la organización que solo el personal autorizado tenga acceso a las instalaciones?	
Criterios: La organización implementa medidas de seguridad a fin de prevenir el acceso físico no autorizado a instalaciones clave de TI (sala de servidores, almacenamiento de datos, etc.)	
Información Requerida	**Método(s) de Análisis**
Plan de instalación del hardware de TI. Plan de Seguridad del sitio. Configuración de dispositivos. Informe periódico de pruebas físicas. Informes de incidentes.	Revisión de las instrucciones de seguridad, diagramas de red y documentos conexos y verificar de qué manera la organización controla el acceso a las áreas sensibles de sus instalaciones. Revisión y observación del tráfico de entrada/salida y de qué manera funciona el sistema de seguridad física. Determinar qué medios son utilizados. Implementar las políticas y procedimientos relativos a la seguridad de las instalaciones (puertas, credenciales, molinetes, guardias, barreras, clave de acceso y acceso mediante lector de tarjeta, etc.) y determinar si dichos procedimientos constituyen una identificación y autenticación adecuadas. Verificar quién mantiene y controla las asignaciones de control de acceso en las ubicaciones sensibles. Verificar si el nivel de gestión es suficiente para la Seguridad de la Información. Verificar si el acceso a las áreas seguras/salas seguras/ubicaciones de servidor se encuentra restringido. Seleccionar una muestra de usuarios/empleados y determinar si su acceso a las instalaciones es apropiado en base a las responsabilidades de su trabajo. Verificar si éstos informan los incidentes a un sistema de gestión de incidentes/ problemas. Verificar si estos se analizan y si las lecciones se han aprendido.
Tema 16 de auditoría: Protección contra Intrusiones ¿Cuenta y cumple la organización con una política de detección de intrusiones?	
Criterios: Procedimientos para prevenir intrusiones según se establece en la Política de Seguridad interna de la Organización	
Información Requerida	**Método(s) de Análisis**
Plan de Seguridad del sitio. Configuración de dispositivos. Informes de incidentes.	Examinar de qué manera la unidad de seguridad de la organización toma conocimiento de que se ha producido una intrusión, a fin de proteger las ubicaciones. Revisión de las instrucciones para conocer el Proceso de gestión de una intrusión a un espacio o edificio seguro. Revisión de los informes de incidentes para identificar si la intrusión fue detectada a tiempo. Verificar si la organización cuenta con una política clara de escritorio limpio o pantalla limpia para evitar el acceso no autorizado.
Conclusión de la auditoría	

Control de Acceso

Objetivo de auditoría: Garantizar que solamente los usuarios autorizados tengan acceso a la información relevante.

Tema 17 de auditoría: Política de Acceso
¿Cuenta la organización con una política clara y eficiente sobre control de acceso?

Criterios:
La Política de Acceso brinda una base sólida para el control de la distribución de información relevante.

Información Requerida	Método(s) de Análisis
Políticas y procedimientos de acceso. Lista de usuarios. Lista/matriz de control de acceso.	Análisis de las Políticas y los procedimientos de Acceso para garantizar que las obligaciones y las áreas que son responsabilidad de los empleados estén divididas a fin de reducir las situaciones de acceso no autorizado y la aprobación de privilegios**.** ***Prueba de Validación:*** La eficacia operativa de la autorización de acceso de los usuarios a LAN (no se debe realizar ninguna prueba separada de acceso del usuario a las aplicaciones conjuntamente con revisiones de la aplicación). Selección de una muestra de usuarios y de cuentas del sistema para determinar la existencia (se puede utilizar un software de control de acceso) de: • Rol solicitado claramente definido, y/o privilegios asignados a funciones de trabajo. • Fundamento del negocio para el acceso. • Titular de los datos y autorización de la gerencia (es decir, firmas/ aprobaciones por escrito). • Fundamento del negocio/riesgo, y aprobación de la gerencia para las solicitudes atípicas; • El acceso solicitado es compatible con la tarea/rol y la división de funciones requerida.

Tema 18 de auditoría: Gestión de Privilegios
¿Es seguro y efectivo el proceso para el otorgamiento y la revocación del control de acceso a los empleados y contratistas?

Criterios:
La función de Seguridad de la Información controla las operaciones de administración de la cuenta del usuario de manera oportuna e informa la eficiencia y la efectividad de las operaciones.

