PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

PROCESO DE AUDITORÍA DE LA INFORMACIÓN Y COMUNICACIÓN DENTRO DEL CONTROL INTERNO SEGÚN EL MARCO COSO II - ERM

Tesis para optar por el Título de Ingeniero Informático, que presenta el bachiller:

Victor Johao Villarroel Yabar

ASESOR: Manuel Tupia Anticona

Lima, Junio del 2013

ANEXOS

1. ANEXO A

- **Ambiente de Control:** Consiste en acciones, políticas y procedimientos que reflejan la actitud global de los empleados acerca de la importancia del control interno.
  - **Integridad y Valores Éticos:** Los empleados están obligados a cumplir con el código ético y conductuales de la organización, tales como Principios Éticos de los servidores públicos y el código de éticas de sus respectivas profesiones.
  - **Competencia:** Los empleados deben de tener un nivel de conocimiento que les permitan desempeñar de forma eficaz y eficiente su labor, así como también entendimiento amplio de los controles internos para cumplir con los objetivos de la empresa.
  - **Filosofía y Estilo de Operación:** La alta dirección debe de definir las políticas y procedimientos que serán acatadas por el personal.
  - **Estructura Organizativa:** Las organizaciones deben de elaborar una estructura organizativa en donde se defina claramente las responsabilidades y autoridades que vayan de acorde al cumplimiento de los objetivos de la organización.
  - **Autoridad y Responsabilidad:** Las organizaciones deberán crear manuales de funciones en donde se detallen las responsabilidades de los empleados.
  - **Políticas y Prácticas de Recursos Humanos:** Las instituciones públicas deben establecer el sistema de administración de los recursos humanos que promueva y motive al personal.

- **Evaluación de Riesgos:** Conjunto de procesos que desarrolla la organización para determinar la existencia de riesgos relevantes, que puedan afectar el cumplimiento de sus objetivos.
  - **Actividades Financieras y Operacionales:** Las organizaciones deben de asegurarse que las Normas de Control Interno incluyan controles adecuados para superar los riesgos de manera que se satisfagan las afirmaciones de la administración que deben de cumplir con los siguientes criterios:
    - ✓ Existencia u ocurrencia
    - ✓ Integridad

- ✓ Valuación o asignación
- ✓ Derechos y obligaciones
- ✓ Presentación y revelación
- ✓ Eficiencia
- ✓ Efectividad
- ✓ Economía

➢ **Evaluación Continua de Riesgos:** Los organizaciones deberán evaluar continuamente sus actividades y operaciones con la finalidad de identificar áreas de riesgo que puedan afectar el cumplimiento de sus objetivos y metas. La Evaluación de Riesgos se realizará con la finalidad de fortalecer, ajustar adecuar y renovar los controles internos establecidos, de manera que los mismos sean cada vez más eficientes y efectivos.

- **Información y Comunicación:** El sistema de información y comunicación de las entidades públicas tendrá como propósito identificar, reunir, clasificar, analizar, registrar e informar sobre las operaciones, así como mantener la contabilización del presupuesto, activos, pasivos, patrimonio, ingresos y gastos de la entidad.
  - ➢ **Sistema de Contabilidad:** La alta dirección establecerán un adecuado sistema de contabilidad para el registro de sus operaciones. el cual deberá ajustarse al Manual de Contabilidad Gubernamental para la República de Panamá, y el Decreto No. 106 del 5 de mayo de 1998, a las Normas de Contabilidad Gubernamental, emitidas por la Contraloría General de la República.
  - ➢ **Estados Financieros:** El sistema financiero debe de estar en la capacidad de producir estados financieros, información presupuestaria y complementaria, oportuna y pertinente para ayudar a la toma de decisiones en la administración de la organización.
  - ➢ **Sistemas de Procesamiento de Datos:** La alta dirección deberán garantizar la existencia de sistemas de información computarizados o manuales, con los debidos controles para el proceso de las operaciones, que facilite el registro de las transacciones de manera que permita la emisión de reportes oportunos y confiables para la toma de decisiones.

- **Políticas Contables:** Las organizaciones establecerán y mantendrán políticas contables específicas acordes con la naturaleza de la institución. Las políticas contables serán evaluadas y actualizadas periódicamente.
- **Registro de la Operaciones:** Para garantizar controles efectivos de la información contable y sistema de comunicación el registro de operaciones debe de asegurar:
  - ✓ **Existencia:** Corroborar que las operaciones registradas de hecho ocurrieron.
  - ✓ **Integridad:** Todas las operaciones que produzcan variaciones en las cuentas que conforman el sistema de contabilidad deberán ser registrados en los libros principales y auxiliares correspondientes.
  - ✓ **Precisión:** Las operaciones deben de registrarse libres de errores, alteraciones, borrones y tachones, tanto en los registros como en los documentos fuentes.
  - ✓ **Clasificación:** Las operaciones registradas debe de ser debidamente clasificada para facilitar su administración y la creación de reportes.
  - ✓ **Oportunidad:** Las operaciones de la entidad se registrarán en la fecha y en el momento en que se produjo la transacción.
  - ✓ **Asentamiento y resumen:** El registro de las operaciones debe efectuarse en la cuenta. cliente, usuario o beneficiario a la cual corresponde, de forma tal que permita. resúmenes y acumulación de saldos libre de errores.

- **Requerimientos para los Reportes que se Emitan:** Como soporte de la información contable se debe implantar y mantener un sistema de comunicación y coordinación que provea información relativa a las operaciones de manera confiable, oportuna, actualizada y acorde a las necesidades de la entidad.

- **Actividades de Control:** Los controles que se presentan en esta sección son los que se utilizan comúnmente en una estructura de control interno ordenada y eficaz
  - **Separación de Responsabilidades:** La asignación de tareas y responsabilidades deben de tener los siguientes criterios**:**
    - ✓ Las funciones y responsabilidades deben asignarse sistemáticamente a varias personas para asegurar equilibrio entre las diferentes funciones.

- ✓ Entre las funciones claves figuran la autorización y el registro de las transacciones, la emisión y el recibo de los haberes los pagos y la revisión o fiscalización de las transacciones.
- ✓ La rotación del personal contribuye a que los aspectos centrales de las transacciones o hechos contables no se concentren en una sola persona.
- ✓ Debe promoverse e incluso exigirse el disfrute del período de vacaciones anual para ayudar a reducir estos riesgos.

- **Autorización:** Las transacciones deben de ser autorizadas por aquellas personas que actúen en el ámbito de su competencia.
- **Documentos y Archivos:** La estructura del control interno y todas las transacciones deben estar claramente documentadas y disponibles para su verificación.
- **Control Físico de Archivos:** El acceso a los recursos y registros debe limitarse a las personas autorizadas para ello, quienes están obligadas a rendir cuentas de su custodia o utilización.
- **Verificación del Desempeño:** Debe existir una supervisión competente para garantizar el logro de los objetivos del control interno. Los supervisores deben examinar y aprobar el trabajo encomendado a sus subordinados.
- **Supervisión:** Las asignaciones, revisión y aprobación del trabajo del personal exige:
  - ✓ Indicar claramente las funciones y responsabilidades atribuidas a cada empleado.
  - ✓ Examinar sistemáticamente el trabajo de cada empleado, en la medida que sea necesario.
  - ✓ Aprobar el trabajo en puntos críticos del desarrollo para asegurarse de que avanza según lo previsto.

- **Control de Resultados:** Se debe de corroborar lo siguiente:
  - ✓ La observancia de los procedimientos y requisitos aprobados.
  - ✓ La constatación y eliminación de los errores, los malentendidos y las prácticas inadecuadas.
  - ✓ La reducción de las posibilidades de que ocurran o se repitan actos ilícitos y el examen de la eficiencia y eficacia de las operaciones.

- ✓ Contratación del personal idóneo a través de políticas y procedimientos establecidos.

➢ **Asignación de Responsabilidades:** La delegación del trabajo de los supervisores no exime a éstos de la obligación de rendir cuentas de las responsabilidades y tareas.