Información Requerida	Método(s) de Análisis
Procedimientos de control de acceso. Muestras de traslados y terminación de tareas del personal.	Verificación de los procedimientos para determinar con qué frecuencia se revisan los distintos accesos y privilegios que los empleados o usuarios tienen en la organización. Verificar de qué manera se confirman los privilegios que se conceden a un empleado (por ejemplo, solicitud al supervisor, gerente de área, grupo, etc.). Entrevista a una muestra de usuarios y verificación de las instrucciones para corroborar de qué manera se informa a los usuarios su responsabilidad en cuanto a la protección de información o activos sensibles cuando se les otorga el acceso. Determinar si las prácticas de seguridad de la organización requieren que los usuarios y procesos del sistema sean identificables individualmente y que los sistemas sean configurados para cumplir con la autenticación antes de otorgar el acceso, y que tales mecanismos de control se utilicen para el control de acceso lógico de todos los usuarios, los procesos del sistema y recursos de TI. Análisis de otros elementos además de los distintos privilegios de contraseñas, por ejemplo, ¿de qué manera se verifica que un usuario cuenta con acceso y privilegios suficientes para el recurso solicitado? (por ejemplo, el acceso desde una ubicación segura, autenticación de hardware o lectores de huellas digitales, etc.).

	Prueba de Validación 1: Eficacia operativa de los traslados y terminación de tareas: Obtener de RR.HH. una muestra de los traslados y las terminaciones de tareas de los empleados y, a través de la revisión de los perfiles de la cuenta del sistema y/o CAAT (por ejemplo, ACL, IDEA) determinar si el acceso ha sido modificado y/o revocado adecuadamente y de manera oportuna. ***Prueba de Validación 2:*** Administración de la contraseña: Verificar que los requerimientos de calidad para las contraseñas sean definidos y cumplidos por el sistema de gestión de la red o sistemas operativos sobre la base de los requerimientos locales/ política de organización o buenas prácticas.
Conclusión de la auditoría	

La adquisición, el desarrollo y el mantenimiento de Sistemas se detallan en el Anexo III.

La Gestión de la Continuidad del Negocio se presenta en el Anexo VI.

ANEXO VIII
MATRIZ SUGERIDA PARA LA AUDITORÍA DE LOS CONTROLES DE APLICACIÓN

<table>
<tr><th colspan="2">Entrada</th></tr>
<tr><td colspan="2">Objetivo de auditoría: Evaluar si los datos válidos son ingresados en la aplicación por el personal autorizado.</td></tr>
<tr><td colspan="2">Tema 1 de auditoría: Validación de Entrada
¿Cuenta la aplicación con controles de validación de entrada adecuados?</td></tr>
<tr><td colspan="2">Criterios:
Numerosas buenas prácticas constituyen la base de los criterios para los controles de validación de entrada, por ejemplo, que las reglas de validación sean exhaustivas, estén documentadas e implementadas en las interfaces de entrada de la aplicación; se documenten diferentes métodos e interfaces para el ingreso de datos; los datos inválidos son debidamente rechazados por la aplicación; los criterios de validación se actualizan de manera oportuna, adecuada y por medio de autorización; existen controles compensatorios, como registros y reglas de autorización ante la posibilidad de anular los controles de entrada; y existen controles y documentación adecuados para las interfaces de la aplicación.</td></tr>
<tr><td>Información Requerida

Requerimiento y reglas del negocio

Tipos de entrada de datos

Requerimientos de cumplimiento legales y externos

Estructura de interfaces de datos con otras aplicaciones

Diagramas de flujo del sistema

Manuales de usuario

Reglas de validación</td><td>Método(s) de Análisis

Análisis de las reglas y requerimientos del negocio, y de la documentación de la aplicación; y solicitar a los titulares de los procesos del negocio que indiquen que reglas de validación deben estar garantizadas en el proceso del negocio que se está evaluando. Verificar si estas reglas de validación fueron adecuadamente diseñadas y documentadas. Verificar si se aplican los controles de validación para el ingreso de datos: observar a los usuarios de las aplicaciones en sus verdaderas actividades; ejecutar la aplicación en un entorno de prueba y probar las diferentes interfaces para el ingreso de datos y analizar los registros de datos almacenados en la base de datos mediante el uso de CAAT.

Solicitar una descripción funcional para cada tipo de entrada e información de diseño sobre el ingreso de registros. Revisar la funcionalidad y el diseño para corroborar la existencia de controles oportunos y completos y mensajes de error. Si es posible, examinar el ingreso de registros.