- **Monitoreo:** Se refiere a la evaluación continua o periódica, de la eficacia y el diseño de operación de una estructura de control interno por parte de la alta dirección, a fin de determinar que esté funcionando de conformidad con los planes y que se modifique de acuerdo con los cambios en las condiciones.
  - ➢ **Evaluación y Control:** Las organizaciones deberán de velar por el establecimiento de formal de un sistema de evaluación y Control Interno según sus características y las leyes, normas y reglamentos establecidos al respecto.
  - ➢ **Definición de la Unidad de Auditoría Interna:** Se debe de crear una unidad de Auditoría interna con la finalidad de medir y evaluar la eficiencia, eficacia y economía de los controles establecidos.
  - ➢ **Designación del Jefe de Auditoría Interna:** Las organizaciones deben de asignar un jefe de la Auditoría Interna completamente independiente de la organización, es decir, que no tenga ninguna participación en las labores administrativas.
  - ➢ **Selección del Auditor Interno:** El Auditor Interno será seleccionado considerando los requisitos de idoneidad previstos en la Ley 57 de 1978, así como los establecidos en las Normas de Auditoría Gubernamental de la República de Panamá, en concordancia con las reglamentaciones internas para el reclutamiento de los recursos humanos en cada institución.
  - ➢ **Dotación de Recursos:** Las organizaciones deben dotar a las unidades de auditoría interna del personal idóneo y necesario así como de recursos, materiales y administrativos que faciliten la efectiva labor de monitoreo en cada organización.
  - ➢ **Equipos Interdisciplinarios:** Las Unidades de Auditoría Interna, cuando sea necesario, se apoyaran o contaran con profesionales de otras disciplinas de acuerdo con la naturaleza de la Auditoría

- **Plan y Cronograma de Auditoría Interna:** Las funciones de la Unidad de Auditoría Interna serán ejecutadas según un plan y cronograma anual de auditoría, elaborado con criterios de economía, objetividad, oportunidad y de relevancia material.
- **Las funciones del Auditor Interno:** Son las siguientes:
  - ✓ Planificar, dirigir y organizar la verificación y evaluación de la estructura de control interno.
  - ✓ Verificar que la estructura de control interno esté formalmente establecida y que su ejercicio sea intrínseco al desarrollo de las funciones de todos los cargos y en particular de aquellos que tengan responsabilidad de mando.
  - ✓ Verificar que los controles definidos para los procesos y actividades de la organización. se cumplan por los responsables de su ejecución y en especial que las áreas o empleados encargados de la aplicación del régimen disciplinario ejerzan adecuadamente esta función.
  - ✓ Garantizar el cumplimiento de las leyes, normas, planes y políticas de la institución y recomendar los ajustes necesarios.
  - ✓ Servir de apoyo a la alta dirección, identificando y promoviendo el mejoramiento de los puntos débiles de la estructura de control interno, sistemas y procesos políticas y procedimientos, de tal manera que produzca información confiable y oportuna.
  - ✓ Verificar los procesos relacionados con el manejo de los recursos, bienes y los sistemas de información de la entidad y recomendar los correctivos necesarios.
  - ✓ Fomentar en toda la organización la formación de una cultura de control que contribuya al mejoramiento continuo en el cumplimiento de la misión institucional.
  - ✓ Mantener permanentemente informado al titular de la institución acerca de los resultados de la evaluación de la estructura de control interno dando cuenta de las debilidades detectadas y de las sugerencias para su fortalecimiento.
  - ✓ Verificar que se implanten las recomendaciones presentadas por la
  - ✓ Contraloría General de la República y por las propias unidades de auditoría interna.

- **Comité de Auditoría:** Las organizaciones deberán de crear una entidad que este en los más alto de la jerarquía, un Comité de Auditoría con el propósito de ejecutar el seguimiento periódico de los resultados y recomendaciones formuladas por la unidad de auditoría interna y o por auditores externos. Este comité deberá de incluir como mínimo a tres miembros:
  - ✓ Representante del más alto nivel de la administración
  - ✓ El Auditor Interno
  - ✓ El funcionario responsable del área o actividad objeto de la auditoría

- **Funciones del Comité de Auditoría:** Actúa como un órgano consultivo de la alta dirección y tendrá como funciones las siguientes:
  - ✓ Notificar a la Auditoría Interna las prioridades identificadas a los fines de considerarlo en el Plan Anual de Auditoria
  - ✓ Conocer los informes de las Auditorías Internas y Externas, ponderar la importancia del contenido de las recomendaciones y ejecutar el seguimiento de los acuerdos del Comité
  - ✓ Reglamentar el funcionamiento del Comité para asegurar el seguimiento y cumplimiento de las recomendaciones
- **Informes de Auditoría Interna:** La Contraloría General de la República solicitará de manera discrecional, los informes en los que presenten el resultado de la ejecución del Plan Anual de Auditoría Interna de acuerdo a lo establecido en las leyes.
- **Aplicación de la Recomendaciones:** La alta dirección queda con la responsabilidad de elaborar un plan y cronograma con la finalidad de aplicar las recomendaciones definidas en el informe de auditoría interna.

2. ANEXO B

- **Evaluación de la estructura del control interno:** Se debe de realizar una adecuada investigación sobre los controles internos existentes en la organización con la finalidad de definir la efectividad de los controles internos implementados y determinar los riesgos de control así como identificar las áreas críticas; e informar al auditado sobre ellas y que medidas debe de tomar para mitigarlas. Esta norma define cinco componentes del control interno:
  - **Ambiente de control:** Se refiere a como las organizaciones estimulen e influyen en su personal para que tomen conciencia de la importancia de la existencia de un control interno.
  - **Evaluación del riesgo:** Consiste en la forma como la organización identifica, analiza y administra los riesgos que amenazan el cumplimiento de sus objetivos.
  - **Actividades de control Gerencial:** Son las políticas y procedimientos que imparte la alta dirección de la organización con la finalidad de garantizar el cumplimiento de sus objetivos.
  - **Sistemas de información y Comunicación:** Consiste en los métodos y procedimientos establecidos por la alta dirección de la organización para procesar la información y dar cuenta de las operaciones para fines de toma de decisiones**.**
  - **Actividades de monitoreo:** La alta dirección tiene la responsabilidad de implementar y mantener el control interno, para lo cual los evalúa teniendo dos etapas:
    - ✓ Obtención de información relacionada con el diseño e implementación de los controles sujetos a evaluación.
    - ✓ Comprobación de que los controles funcionan efectivamente y logran sus objetivos.

  Al término de esta evaluación se deberá emitir el documento denominado Memorándum de Control Interno a la alta dirección.

- **Evaluación del cumplimiento de disposiciones legales y reglamentarias:** En la ejecución de la Auditoria Gubernamental se debe de corroborar el cumplimiento de las leyes y reglamentos vigentes y aplicables cuando sean necesarios para los

objetivos de la auditoria. Para ellos el auditor debe de tener pleno conocimiento sobre los objetivos de la organización y además deberá:

- ✓ Determinar la normativa que pueda tener un efecto directo y significativo en los estados financieros, información presupuestaria o área auditada
- ✓ Elaborar procedimientos de auditoría que permitan verificar el cumplimiento la normativa aplicable o de estipulaciones contractuales
- ✓ Evaluar los resultados de dichas pruebas

- **Supervisión del trabajo de auditoría:** El trabajo de auditoría debe de ser supervisado durante todo su proceso con la finalidad de asegurar los objetivos propuesto, mejorar la calidad del informe de Auditoría, asegurar la eficiencia, eficacia y economía de los recursos de la auditoria, promover el entrenamiento técnico y la capacidad profesional de los auditores y orientar el trabajo de los mismos.

  Los miembros que conforman el equipo de supervisión de la auditoria y las funciones que ellos ejercen deben de estar registrados en los papeles de trabajo durante el desarrollo de la auditoria con la finalidad de establecer la oportunidad y el aporte técnico al trabajo de auditoría.

  La participación en los trabajo de auditoría a supervisar dependerá de los objetivos y alcance de la auditoria definidos en el documento de Planeamiento de dicha auditoria.

- **Evidencia suficiente, competente y relevante:** La evidencia obtenida por el auditor debe de tener las siguientes características:
  - ➢ **Suficiente:** La evidencia objetiva y convincente es suficiente cuando por si sola sustenta los hallazgos, conclusiones y recomendaciones expresadas en el informe.
  - ➢ **Competencia:** Para ser competente la evidencia debe de ser válida y confiable por lo tanto deben de cumplir con los siguientes criterios:
    - ✓ La evidencia obtenida por fuentes independientes es más confiable que a obtenida del propio organismo auditado
    - ✓ La evidencia obtenida de un sistema de control interno apropiado es más confiable que aquella que se obtiene de un control interno deficiente
    - ✓ Los documentos originales son más confiables que sus copias

- ✓ La evidencia testimonial que se obtiene en circunstancias en donde el informante puede expresarse con libertad es más confiable que aquellas obtenidas en circunstancias comprometedoras

➢ **Relevantes:** La evidencia debe ser útil para demostrar o refutar un hecho o de lo contrario será irrelevante y no podrá incluirse como evidencia.

- **Papeles de trabajo:** El auditor debe de organizar un registro ordenado, completo y detallado de la labor efectuada y las conclusiones alcanzadas, en forma de papeles de trabajo. Tienen los siguientes propósitos:
  - ✓ Contribuir a la planeación y realización de la auditoria.
  - ✓ Proporcionar el principal sustento del informe del auditor.
  - ✓ Permitir una adecuada ejecución, revisión y supervisión del trabajo de auditoria.
  - ✓ Contribuir la evidencia del trabajo realizado y el soporte de las conclusiones, comentarios y recomendaciones incluidas en el informe.
  - ✓ Permitir la revisión de calidad del informe de auditoría.

3. ANEXO C

- Políticas de seguridad de la información: Según el estándar internacional ISO20072, se debe de proporcionar la dirección gerencial y el soporte para la seguridad de la información mediante el establecimiento de reglas.

- Aspectos organizativos para la seguridad: Según el estándar internacional ISO20072, se debe de :

  - ✓ Administrar la seguridad de la información dentro de la compañía
  - ✓ Mantener la seguridad de la infraestructura de procesamiento de la información y de los activos de organización accedidos por terceros.
  - ✓ Mantener la seguridad de la información cuando la responsabilidad del procesamiento de la información ha sido tercerizada a otra organización.