Evaluar si los criterios y los parámetros de validación de los datos ingresados coinciden con las regulaciones del negocio y obligan al rechazo de tipos de entrada dispares. En el caso de los sistemas de procesamiento on -line, verificar que los datos inválidos sean rechazados o editados al momento del ingreso y probar los controles lógicos/ controles de cálculos efectuados. Los símbolos de la base de datos (por ejemplo*, = o, seleccionar) deben ser denegados como entradas válidas, ya que pueden ser utilizados para alterar u obtener información de la base de datos.

Consultar a los gerentes si los criterios y parámetros de validación sobre los datos ingresados son revisados, validados y actualizados periódicamente de manera oportuna, adecuada y mediante autorización. Se puede confirmar esto a través de la revisión de la documentación, análisis de código o entrevistas.

Consultar y controlar la documentación a fin de verificar la posibilidad de anular las validaciones del control de datos de entrada y los controles. Verificar si las acciones de anulación están debidamente registradas y revisadas para constatar su adecuación. Verificar si la autoridad para anular se limita solo al personal de supervisión y a un número restringido de situaciones. Examinar correcciones de errores, anulaciones de entrada y otros documentos para verificar que se</td></tr>
</table>

	cumplen los procedimientos. Determinar qué interfaces existen en la aplicación. Estas interfaces podrían presentarse bajo la forma de transmisión de datos en tiempo real o transmisión periódica de archivos de datos a través del proceso por lotes. Revisión de los diagramas de flujo del sistema y código del sistema, y entrevista a los desarrolladores o administradores de la aplicación para obtener información sobre las interfaces y los controles de las mismas. Por ejemplo: los totales del control de las transmisiones de interfaz, ejemplo: totales de comprobación (*Hash*). [60]
Tema 2 de auditoría: ¿Es adecuada la gestión de documentos fuente, recopilación e ingreso de datos?	
Criterios: Los procedimientos de preparación de datos son documentados y comprendidos por los usuarios; existen registros adecuados de los documentos fuente recibidos hasta su eliminación; se asigna un número único y secuencial a cada registro; y se conservan los documentos fuente por el tiempo requerido por las políticas y normas legales.	
Información Requerida	**Método(s) de Análisis**
Clases de documentos fuente Criterio de la entidad para la puntualidad, integridad y exactitud de los documentos fuente Procedimientos de preparación de datos. Interfaces de datos con otras aplicaciones Políticas de conservación de documentos Diagramas de flujo del sistema	Revisión y observación de la elaboración y documentación de los procedimientos de preparación de datos, y consultar y confirmar si se comprenden los procedimientos y se utilizan los medios de fuente correctos. Evaluar si el equipo de procesamiento de datos (DP) o equivalente conserva un registro de todos los documentos fuente de los departamentos de usuarios recibidos y lleva a cabo su eliminación final. Verificar la existencia de un sistema de conciliación de las cuentas del registro con los equipos del departamento del usuario. Verificar que todos los documentos fuente incluyan elementos estandarizados, contengan documentación apropiada (por ejemplo, la puntualidad, los códigos de entrada predeterminados, valores por defecto) y que estén autorizados por la gerencia. Verificar que los documentos fuente críticos estén pre-enumerados y de qué manera se identifican y se abordan los números fuera de secuencia. Identificar y revisar los números fuera de secuencia, brechas y duplicaciones utilizando herramientas automatizadas (CAAT). Verificar si se asigna un número único y secuencial a cada registro a fin de evitar la duplicación. Consultar al personal pertinente sobre las políticas de conservación. Verificar de qué manera se garantizan estas políticas. Se podría cotejar una muestra de los registros del sistema con los documentos fuente.
Tema 3 de auditoría: ¿Cuenta la aplicación con procedimientos adecuados para el manejo de errores?	
Criterios: Existe un sistema de mensajes de error claros y concisos que comunican los problemas a fin de que se puedan aplicar medidas correctivas inmediatas para cada tipo de error. Los errores son corregidos o debidamente eliminados antes del procesamiento de registros. Se revisan los registros periódicamente y se toman las medidas correctivas necesarias.	
Información Requerida	**Método(s) de Análisis**
Tipos y mensajes de error Procedimientos de revisión de registros	Discutir el manejo de errores en la aplicación y excepciones con el desarrollador y/o administrador. Consultar y confirmar si existen políticas y procedimientos para el manejo de registros que no cumplen con los controles de edición y validación.