- Seguridad ligada al personal: Según el estándar internacional ISO20072, se debe de reducir riesgos de error humano, hurto, fraude o mal uso de instalaciones y equipos; asegurarse de que los usuarios estén enterados de las amenazas de seguridad de la información, y estén capacitados para apoyar la política corporativa de seguridad en el curso de su trabajo normal; reducir al mínimo el daño por incidentes y mal funcionamiento de la seguridad y aprender de tales incidentes.

- Clasificación y control de activos: Según el estándar internacional ISO20072, se debe de mantener la protección apropiada de activos corporativos y asegurarse de que los activos de información cuentan con un nivel apropiado de protección.

- Seguridad física y del entorno: Según el estándar internacional ISO20072, se debe de prevenir el acceso no autorizado, el daño e interferencia a las instalaciones, recursos e información; para prevenir pérdida, ó daño de activos y la interrupción de las actividades por hurto de activos e información y por desastres.

- Gestión de comunicaciones y operaciones: Según el estándar internacional ISO20072, se debe de:
  - ✓ Asegurar la operación correcta de los equipos y el procesamiento de la información
  - ✓ Minimizar el riesgo de fallos de los sistemas
  - ✓ Proteger la integridad del software y de la información

- ✓ Mantener la integridad y la disponibilidad del procesamiento y de la información y comunicaciones
- ✓ Salvaguardar la información que se transfiere a través de las redes
- ✓ Prevenir daño a los activos e interrupciones a las actividades
- ✓ Prevenir la pérdida, la modificación o el uso erróneo de la información que se transfiere a través de las redes.

- Control de accesos: Según el estándar internacional ISO20072, se debe de:
  - ✓ Controlar el acceso a la información
  - ✓ Prevenir el acceso no autorizado a los sistemas de información;
  - ✓ Asegurar la protección de servicios de red
  - ✓ Prevenir el acceso no autorizado a las computadoras
  - ✓ Detectar actividades no autorizadas
  - ✓ Asegurar la información al usar cómputo móvil y servicios de red a distancia.

- Desarrollo y mantenimiento de sistemas: Según el estándar internacional ISO20072, se debe de:
  - ✓ Garantizar la seguridad de los sistemas operativos
  - ✓ Prevenir pérdida, modificación o uso erróneo de los datos del usuario en los sistemas
  - ✓ Proteger la confidencialidad, la autenticidad y la integridad de la información
  - ✓ Garantizar que los proyectos de tecnologías de la información y el soporte se conduzcan de manera segura
  - ✓ Mantener la seguridad de las aplicaciones y los datos que usa

- Gestión de continuidad del negocio: Según el estándar internacional ISO20072, se debe de contrarrestar interrupciones de las actividades y proteger los procesos críticos como consecuencia de fallas o desastres importantes.

- Conformidad legal: Según el estándar internacional ISO20072, se debe de:
  - ✓ Evitar incumplimiento de cualquier ley civil o penal, obligación estatutaria, reguladora o contractual y de algún requerimiento de seguridad
  - ✓ Asegurar la conformidad de los sistemas con políticas de seguridad y estándares de la organización

- ✓ Maximizar la efectividad y reducir al mínimo los procesos de auditoría de sistemas

- Cumplimiento: Según el estándar internacional ISO20072, se debe de promover el cumplimiento de los requerimientos legales, políticas y estándares de seguridad ; además de cumplimiento de especificaciones técnicas.

- Definir la arquitectura de la información: Según el marco de referencia COBIT 5.0, se debe:
  - ✓ Establecer y mantener un modelo de información empresarial
  - ✓ Mantener un diccionario de datos empresarial
  - ✓ Establecer un esquema de clasificación de datos que aplique a toda la empresa
  - ✓ Definir e implantar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico, tales como bases de datos, almacenes de datos y archivos

- Administrar la calidad: Según el marco de referencia COBIT 5.0, se debe de:
  - ✓ Establecer y mantener un sistema de administración de calidad que proporcione un enfoque estándar, formal y continuo, con respecto a la administración de la calidad, que esté alineado con los requerimientos del negocio
  - ✓ Identificar y mantener estándares, procedimientos y prácticas para los procesos clave de TI para orientar a la organización hacia el cumplimiento del sistema de administración de calidad
  - ✓ Adoptar y mantener estándares para todo el desarrollo y adquisición que siguen el ciclo de vida, hasta el último entregable e incluyen la aprobación en puntos clave con base en criterios de aprobación acordados
  - ✓ Elaborar y comunicar un plan global de calidad que promueva la mejora continua, de forma periódica
  - ✓ Garantiza que la administración de calidad se enfoque en los clientes, al determinar sus requerimientos y alinearlos con los estándares y prácticas de TI
  - ✓ Definir, planear e implantar mediciones para monitorear el cumplimiento continuo del sistema de administración de calidad, así como el valor que este proporciona

- Educar y entrenar a los usuarios : Según el marco de referencia COBIT 5.0, se debe:
  - ✓ Establecer y actualizar de forma regular un programa de entrenamiento para cada grupo objetivo de empleados
  - ✓ Identificar a los grupos objetivo y a sus miembros, a los mecanismos de impartición eficientes, a maestros, instructores y consejeros
  - ✓ Evaluar el contenido de la entrenamiento respecto a la relevancia, calidad, efectividad, percepción y retención del conocimiento, costo y valor

- Administrar la información: Según el marco de referencia COBIT 5.0, se debe:
  - ✓ Establecer mecanismos para garantizar que el negocio reciba los documentos originales que espera, que se procese toda la información
  - ✓ Definir e implementar procedimientos para el archivo y almacenamiento de los datos, de manera que los datos permanezcan accesibles y utilizables
  - ✓ Definir e implementar procedimientos para mantener un inventario de medios en sitio y garantizar su integridad y su uso
  - ✓ Definir e implementar procedimientos para prevenir el acceso a datos sensitivos y al software desde equipos o medios una vez que son eliminados o transferidos para otro uso
  - ✓ Definir e implementar procedimientos de respaldo y restauración de los sistemas, datos y configuraciones que estén alineados con los requerimientos del negocio y con el plan de continuidad
  - ✓ Establecer mecanismos para identificar y aplicar requerimientos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos

- Monitorear y evaluar el control interno: Según el marco de referencia COBIT 5.0, se debe:
  - ✓ Monitorear de forma continua el ambiente de control y el marco de control de TI.
  - ✓ Monitorear y reportar la efectividad de los controles internos sobre TI por medio de revisiones de auditoría incluyendo
  - ✓ Registrar la información referente a todas las excepciones de control y garantizar que esto conduzca al análisis de las causas subyacentes y a la toma de acciones correctivas

- ✓ Evaluar la completitud y efectividad de los controles internos de la administración de los procesos, políticas y contratos de TI por medio de un programa continuo de auto-evaluación
- ✓ Obtener, según sea necesario, aseguramiento adicional de la completitud y efectividad de los controles internos por medio de revisiones de terceros.
- ✓ Determinar el estado de los controles internos de cada proveedor externos de servicios
- ✓ Identificar e iniciar medidas correctivas basadas en las evaluaciones y en los reportes de control

- Garantizar el cumplimiento regulatorio : Según el marco de referencia COBIT 5.0, se debe de:
  - ✓ Definir e implantar un proceso para garantizar la identificación oportuna de requerimientos locales e internacionales legales, contractuales, de políticas y regulatorios, relacionados con la información, con la prestación de servicios de información – incluyendo servicios de terceros – y con la función, procesos e infraestructura de TI
  - ✓ Revisar y optimizar las políticas, estándares y procedimientos de TI para garantizar que los requisitos legales y regulatorios se cubran de forma eficiente.
  - ✓ Evaluar de forma eficiente el cumplimiento de las políticas, estándares y procedimientos de TI, incluyendo los requerimientos legales y regulatorios, con base en la supervisión del gobierno de la gerencia de TI y del negocio y la operación de los controles internos.
  - ✓ Definir e implantar procedimientos para obtener y reportar un aseguramiento del cumplimiento y, donde sea necesario, que el propietario del proceso haya tomado las medidas correctivas oportunas para resolver cualquier brecha de cumplimiento
  - ✓ Integrar los reportes de TI sobre cumplimiento regulatorio con las salidas similares provenientes de otras funciones del negocio.

- Mantenimiento de la seguridad, integridad y respaldo de la data: Según la publicación numero 800-34 de la National Institute of Standards and Technology (NIST), se debe de mantener la integridad y la seguridad del sistema de datos y software ya que es una llave importante en la planificación de contingencias

- Identificación de almacenamiento alternativo y las instalaciones de procesamiento: Según la publicación numero 800-34 de la National Institute of Standards and Technology (NIST), los medios de copia de seguridad se deben de almacenar fuera del área laboral en un lugar seguro y ambientalmente controlado.

- Uso de la alta disponibilidad de los procesos : Según la publicación numero 800-34 de la National Institute of Standards and Technology (NIST), se debe de integrar los procesos de de redundancia y de recuperación de fallos para maximizar su tiempo de actividad y la disponibilidad.

- Definir un plan estratégico de TI: Según el marco de referencia COBIT 5.0, se debe:
  - ✓ Trabajar con el negocio para garantizar que el portafolio de inversiones de TI de la empresa contenga programas con casos de negocio sólidos.
  - ✓ Educar a los ejecutivos sobre las capacidades tecnológicas actuales y sobre el rumbo futuro, sobre las oportunidades que ofrece TI, y sobre qué debe hacer el negocio para capitalizar esas oportunidades.
  - ✓ Evaluar el desempeño de los planes existentes y de los sistemas de información en términos de su contribución a los objetivos de negocio, su funcionalidad, su estabilidad, su complejidad, sus costos, sus fortalezas y debilidades.
  - ✓ Crear un plan estratégico que defina, en cooperación con los interesados relevantes, cómo la TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados. Incluye cómo la TI dará soporte a los programas de inversión facilitados por TI y a la entrega de los servicios operacionales}
  - ✓ Crear un portafolio de planes tácticos de TI que se deriven del plan estratégico de TI
  - ✓ Administrar de forma activa, junto con el negocio, el portafolio de programas de inversión de TI requerido para lograr objetivos de negocio estratégicos y específicos por medio de la identificación, definición, evaluación, asignación de prioridades, selección, inicio, administración y control de los programas

- Determinar la dirección tecnológica: Según el marco de referencia COBIT 5.0, se debe:

- ✓ Analizar las tecnologías existentes y emergentes y planear cuál dirección tecnológica es apropiado tomar para materializar la estrategia de TI y la arquitectura de sistemas del negocio.
- ✓ Crear y mantener un plan de infraestructura tecnológica que esté de acuerdo con los planes estratégicos y tácticos de TI.
- ✓ Establecer un proceso para monitorear las tendencias ambientales del sector / industria, tecnológicas, de infraestructura, legales y regulatorias. Incluir las consecuencias de estas tendencias en el desarrollo del plan de infraestructura tecnológica de TI.
- ✓ Proporcionar soluciones tecnológicas consistentes, efectivas y seguras para toda la empresa, establecer un foro tecnológico para brindar directrices tecnológicas, asesoría sobre los productos de la infraestructura y guías sobre la selección de la tecnología, y medir el cumplimiento de estos estándares y directrices
- ✓ Establecer un consejo de arquitectura de TI que proporcione directrices sobre la arquitectura y asesoría sobre su aplicación y que verifique el cumplimiento.

- Definir los procesos, organización y relaciones de TI: Según el marco de referencia COBIT 5.0, se debe:
  - ✓ Definir un marco de trabajo para el proceso de TI para ejecutar el plan estratégico de TI.
  - ✓ Establecer un comité estratégico de TI a nivel del consejo directivo.
  - ✓ Establecer un comité directivo de TI (o su equivalente) compuesto por la gerencia ejecutiva, del negocio y de TI
  - ✓ Ubicar a la función de TI dentro de la estructura organizacional general con un modelo de negocios supeditado a la importancia de TI dentro de la empresa, en especial en función de que tan crítica es para la estrategia del negocio y el nivel de dependencia operativa sobre TI.
  - ✓ Establecer una estructura organizacional de TI interna y externa que refleje las necesidades del negocio.
  - ✓ Definir y comunicar los roles y las responsabilidades para todo el personal en la organización con respecto a los sistemas de información para permitir que ejerzan los roles y responsabilidades asignados con suficiente autoridad.

- ✓ Asignar la responsabilidad para el desempeño de la función de aseguramiento de calidad y proporcionar al grupo de aseguramiento los sistemas de aseguramiento de calidad, los controles y la experiencia para comunicarlos.
- ✓ Incluir la propiedad y la responsabilidad de los riesgos relacionados con TI a un nivel senior apropiado.
- ✓ Proporcionar al negocio los procedimientos y herramientas que le permitan enfrentar sus responsabilidades de propiedad sobre los datos y los sistemas de información.
- ✓ Implantar prácticas adecuadas de supervisión dentro de la función de TI para garantizar que los roles y las responsabilidades se ejerzan de forma apropiada, para evaluar si todo el personal cuenta con la suficiente autoridad y recursos para ejecutar sus roles y responsabilidades y para revisar en general los indicadores clave de desempeño
- ✓ Implantar una división de roles y responsabilidades que reduzca la posibilidad de que un solo individuo afecte negativamente un proceso crítico.
- ✓ Evaluar los requerimientos de personal de forma regular o cuando existan cambios importantes en el ambiente de negocios, operativo o de TI para garantizar que la función de TI cuente con un número suficiente de personal competente
- ✓ Definir e identificar al personal clave de TI y minimizar la dependencia excesiva en ellos
- ✓ Definir e implantar políticas y procedimientos para controlar las actividades de los consultores y otro personal contratado por la función de TI para garantizar la protección de los activos de información de la empresa y satisfacer los requerimientos contractuales.
- ✓ Establecer y mantener una estructura óptima de enlace, comunicación y coordinación entre la función de TI y otras funciones dentro y fuera de la función de TI

- Comunicar las aspiraciones y la dirección de la gerencia: : Según el marco de referencia COBIT 5.0, se debe:
  - ✓ Definir los elementos de un ambiente de control para TI, alineados con la filosofía administrativa y el estilo operativo de la empresa.

- ✓ Elaborar y dar mantenimiento a un marco de trabajo que establezca el enfoque empresarial general hacia los riesgos y hacia el control interno para entregar valor mientras al mismo tiempo se protegen los recursos y sistemas de TI
- ✓ Elaborar y dar mantenimiento a un conjunto de políticas que apoyen la estrategia de TI.
- ✓ Asegurar que las políticas de TI se implantan y se comunican a todo el personal relevante, y se refuerzan, de tal forma que estén incluidas y sean parte integral de las operaciones empresariales.
- ✓ Asegurar que la conciencia y el entendimiento de los objetivos y la dirección del negocio y de TI se comunican a toda la organización.

- Administrar los recursos humanos de TI: Según el marco de referencia COBIT 5.0, se debe:
  - ✓ Asegurar que los procesos de reclutamiento del personal de TI estén de acuerdo a las políticas y procedimientos generales de personal de la organización
  - ✓ Verificar de forma periódica que el personal tenga las habilidades para cumplir sus roles con base en su educación, entrenamiento y/o experiencia
  - ✓ Definir, monitorear y supervisar los marcos de trabajo para los roles, responsabilidades y compensación del personal, incluyendo el requisito de adherirse a las políticas y procedimientos administrativos, así como al código de ética y prácticas profesionales.
  - ✓ Proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo para conservar su conocimiento, aptitudes, habilidades, controles internos y conciencia sobre la seguridad, al nivel requerido para alcanzar las metas organizacionales.
  - ✓ Minimizar la exposición a dependencias críticas sobre individuos clave por medio de la captura del conocimiento (documentación), compartir el conocimiento, planeación de la sucesión y respaldos de personal.
  - ✓ Incluir verificaciones de antecedentes en el proceso de reclutamiento de TI. El grado y la frecuencia de estas verificaciones dependen de que tan delicada ó crítica sea la función y se deben aplicar a los empleados, contratistas y proveedores.

- ✓ Es necesario que las evaluaciones de desempeño se realicen periódicamente, comparando contra los objetivos individuales derivados de las metas organizacionales, estándares establecidos y responsabilidades específicas del puesto.
- ✓ Tomar medidas expeditas respecto a los cambios en los puestos, en especial las terminaciones.

- Facilitar la operación y el uso: Según el marco de referencia COBIT 5.0, se debe:
  - ✓ Desarrollar un plan para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos, de manera que todos los interesados puedan tomar la responsabilidad oportunamente por la producción de procedimientos de administración, de usuario y operacionales, como resultado de la introducción o actualización de sistemas automatizados o de infraestructura.
  - ✓ Transferir el conocimiento a la gerencia de la empresa para permitirles tomar posesión del sistema y los datos y ejercer la responsabilidad por la entrega y calidad del servicio, del control interno, y de los procesos administrativos de la aplicación
  - ✓ Transferencia de conocimiento y habilidades para permitir que los usuarios finales utilicen con efectividad y eficiencia el sistema de aplicación como apoyo a los procesos del negocio.
  - ✓ Transferir el conocimiento y las habilidades para permitir al personal de soporte técnico y de operaciones que entregue, apoye y mantenga la aplicación y la infraestructura asociada de manera efectiva y eficiente de acuerdo a los niveles de servicio requeridos.

- Instalar y acreditar soluciones y cambios: Según el marco de referencia COBIT 5.0, se debe:
  - ✓ Entrenar al personal de los departamentos de usuario afectados y al grupo de operaciones de la función de TI de acuerdo con el plan definido de entrenamiento e implantación y a los materiales asociados, como parte de cada proyecto de desarrollo, implantación o modificación de sistemas de información.
  - ✓ Establecer un plan de pruebas y obtener la aprobación de las partes relevantes.