[60] PC Magazine Encyclopaedia extraído de http://www.pcmag.com/encyclopedia/term/44130/hash-totals:
Método para garantizar la precisión de los datos procesados. Representa el total de varios campos de datos en un archivo, incluidos los campos que normalmente no se utilizan en los cálculos, como el número de cuenta. En varias etapas del procesamiento, el total de comprobación se recalcula y se compara con el original. Si algún dato se perdió o modificó, la incompatibilidad marca un error.

Políticas y procedimientos para abordar datos rechazados Procedimientos de revisión de archivos transitorios.	Verificar si el sistema proporciona mensajes de error para cada tipo de error (a nivel de campo o nivel de registro) que no cumpla con la validación de edición. Verificar de qué manera la aplicación actúa si los datos son rechazados por los controles de entrada. Verificar si las partidas de datos son registradas o si se guardan automáticamente en un archivo transitorio. Verificar si el archivo transitorio automatizado incluye códigos que indican los tipos de errores, la fecha y hora de entrada, e identificar el usuario que ingresa los datos. Evaluar si existen procedimientos para la revisión y corrección de los datos en el archivo transitorio antes de procesarlos nuevamente. Evaluar si existe un procedimiento de escalada cuando la tasa de errores es demasiado alta y si se toman medidas correctivas. Consultar a los gerentes si existen procedimientos para revisar periódicamente el registro. Verificar si los procedimientos incluyen el inicio de medidas correctivas. Obtener evidencia, ya sea documental o digital, de que el registro se revisa periódicamente.
Tema 4 de auditoría: ¿De qué manera se gestiona la autorización del ingreso de datos en la aplicación?	
Criterios: Se establecieron niveles de autorización para el ingreso de datos y estos se aplican mediante controles adecuados; existe una adecuada división de funciones para el ingreso de datos; existen controles compensatorios para aquellos casos en los que no es posible la división de funciones.	
Información Requerida	**Método(s) de Análisis**
Requerimientos de cumplimiento legales y externos Requerimientos y reglas del negocio Manuales del usuario	Consultar y confirmar si el diseño del sistema contempla el uso de listas de autorización pre-aprobadas. Verificar, mediante la revisión de listas de autorización, que los niveles de autorización estén adecuadamente definidos para cada grupo de registros. Evaluar si las reglas de autorización para el ingreso, edición, aceptación, rechazo y anulación de datos para los principales tipos de registros están bien elaboradas y documentadas. Verificar que los niveles de autorización se apliquen adecuadamente mediante la ejecución de la aplicación en un entorno de pruebas. Verificar, mediante el uso de CAAT o módulos de auditoría incorporados, que los registros de autorización presentes en la base de datos cumplan con las normas de autorización establecidas. Determinar si existe un cuadro para la división de funciones y verificar que existan una división de funciones /tareas clave adecuada y operaciones permitidas; a continuación, verificar la lista de usuarios y privilegios de acceso para cada usuario específico. Evaluar si la división de funciones garantiza que la persona que ingresa los datos no sea también responsable de la verificación de los documentos. Verificar la adopción de los controles compensatorios en los casos en que la división de funciones no sea factible.

Procesamiento
Objetivo de auditoría: Evaluar si la aplicación garantiza la integridad, la validez y la confiabilidad de los datos durante el ciclo de procesamiento de registros.
Tema 5 de auditoría: ¿Están las reglas y requerimientos del negocio correctamente internalizados en la aplicación?
Criterios: Las operaciones de la aplicación se ejecutan según se espera.