- ✓ Establecer un plan de implantación y obtener la aprobación de las partes relevantes.
- ✓ Establecer un ambiente de prueba separado para pruebas.
- ✓ Garantizar que los métodos de desarrollo de la organización, contemplen para todos los proyectos de desarrollo, implantación o modificación, que todos los elementos necesarios, tales como hardware, software, datos de transacciones, archivos maestros, respaldos y archivos, interfases con otros sistemas, procedimientos, documentación de sistemas, etc., sean convertidos del viejo al nuevo sistema de acuerdo con un plan preestablecido. Se desarrolla y mantiene una pista de auditoría de los resultados previos y posteriores a la conversión
- ✓ Garantizar que se prueban los cambios de acuerdo con el plan de aceptación definido y en base en una evaluación de impacto y recursos que incluye el dimensionamiento del desempeño en un ambiente separado de prueba
- ✓ Garantizar que los procedimientos proporcionan, como parte de la aceptación final o prueba de aseguramientos de la calidad de los sistemas de información nuevos o modificados, una evaluación formal y la aprobación de los resultados de prueba por parte de la gerencia de los departamentos afectados del usuario y la función de TI.
- ✓ Implantar procedimientos formales para controlar la transferencia del sistema desde el ambiente de desarrollo al de pruebas, de acuerdo con el plan de implantación.
- ✓ Garantizar que la liberación del software se regula con procedimientos formales que aseguren la autorización, acondicionamiento, pruebas de regresión, distribución, transferencia de control, rastreo de estatus, procedimientos de respaldo y notificación de usuario.
- ✓ Establecer procedimientos de control para asegurar la distribución oportuna y correcta, y la actualización de los componentes aprobados de la configuración.
- ✓ Automatizar el sistema utilizado para monitorear cambios a sistemas aplicativos para soportar el registro y rastreo de cambios hechos en aplicaciones, procedimientos, procesos, sistemas y parámetros de servicio, y a las plataformas subyacentes.
- ✓ Establecer procedimientos de acuerdo con los estándares de desarrollo y de cambios de la empresa, que requieren una revisión posterior a la implantación del sistema de información en operación para evaluar y reportar si el cambio

satisfizo los requerimientos del cliente y entregó los beneficios visualizados, de la forma más rentable.

- Definir y administrar los niveles de servicio: Según el marco de referencia COBIT 5.0, se debe:
  - ✓ Definir un marco de trabajo que brinde un proceso formal de administración de niveles de servicio entre el cliente y el prestador de servicio.
  - ✓ Definir y acordar convenios de niveles de servicio para todos los procesos críticos de TI con base en los requerimientos del cliente y las capacidades en TI.
  - ✓ Asegurar que los acuerdos de niveles de operación expliquen cómo serán entregados técnicamente los servicios para soportar los acuerdos de nivel de servicio de manera óptima
  - ✓ Monitorear continuamente los criterios de desempeño especificados para el nivel de servicio.
  - ✓ Revisar regularmente con los proveedores internos y externos los acuerdos de niveles de servicio y los contratos de apoyo, para asegurar que son efectivos, que están actualizados y que se han tomado en cuenta los cambios en requerimientos.

- Garantizar la seguridad de los sistemas: Según el marco de referencia COBIT 5.0, se debe:
  - ✓ Administrar la seguridad de TI al nivel más apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio.
  - ✓ Trasladar los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI.
  - ✓ Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por la gerencia de cuentas de usuario.
  - ✓ Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa
  - ✓ Garantizar que las características de los posibles incidentes de seguridad sean definidas y comunicadas de forma clara, de manera que los problemas de

seguridad sean atendidos de forma apropiada por medio del proceso de administración de problemas o incidentes.

- ✓ Garantizar que la tecnología importante relacionada con la seguridad no sea susceptible de sabotaje y que la documentación de seguridad no se divulgue de forma innecesaria, es decir, que mantenga un perfil bajo
- ✓ Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas
- ✓ Garantizar que se cuente con medidas de prevención, detección y corrección (en especial contar con parches de seguridad y control de virus actualizados) a lo largo de toda la organización para proteger a los sistemas de información y a la tecnología contra software malicioso (virus, gusanos, spyware, correo basura, software fraudulento desarrollado internamente, etc.).
- ✓ Garantizar que se utilizan técnicas de seguridad y procedimientos de administración asociados (por ejemplo, firewalls, dispositivos de seguridad, segmentación de redes, y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.
- ✓ Garantizar que las transacciones de datos sensibles sean intercambiadas solamente a través de una ruta o medio confiable con controles para brindar autenticidad de contenido, prueba de envío, prueba de recepción y no rechazo del origen

- Administrar la mesa de servicio y los incidentes: Según el marco de referencia COBIT 5.0, se debe:
  - ✓ Establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información
  - ✓ Establecer una función y sistema que permita el registro y rastreo de llamadas, incidentes, solicitudes de servicio y necesidades de información.
  - ✓ Establecer procedimientos de mesa de servicios de manera que los incidentes que no puedan resolverse de forma inmediata sean escalados apropiadamente de acuerdo con los límites acordados en el acuerdo de nivel de servicio y, si es adecuado, brindar soluciones alternas

- ✓ Establecer procedimientos para el monitoreo puntual de la resolución de consultas de los clientes.
- ✓ Emitir reportes de la actividad dela mesa de servicios para permitir a la gerencia medir el desempeño del servicio y los tiempos de respuesta, así como para identificar tendencias de problemas recurrentes de forma que el servicio pueda mejorarse de forma continua.

- Administrar los problemas: Según el marco de referencia COBIT 5.0, se debe garantizar la satisfacción de los usuarios finales con ofrecimientos de servicios y niveles de servicio, y reducir el retrabajo y los defectos de la prestación de los servicios y de las soluciones

- Administrar las operaciones: Según el marco de referencia COBIT 5.0, se debe mantener la integridad de la información y garantizar que la infraestructura de TI pueda resistir y recuperarse de errores y fallas

- Monitorear y evaluar el desempeño de TI: : Según el marco de referencia COBIT 5.0, se debe:
  - ✓ Garantizar que la gerencia establezca un marco de trabajo de monitoreo general y un enfoque que definan el alcance, la metodología y el proceso a seguir para monitorear la contribución de TI a los resultados de los procesos de administración de programas y de administración del portafolio empresarial y aquellos procesos que son específicos para la entrega de la capacidad y los servicios de TI
  - ✓ Garantizar que la gerencia de TI, trabajando en conjunto con el negocio, defina un conjunto balanceado de objetivos, mediciones, metas y comparaciones de desempeño y que estas se encuentren acordadas formalmente con el negocio y otros interesados relevantes
  - ✓ Garantizar que el proceso de monitoreo implante un método (ej. Balanced Scorecard), que brinde una visión sucinta y desde todos los ángulos del desempeño de TI y que se adapte al sistema de monitoreo de la empresa.
  - ✓ Comparar de forma periódica el desempeño contra las metas, realizar análisis de la causa raíz e iniciar medidas correctivas para resolver las causas subyacentes

- ✓ Proporcionar reportes administrativos para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas, específicamente en términos del desempeño del portafolio empresarial de programas de inversión habilitados por TI, niveles de servicio de programas individuales y la contribución de TI a ese desempeño
- ✓ Identificar e iniciar medidas correctivas basadas en el monitoreo del desempeño, evaluación y reportes

- Garantizar el cumplimiento regulatorio: Según el marco de referencia COBIT 5.0, se debe:
  - ✓ Definir e implantar un proceso para garantizar la identificación oportuna de requerimientos locales e internacionales legales, contractuales, de políticas y regulatorios, relacionados con la información, con la prestación de servicios de información – incluyendo servicios de terceros – y con la función, procesos e infraestructura de TI.
  - ✓ Revisar y optimizar las políticas, estándares y procedimientos de TI para garantizar que los requisitos legales y regulatorios se cubran de forma eficiente.
  - ✓ Evaluar de forma eficiente el cumplimiento de las políticas, estándares y procedimientos de TI, incluyendo los requerimientos legales y regulatorios, con base en la supervisión del gobierno de la gerencia de TI y del negocio y la operación de los controles internos.
  - ✓ Definir e implantar procedimientos para obtener y reportar un aseguramiento del cumplimiento y, donde sea necesario, que el propietario del proceso haya tomado las medidas correctivas oportunas para resolver cualquier brecha de cumplimiento. Integrar los reportes de avance y estado del cumplimiento de TI con salidas similares provenientes de otras funciones de negocio
  - ✓ Integrar los reportes de TI sobre cumplimiento regulatorio con las salidas similares provenientes de otras funciones del negocio
  - ✓ Proporcionar Gobierno de TI
  - ✓ Trabajar con el consejo directivo para definir y establecer un marco de trabajo para el gobierno de TI, incluyendo liderazgo, procesos, roles y responsabilidades, requerimientos de información, y estructuras organizacionales para garantizar que los programas de inversión habilitados por

TI de la empresa ofrezcan y estén alineados con las estrategias y objetivos empresariales

- ✓ Facilitar el entendimiento del consejo directivo y de los ejecutivos sobre temas estratégicos de TI tales como el rol de TI, características propias y capacidades de la tecnología.
- ✓ Administrar los programas de inversión habilitados con TI, así como otros activos y servicios de TI, para asegurar que ofrezcan el mayor valor posible para apoyar la estrategia y los objetivos empresariales.
- ✓ Optimizar la inversión, uso y asignación de los activos de TI por medio de evaluaciones periódicas, garantizando que TI cuente con recursos suficientes, competentes y capaces para ejecutar los objetivos estratégicos actuales y futuros y seguir el ritmo de los requerimientos del negocio.
- ✓ Trabajar en conjunto con el consejo directivo para definir el nivel de riesgo de TI aceptable por la empresa.
- ✓ Informar el desempeño relevante del portafolio de los programas de TI al consejo directivo y a los ejecutivos de manera oportuna y precisa
- ✓ Garantizar que la organización establezca y mantenga una función competente y que cuente con el personal adecuado y/o busque servicios de aseguramiento externo para proporcionar al consejo directivo– esto ocurrirá probablemente a través de un comité de auditoría – aseguramiento independiente y oportuno sobre el cumplimiento que tiene TI respecto a sus políticas, estándares y procedimientos, así como con las prácticas generalmente aceptadas.

- Desarrollar Consideraciones de contingencia para las telecomunicaciones: Según la publicación numero 800-34 de la National Institute of Standards and Technology (NIST), se debe revisar los siguientes puntos:
  - ✓ La red de telecomunicaciones
  - ✓ Coordinaciones con los proveedores
  - ✓ Coordinaciones con las políticas de seguridad y controles
  - ✓ Los puntos únicos de fallo
  - ✓ Implementación de redundancia en componentes críticos
  - ✓ Monitoreo de la red de telecomunicaciones

- Desarrollar Consideraciones de contingencia de los servidores: Según la publicación numero 800-34 de la National Institute of Standards and Technology (NIST), se debe tomar las siguientes medidas al determinar los requisitos centrales de contingencia:
  - ✓ Administrar copias de respaldo fuera del área laboral
  - ✓ Documentar las configuraciones de los sistemas y los proveedores
  - ✓ Coordinar con las políticas de seguridad y sistemas de control de seguridad

- Desarrollar Consideraciones de contingencia de los sistemas cliente/servidor: Según la publicación numero 800-34 de la National Institute of Standards and Technology (NIST), se debe de hacer hincapié en la disponibilidad de datos, la confidencialidad y la integridad, tanto en el nivel de sistema del servidor y el nivel de cliente. Para hacer frente a estos requerimientos, copias de seguridad periódicas y frecuentes de los datos deben ser almacenados fuera del área laboral.

4. ANEXO D

Aspecto	Criterio	Auditado	Documentos a pedir	Objetivo de revisión del documento	Ejecutar trabajo de campo
Información	Políticas de seguridad de la información	Gerencia	Documento de la política de seguridad de la información	Verificar una definición de seguridad de la información, sus objetivos y alcance generales y la importancia de la seguridad como un mecanismo facilitador para intercambiar información Verificar un enunciado de la intención de la gerencia, fundamentando sus objetivos y los principios de la seguridad de la información en línea con la estrategia y los objetivos comerciales Verificar un marco referencial para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación del riesgo y la gestión de riesgo Verificar una explicación breve de las políticas, principios, estándares y requerimientos de conformidad de la seguridad de particular importancia para la organización, incluyendo: 1. conformidad con los requerimientos legislativos, reguladores y restrictivos. 2. educación, capacitación y conocimiento de seguridad. 3. gestión de la continuidad del negocio. 4. consecuencias de las violaciones de la política de seguridad de la información. Verificar una definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información incluyendo el reporte de incidentes de seguridad de la información. Verificar referencias a la documentación que fundamenta la política; por ejemplo, políticas y procedimientos de seguridad más detallados para sistemas de información específicos o reglas de seguridad que los usuarios debieran observar.	Recolectar la siguiente información: • Resultados de revisiones independientes • Estado de acciones preventivas y correctivas • Resultados de revisiones gerenciales previas • Desempeño del proceso y conformidad con la política de seguridad de la información • Cambios que podrían afectar el enfoque de la organización en el manejo de la seguridad de la información, incluyendo los cambios en el ambiente organizacional; las circunstancias comerciales; la disponibilidad de recursos; condiciones contractuales, reguladoras y legales; o el ambiente técnico; • Tendencias relacionadas con amenazas y vulnerabilidades; • Incidentes de seguridad de información reportados • Recomendaciones provistas por autoridades relevantes

Información	Aspectos organizativos para la seguridad	Gerencia Gerente de seguridad de información	Documento de la política de seguridad de la información Documento de creación de organismo de coordinación de la seguridad de la información Documento de asignación de responsabilidades de la seguridad de la información Autorización de proceso para facilidades procesadoras de información Acuerdos de confidencialidad Contacto con las autoridades Contacto con grupos de interés	Asegurar que los objetivos de seguridad de la información estén identificados, cumplan con los requerimientos organizacionales y estén integrados en los procesos relevantes Formular, revisar y aprobar la política de seguridad de la información Revisar la efectividad de la implementación de la política de seguridad de la información Proporcionar una dirección clara y un apoyo gerencial visible para las iniciativas de seguridad Proporcionar los recursos necesarios para la seguridad de la información Aprobar la asignación de roles y responsabilidades específicas para la seguridad de la información a lo largo de toda la organización Iniciar planes y programas para mantener la conciencia de seguridad de la información Asegurar que la implementación de los controles de seguridad de la información sea coordinada en toda la organización. Asegurar que las actividades de seguridad sean ejecutadas en conformidad con la política de seguridad de la información Identificar cómo manejar las no-conformidades Aprobar las metodologías y procesos para la seguridad de la información; por ejemplo, la evaluación del riesgo, la clasificación de la información; Identificar cambios significativos en las amenazas y la exposición de la información y los medios de procesamiento de la información ante amenazas	Revisar los medios de procesamiento de información a los cuales necesita tener acceso un grupo externo Revisar el tipo de acceso que tendría un grupo externo a la información y los medios de procesamiento de la información; por ejemplo: 1) acceso físico; por ejemplo, oficinas, edificios de cómputo, archivadores; 2) acceso lógico; por ejemplo, a las bases de datos o sistemas de información de la organización; 3) conectividad de red entre las redes de la organización y el grupo externo; por ejemplo, conexión permanente, acceso remoto 4) si el acceso se da fuera o dentro del local Revisar el valor y sensibilidad de la información involucrada, y su grado crítico para las operaciones comerciales Revisar los controles existentes para proteger la información que no está destinada a ser accesible para los grupos externos Revisar los diferentes medios y controles empleados por un grupo externo cuando almacena, procesa, comunica, comparte e intercambia información Medir el impacto del acceso no disponible para un grupo externo cuando lo requiere, y el grupo externo que ingresa o recibe información inexacta o confusa Revisar prácticas y procedimientos para lidiar con los incidentes en la seguridad de la información y los daños potenciales, y los términos y condiciones para la continuación del acceso del grupo externo en caso de un incidente en la seguridad de la información;

			especial	Evaluar la idoneidad y coordinar la implementación de los controles de la seguridad de información;	
			Revisiones independiente de la seguridad de la información	Promover de manera efectiva la educación, capacitación y conocimiento de la seguridad de la información a través de toda la organización	Revisar protección de activos, incluyendo: 1) procedimientos para proteger los activos de la organización, incluyendo información y software, y el manejo de las vulnerabilidades conocidas; 2) procedimientos para determinar si algún activo está comprometido; por ejemplo, cuando ha ocurrido una pérdida o modificación de data; 3) integridad; 4) restricciones sobre el copiado y divulgación de información;
			Riesgos relacionados con los grupos externos	Evaluar la información recibida del monitoreo y revisar los incidentes de seguridad de la información, y recomendar las acciones apropiadas en respuesta a los incidentes de seguridad de información identificados. Identificar y definir claramente los activos y procesos de seguridad asociados con cada sistema particular	Revisar las política de seguridad de la información
			Tratamiento de la seguridad cuando se lidia con clientes	Designar la entidad responsable de cada activo o proceso de seguridad y se debieran documentar los detalles de esta responsabilidad. Definir y documentar claramente los niveles de autorización.	Inspeccionar la capacitación del usuario y administrador en métodos, procedimientos y seguridad Inspeccionar las responsabilidades relacionadas con la instalación y mantenimiento de hardware y software
			Tratamiento de la seguridad en acuerdos con terceros	Verificar hardware y el software para asegurar que son compatibles con otros componentes del sistema Verificar el uso de facilidades para el procesamiento de información, bien sean personales o privadas pueden introducir nuevas vulnerabilidades y controles necesarios debieran ser identificados e implementados. Verificar una definición de la información a protegerse (por ejemplo, información confidencial) Verificar duración esperada de un acuerdo, incluyendo casos donde se podría necesitar mantener la confidencialidad indefinidamente Verificar acciones requeridas cuando se termina un acuerdo Verificar responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada	Revisar que se cuente una estructura de reporte clara y formatos de reporte acordados Revisar que las políticas de control de acceso contengan: 1) las diferentes razones, requerimientos y beneficios que hacen que sea necesario el acceso de terceros; 2) métodos de acceso permitidos, y el control y uso de identificadores singulares como IDs del usuario y claves secretas; 3) un proceso de autorización para el acceso y privilegios del usuario; 4) un requerimiento para mantener una lista de personas autorizadas a utilizar los servicios que se están poniendo a disposición, y los derechos y privilegios con respecto a este uso;