Información Requerida	Método(s) de Análisis
Documentación de la aplicación Reglas y requerimientos del negocio Diagrama de flujo de datos Lista de las operaciones altamente críticas Código fuente	Identificar los programas ejecutables en la aplicación mediante el análisis del diagrama de flujo de datos y compararlos con las normas de procesos del negocio definidas y establecidas. Revisión de la documentación de la aplicación para verificar que sea aplicable y adecuada para la tarea. Cuando sea apropiado para operaciones críticas, revisar el código para confirmar que los controles en las herramientas y las aplicaciones funcionan conforme a su diseño. Procesar nuevamente una muestra representativa para verificar que las herramientas automatizadas funcionan según lo previsto. Para transacciones altamente críticas, establecer un sistema de prueba que funcione como el sistema real. Procesar operaciones en el sistema de prueba para garantizar que las operaciones válidas sean procesadas adecuadamente y de manera oportuna.
Tema 6 de auditoría: ¿Garantizan los controles de la aplicación la integridad de las operaciones?	
Criterios: La aplicación identifica correctamente los errores en las operaciones. La integridad de los datos se mantiene incluso durante interrupciones inesperadas en el procesamiento de las operaciones. Existe un mecanismo adecuado para el manejo de errores de procesamiento, revisión de los archivos transitorios y depuración.	
Información Requerida	**Método(s) de Análisis**
Documentación de diseño de la aplicación Reglas y requerimientos del negocio Informes de desequilibrios Conciliaciones Procedimientos de revisión de informes Archivos transitorios	Evaluar si la aplicación cuenta con controles de validación adecuados para garantizar la integridad del procesamiento. Revisión de la funcionalidad y del diseño para verificar la existencia de errores de secuencia y duplicación, verificación de integridad de referencia, controles, y totales de comprobación.[61] Revisar las conciliaciones y otros documentos para verificar que las cuentas de entrada coincidan con las cuentas de salida a fin de garantizar la integridad del procesamiento de datos. Realizar un seguimiento de las operaciones a través de todo el proceso para verificar que las conciliaciones determinen efectivamente que los totales de los archivos coinciden o que se informa la condición de desequilibrio. Consultar si los archivos de control son utilizados para registrar los cálculos y el valor monetario de las transacciones, y si los valores son comparados luego de su ingreso. Verificar que los informes especifiquen las condiciones de desequilibrio al generarse, y que los informes sean revisados, aprobados y distribuidos al personal pertinente. Tomar una muestra de las operaciones de ingreso de datos. Utilizar un análisis y herramientas de búsqueda automatizados y apropiados para identificar casos en los que se identificaron errores equivocadamente y casos en los que los errores no fueron detectados. Consultar y confirmar si las funcionalidades son utilizadas, siempre que sea posible, para mantener automáticamente la integridad de los datos durante interrupciones inesperadas en el procesamiento de datos. Revisar las pistas de auditoría y otros documentos, planes, políticas y procedimientos para verificar que las funcionalidades del sistema fueron diseñadas de manera efectiva para mantener automáticamente la integridad de los datos. Revisar la descripción funcional y la información del diseño sobre el ingreso de datos para verificar si los registros que no superan las rutinas de validación son mantenidas en los archivos transitorios. Verificar que los archivos transitorios se

[61] F/N: ibid.

	generen de manera correcta y sistemática, y que se informen a los usuarios los registros ingresados a las cuentas transitorias. En una muestra de sistemas de transacción, verificar que las cuentas transitorias y los archivos transitorios para los registros que no superan las rutinas de validación sólo contengan errores recientes. Confirmar que los registros fallidos más antiguos hayan sido adecuadamente corregidos.

Salida

Objetivo de auditoría: evaluar si la aplicación garantiza que la información de salida sea completa y precisa antes de proseguir con su uso y que esté debidamente protegida.

Tema 7 de auditoría:
¿Cuenta la aplicación con controles para garantizar la integridad y exactitud de los datos de salida?

Criterios:
Se han diseñado procedimientos para garantizar que se validen la integridad y exactitud de los datos de salida de la aplicación antes de que sean utilizados para el procesamiento posterior, incluido el uso en el procesamiento de usuarios finales; se permite la realización del seguimiento de los datos de salida de la aplicación; se verifican los datos de salida para corroborar su razonabilidad y exactitud; y los controles de integridad y precisión son eficaces.

Información Requerida	**Método(s) de Análisis**
Controles de integridad y exactitud Métodos para el equilibrio y la conciliación Lista de datos de salida electrónicos / informes Muestra de salida electrónica	Obtener una lista de todos los datos de salida electrónicos que son reutilizados en las aplicaciones del usuario final. Verificar que los datos de salida electrónicos sean probados para corroborar su integridad y exactitud antes de que los datos de salida se reutilicen y reprocesen. Examinar el equilibrio y la conciliación de los datos de salida según lo establecido por métodos documentados. Seleccionar una muestra representativa de los datos de salida electrónicos, y rastrear los documentos seleccionados a través del proceso para garantizar que se verifiquen la integridad y exactitud antes de realizar otras operaciones. Realizar nuevamente las pruebas de integridad y exactitud para validar su efectividad. Examinar si cada dato de salida contiene el nombre o número del programa de procesamiento, título o descripción; período de procesamiento cubierto, nombre y ubicación del usuario; fecha y hora de generación; clasificación de seguridad. Seleccionar una muestra representativa de los informes de salida, y probar la razonabilidad y la precisión de los datos de salida. Verificar que los errores potenciales sean informados y registrados de forma centralizada.