				Verificar la propiedad de la información, secretos comerciales y propiedad intelectual, y cómo se relaciona esto con la protección de la información confidencial Verificar el uso permitido de la información confidencial, y los derechos del firmante para utilizar la información Verificar el proceso de notificación y reporte de divulgación no autorizada o incumplimiento del acuerdo de información confidencial Verificar las condiciones para el retorno o destrucción de la información una vez que se termina el acuerdo; y acciones esperadas a realizarse en caso de incumplimiento de este acuerdo. Mejorar el conocimiento sobre las mejores prácticas y mantenerse al día con la información de seguridad relevantes Asegurar el entendimiento del ambiente de seguridad de la información sea actualizado y completo; Recibir advertencias tempranas de alertas, asesorías y avisos relacionados con ataques y vulnerabilidades Obtener acceso a consultoría especializada de seguridad de la información Compartir e intercambiar información sobre tecnologías, productos, amenazas o vulnerabilidades Proporcionar vínculos adecuados cuando se trata incidentes de seguridad de la información Verificar la política de control de acceso, abarcando : 1) métodos de acceso permitidos, y el control y uso de identificadores singulares como IDs del usuario y claves secretas; 2) un proceso de autorización para el acceso y privilegios del usuario; 3) un enunciado que establezca que está prohibido todo acceso que no esté	5) un enunciado que establezca que está prohibido todo acceso que no esté explícitamente autorizado; 6) un proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas; Revisar una descripción de cada servicio que debiera estar disponible, y una descripción de la información que debiera estar disponible junto con su clasificación de seguridad Inspeccionar las responsabilidades con respecto a temas legales y cómo asegurar que se cumplan los requerimientos legales Revisar las condiciones para la negociación/terminación de los acuerdos: 1) se debiera establecer un plan de contingencia en caso que alguna de las partes desee terminar la relación antes del fin del acuerdo 2) renegociación de acuerdos si los requerimientos de seguridad de la organización cambian 3) documentación actual de las listas de activos, licencias, acuerdos y derechos relacionados a ellos.

				explícitamente autorizado; 4) un proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas Verificar acuerdos para el reporte, notificación e investigación de las inexactitudes de la información (por ejemplo, de detalles personales), incidentes de seguridad de información y fallas en la seguridad; Verificar una descripción de cada servicio que debiera estar disponible y el nivel objetivo del servicio y los niveles inaceptables del servicio; Verificar el derecho a monitorear, y revocar, cualquier actividad relacionada con los activos de la organización Verificar las responsabilidades con respecto a temas legales y cómo asegurar que se cumplan los requerimientos legales; por ejemplo, la legislación de protección de data, especialmente tomando en cuenta los diferentes sistemas legales nacionales si el acuerdo involucra cooperación con los clientes en otros países Verificar derechos de propiedad intelectual (IPRs) y la asignación de derechos de autor y protección de cualquier trabajo cooperativo	
Información	Seguridad ligada al personal		Roles y responsabilidades Investigación de antecedentes Términos y condiciones del empleo	Comprobar la protección de los activos contra el acceso, divulgación, modificación, destrucción o interferencia no autorizada Verificar la disponibilidad de referencias de carácter satisfactorias; por ejemplo, una comercial y una personal Verificar el curriculum vitae del postulante buscando integridad y exactitud Confirmar las calificaciones académicas y profesionales mencionadas	Revisar que implementación y actuación están en concordancia con las políticas de seguridad de la información de la organización Revisar que se asigne a la persona la responsabilidad por las acciones tomadas Inspeccionar los reportes de eventos de seguridad o eventos potenciales u otros riesgos de seguridad para la organización. Verificar que todos los usuarios empleados, contratistas y terceros que tienen acceso a información sensible deben de firmar un acuerdo

			Responsabilidades de la gerencia Conocimiento, educación y capacitación en seguridad de la información Responsabilidades de la terminación Devolución de los activos Retiro de los derechos de acceso	Verificar la identidad independiente (pasaporte o documento similar) del postulante a un empleo Verificar créditos o récords criminales de los postulantes a un empleo. Verificar las responsabilidades y derechos de los empleados, contratistas y cualquier otro usuario Verificar las responsabilidades para la clasificación de la información y la gestión de los activos organizacionales asociadas con los sistemas y servicios de información manejados por el empleado, contratista o tercera persona Verificar las responsabilidades del usuario empleado, contratista o tercera persona con relación al manejo de la información recibida de otras compañías o partes externas Verificar las responsabilidades de la organización por el manejo de la información personal, incluyendo la información personal creada como resultado de, o en el curso de, el empleo con la organización Verificar las responsabilidades que se extienden fuera del local de la organización y fuera del horario normal de trabajo; por ejemplo, en el caso del trabajo en casa Verificar las acciones a tomarse si el usuario empleado, contratista o tercera persona no cumple los requerimientos de seguridad de la organización Verificar que usuarios empleados, contratistas y terceras personas estén motivados para cumplir con las políticas de seguridad de la organización Lograr un nivel de conciencia sobre seguridad relevante para sus roles y responsabilidades dentro de la organización	de confidencialidad o no divulgación antes de otorgarles acceso a los medios de procesamiento de la información Investigar que usuarios empleados, contratistas y terceras personas estén apropiadamente informados sobre sus roles y responsabilidades de seguridad antes de otorgarles acceso a información confidencial o a los sistemas de información Comprobar que usuarios empleados, contratistas y terceras personas reciban lineamientos para establecer las expectativas de seguridad de su rol dentro de la organización Verificar que usuarios empleados, contratistas y terceras personas cumplan con los términos y condiciones de empleo, los cuales incluyen la política de seguridad de la información de la organización y los métodos de trabajo apropiados Verificar que usuarios empleados, contratistas y terceras personas continúen teniendo las capacidades y calificaciones apropiadas

Información	Clasificación y control de activos		Inventario de los activos Propiedad de los activos Uso aceptable de los activos Lineamientos de clasificación de la información Etiquetado y manejo de la información	Asegurar que la información y los activos asociados con los medios de procesamiento de la información sean clasificados apropiadamente Definir y revisar periódicamente las restricciones y clasificaciones de acceso, tomando en cuenta las políticas de control de acceso aplicables Verificar la existencia de reglas para la utilización del correo electrónico e Internet Verificar los lineamientos para el uso de dispositivos móviles, especialmente para el uso fuera del local de la organización	Revisar la información: bases de datos y archivos de data, contratos y acuerdos, documentación del sistema, información de investigaciones, manuales del usuario, material de capacitación, procedimientos operacionales o de soporte, planes de continuidad del negocio, acuerdos para contingencias, rastros de auditoría e información archivada. Revisar activos de software: software de aplicación, software del sistema, herramientas de desarrollo y utilidades Revisar activos físicos: equipo de cómputo, equipo de comunicación, medios removibles y otro equipo Revisar servicios: servicios de computación y comunicación, servicios generales; por ejemplo, calefacción, iluminación, energía y aire acondicionado;
Información	Seguridad física y del entorno		Controles de ingreso físico Asegurar la oficinas, habitaciones y medios Protección contra amenazas externas e internas Trabajo en áreas	Elaborar, si se ve necesario, barreras físicas para prevenir el acceso físico no autorizado y la contaminación ambiental Seleccionar adecuados sistemas de detección de intrusos según estándares nacionales, regionales e internacionales y debieran ser probados regularmente para abarcar todas las puertas externas y ventanas accesibles; las áreas no ocupadas debieran contar con alarma en todo momento; también se debiera proveer protección para otras áreas; por ejemplo, el cuarto de cómputo cuarto de comunicaciones Verificar que los medios de procesamiento de información manejados por la organización Deben de estar físicamente separados de aquellas	Verificar que los perímetros de seguridad deben de estar claramente definidos, y la ubicación y fuerza de cada uno de los perímetros dependerá de los requerimientos de seguridad de los activos dentro del perímetro y los resultados de la evaluación del riesgo Verificar que los perímetros de un edificio o local que contienen los medios de procesamiento de información debieran ser físicamente sólidos ,es decir, no debieran existir brechas en el perímetro o áreas donde fácilmente pueda ocurrir un ingreso no autorizado Verificar que las paredes externas del local debieran ser una construcción sólida y todas las puertas externas debieran estar adecuadamente protegidas contra accesos no autorizados

			aseguradas	manejadas por terceros	mediante mecanismos de control; por ejemplo, vallas, alarmas, relojes, etc.; las puertas y ventanas debieran quedar aseguradas cuando están desatendidas y se debiera considerar una protección externa para las ventas, particularmente en el primer piso
			Áreas de acceso público, entrega y cargas Ubicación y protección del equipo Servicios públicos de soporte Seguridad del cableado Mantenimiento del equipo Seguridad del equipo fuera del local Seguridad de la eliminación o re-uso del equipo Retiro de propiedad	Verificar que los derechos de acceso a áreas seguras debieran ser revisados y actualizados regularmente, y revocados cuando sea necesario Verificar si se tomaron en cuenta los estándares y regulaciones de sanidad y seguridad relevantes; Verificar que los materiales peligrosos o combustibles deben ser almacenados a una distancia segura del área asegurada. Los suministros a granel como papelería no debiera almacenarse en el área asegurada Verificar que el equipo de reemplazo y los medios de respaldo deben ubicarse a una distancia segura para evitar el daño de un desastre que afecte el local principal Verificar el registro del material que ingresa en concordancia con los procedimientos de gestión de activos a su ingreso al local Verificar cuando fuese posible, que los embarques que ingresan y salen estén segregados. Verificar que el equipo esté ubicado de manera que se minimice el acceso innecesario a las áreas de trabajo Verificar la existencia de controles para minimizar el riesgo de amenazas potenciales; por ejemplo, robo, fuego, explosivos, humo, agua (o falla en el suministro de agua), polvo, vibración, efectos químicos, interferencias en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo	Verificar que se cuenta con un área de recepción con un(a) recepcionista u otros medios para controlar el acceso físico al local o edificio; el acceso a los locales y edificios debieran restringirse solamente al personal autorizado Verificar que todas las puertas de emergencia en un perímetro de seguridad deben contar con alarma, ser monitoreadas y probadas en conjunción con las paredes para establecer el nivel de resistencia requerido en concordancia con los adecuados estándares regionales, nacionales e internacionales y también operar en concordancia con el código contra-incendios local de una manera totalmente segura. Revisar el rastro de auditoría de todos los accesos Verificar que el acceso a áreas donde se procesa o almacena información sensible se controle y restrinja sólo a personas autorizadas; se debe utilizar controles de autenticación; por ejemplo, tarjeta de control de acceso más PIN; para autorizar y validar todo los accesos; se debiera mantener un rastro de auditoría de todos los accesos Verificar que todos los usuarios empleados, contratistas y terceras personas y todos los visitantes usen alguna forma de identificación visible y se debiera notificar inmediatamente al personal de seguridad si se encuentra a un visitante no acompañado y cualquiera que no use una identificación visibles