Tema 8 de auditoría:
¿Los datos de salida están protegidos adecuadamente?

Criterios:
La salida de datos se maneja de acuerdo con la clasificación de confidencialidad aplicable; la distribución de los datos de salida/los informes se controlan adecuadamente.

Información Requerida	**Método(s) de Análisis**
Manejo de datos de salida y procedimientos de conservación Políticas de clasificación de la información	Revisar los procedimientos de manejo y conservación de los datos de salida para verificar su confidencialidad y seguridad. Evaluar si se han establecido procedimientos que requieren el registro de errores potenciales y su resolución previo a la distribución de los informes. Examinar el sistema de conciliación de los totales del control de los datos de salida por lotes con los totales de control de los datos de entrada por lotes antes de la presentación de los informes que determinan la integridad de los datos. Verificar si se dispone de procedimientos documentados para el etiquetado de los datos de salida sensibles de la aplicación y, cuando sea necesario, enviar datos de salida sensibles a dispositivos de salida especiales con control de acceso. Revisar los métodos de distribución de información sensible y verificar

	que los mecanismos procuren la implementación correcta de los derechos de acceso preestablecidos.

Seguridad de la Aplicación	
Objetivo de auditoría: Evaluar si la información de la aplicación está correctamente resguardada contra el uso inadecuado.	
Tema 9 de auditoria: ¿Son los mecanismos de trazabilidad de la aplicación suficientes para su propósito?	
Criterios: Existen pistas de auditoría que captan ediciones, anulaciones y registros de autorización para las operaciones críticas; las pistas de auditoría se revisan periódicamente para detectar actividad inusual; las pistas de auditoría son adecuadamente conservadas y protegidas; se asignan a cada registro números únicos y secuenciales, o identificadores.	
Información Requerida	**Método(s) de Análisis**
Estructura y documentación de las pistas de auditoría Políticas de anulación Procedimientos de revisión Diagramas de flujo del sistema	Obtención de la documentación y evaluación del diseño, la implementación, el acceso y la revisión de las pistas de auditoría. Revisión de la estructura de la pista de auditoría y otros documentos para verificar que sea diseñada con eficacia. Consultar quién puede deshabilitar o eliminar las pistas de auditoría. Revisión de las pistas de auditoría, otros documentos, los planes, las políticas y los procedimientos para verificar que los ajustes, anulaciones y transacciones de alto valor sean diseñados de manera efectiva para que se los pueda examinar en detalle con facilidad. Revisión de las pistas de auditoría, los registros (o lotes), revisiones u otros documentos; rastreo de registros a través de todo el proceso; y, siempre que sea posible, utilizar la recopilación automatizada de evidencias, incluidos los datos de muestra, módulos de auditoría integrados o CAAT, para verificar que la revisión y el mantenimiento periódicos de las pistas de auditoría detecte eficazmente actividades inusuales, y que la revisión del supervisor es eficaz. Consultar de qué manera se restringe el acceso a las pistas de auditoría. Verificar los derechos de acceso y los registros de acceso a los archivos de pistas de auditoría. Verificar si únicamente el personal seleccionado y autorizado tiene acceso a las pistas de auditoría. Evaluar si la pista de auditoría está protegida contra modificaciones privilegiadas. Verificar, en lo posible, el uso de recopilación automatizada de evidencia, si se está asignando un único identificador a cada registro.
Tema 10 de auditoría: ¿Están protegidos adecuadamente los datos de la aplicación?	
Para el control de acceso físico y lógico consultar el Anexo VII sobre la Seguridad de la Información. Para el Plan de Recuperación ante Desastres, consultar el Anexo VI sobre BCP/DRP.	

INTOSAI Working Group on IT Audit
c/o CAG of India
Pocket-9, DDU Marg,
New Delhi- 110124, India

www.intosaiitaudit.org

INTOSAI Development Initiative (IDI)
c/o Riksrevisjonen
Pilestredet 42
Postboks 8130 Dep.
N-0032 Oslo, Norway
www.idi.no