				Verificar la existencia de lineamientos sobre comer, beber y fumar en la proximidad de los medios de procesamiento de información Verificar que se monitoree las condiciones ambientales; tales como temperatura y humedad, que pudiera afectar adversamente la operación de los medios de procesamiento de la información Verificar la protección contra rayos en todos los edificios y la existencia de filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones Verificar el uso de métodos de protección, como membranas de teclado, para el equipo en el ambiente industrial Verificar la utilización de una lista de empalmes documentados para reducir la posibilidad de error Corroborar que para sistemas sensibles o críticos se debieran considerar más controles como: 1) la instalación de un tubo blindado y espacios o cajas con llave en los puntos de inspección y terminación; 2) el uso de rutas alternativas y/o medios de transmisión proporcionan una seguridad adecuada; 3) el uso de cableado de fibra óptica; 4) el uso de un escudo electromagnético para proteger los cables; 5) la iniciación de barridos técnicos e inspecciones físicas de dispositivos no autorizados que se adhieran a los claves; 6) acceso controlado para empalmar los paneles y los cuartos de cableado. Verificar que el equipo se mantenga en concordancia con los intervalos y especificaciones de servicio recomendados por el proveedor	Verificar que al personal de servicio de apoyo de terceros se le deba otorgar acceso restringido a las áreas seguras o los medios de procesamiento de información confidencial, solo cuando sea necesario; este acceso debiera ser autorizado y monitoreado Verificar el registro de la fecha y la hora de entrada y salida de los visitantes, y todos los visitantes deben ser supervisados a no ser que su acceso haya sido previamente aprobado; sólo se les debiera permitir acceso por propósitos específicos y autorizados y se debieran emitir las instrucciones sobre los requerimientos de seguridad del área y sobre los procedimientos de emergencia Verificar que los directorios y teléfonos internos que identifiquen la ubicación de los medios de procesamiento de la información no deben estar accesibles al público. Verificar la existencia de contra-incendios ubicado adecuadamente Verificar que el personal esté al tanto de la existencia o las actividades dentro del área asegurada sólo conforme las necesite conocer Verificar si se evita el trabajo no-supervisado en el área asegurada tanto por razones de seguridad como para evitar las oportunidades para actividades maliciosos Verificar que las áreas aseguradas vacías estén cerradas físicamente bajo llave y revisadas periódicamente Verificar que no se permita equipo fotográfico, de vídeo, audio y otro equipo de grabación; como cámaras en equipos móviles; a no ser que sea

				Comprobar que sólo el personal de mantenimiento autorizado lleve a cabo las reparaciones y dar servicio al equipo Verificar la existencia de registros de todas las fallas sospechadas y reales, y todo mantenimiento preventivo y correctivo Verificar la implementación de los controles apropiados cuando se programa el equipo para mantenimiento, tomando en cuenta si su mantenimiento es realizado por el personal en el local o fuera de la organización; cuando sea necesario, se debe de revisar la información confidencial del equipo, o se debe verificar al personal de mantenimiento Verificar el cumplimiento con todos los requerimientos impuestos por las pólizas de seguros Verificar que el equipo y medios sacados del local nunca estén dejados desatendidos en lugares públicos; durante un viaje, las computadoras portátiles debieran ser llevadas como equipaje de mano y cuando sea posible, de manera disimulada Verificar si se tomaron en cuenta las instrucciones de los fabricantes para proteger el equipo; por ejemplo, protección contra la exposición a fuertes campos electromagnéticos Verificar la existencia de los controles para el trabajo en casa a través de una evaluación del riesgo y los controles apropiados conforme sea apropiado; por ejemplo, archivos con llave, política de escritorio vacío Verificar si se cuenta con un seguro adecuado para proteger el equipo fuera del local. Verificar que los usuarios empleados, contratistas y terceras personas que tienen la autoridad para permitir el retiro de los activos fuera del local estén claramente identificados	autorizado. Verificar que el acceso al área de entrega y carga desde fuera del edificio este restringir al personal identificado y autorizado Verificar que el diseño del área de entrega y carga permita descargar los suministros sin que el personal de entrega tenga acceso a otras partes del edificio Verificar que las puertas externas del área de entrega y carga estén aseguradas cuando se abren las puertas internas Verificar que se inspeccione el material que ingresa para evitar amenazas potenciales antes que el material sea trasladado del área de entrega y carga al punto de uso Verificar que los medios de procesamiento de la información que manejan data confidencia estén ubicados de manera que se restrinja el ángulo de visión para reducir el riesgo que la información sea vista por personas no autorizadas durante su uso; y que medios de almacenaje estén asegurados para evitar el acceso no autorizado Verificar que los ítems que requieren protección especial estén aislados para reducir el nivel general de la protección requerida Verificar la protección del equipo que procesa la información confidencial para minimizar el riesgo de escape de información debido a emanación. Verificar que, de ser posible, las líneas de energía y telecomunicaciones que van a los medios de procesamiento de información sean subterráneas o estén sujetas a una alternativa de protección adecuada Verificar que el cableado de la red este protegido

				Verificar la existencia de límites de tiempo para el retiro del equipo y se debieran realizar un chequeo de la devolución; Verificar que cuando sea necesario y apropiado, el equipo sea registrado como retirado del local y se debiera registrar su retorno	contra intercepciones no autorizadas o daños, por ejemplo, utilizando un tubo o evitando las rutas a través de áreas públicas Verificar que los cables de energía estén separados de los cables de comunicaciones para evitar la interferencia Verificar la utilización de marcadores de cables y equipos claramente identificables para minimizar errores en el manipuleo, como un empalme accidental de los cables de red equivocados
Comunicación	Gestión de comunicaciones y operaciones		Procedimientos y responsabilidades operacionales Procedimientos de operación documentados Gestión del cambio Segregación de los deberes Separación de los medios de desarrollo, prueba y operación Entrega del servicio	Verificar que los procedimientos de operación especifiquen las instrucciones para la ejecución detallada de cada trabajo incluyendo: a) procesamiento y manejo de información; b) copia de seguridad o respaldo c) requerimientos de programación de horarios, incluyendo las interdependencias con otros sistemas, los tiempos de culminación y horarios de los primeros y últimos trabajos d) instrucciones para el manejo de errores u otras condiciones excepcionales, las cuales podrían surgir durante la ejecución del trabajo, incluyendo las restricciones sobre el uso de las utilidades del sistema e) contactos de soporte en el evento de dificultades operacionales o técnicas inesperadas f) instrucciones para el manejo de output especial y medios, tales como el uso de papelería especial o el manejo de output confidencial incluyendo los procedimientos para la eliminación segura del output de trabajo fallidos g) procedimientos de reinicio y recuperación del sistema para su uso en el evento de una falla en el sistema h) la gestión de la información del rastro de auditoría y registro del sistema Verificar la planeación y prueba de cambios, además de la evaluación de los impactos potenciales de los cambios, incluyendo los impactos de seguridad,	Monitorear los niveles de desempeño del servicio de comunicación para chequear adherencia con los acuerdos Revisar los reportes de servicio producidos por terceros y acordar reuniones de avance regulares conforme lo requieran los acuerdos Solicitar información sobre incidentes de seguridad de la información y la revisión de esta información por terceros y la organización conforme lo requieran los acuerdos y cualquier lineamiento y procedimiento de soporte Revisar los rastros de auditoría de terceros y los registros de eventos de seguridad, problemas operacionales, fallas, el monitoreo de fallas e interrupciones relacionadas con el servicio entregado Revisar los cambios realizados por la organización para implementar: 1) aumentos los servicios ofrecidos actualmente; 2) desarrollo de cualquier aplicación y sistema nuevo; 3) modificaciones o actualizaciones de las políticas y procedimientos de la organización; 4) controles nuevos para solucionar incidentes de la seguridad de la información y para mejorar la seguridad;

			Monitoreo y revisión de los servicios de terceros	Verificar la existencia de procedimientos de aprobación formal para los cambios propuestos Corroborar la efectiva comunicación de los detalles del cambio para todos las personas relevantes	Revisar cambios en los servicios de terceros para implementar Revisar cambios y mejoras en las redes;; Revisar el desarrollo de herramientas y ambientes nuevos Revisar los cambios en la ubicación física de los medios del servicio y el cambio de proveedores. Verificar que la instalación del sistema nuevo no afectará adversamente los sistemas existentes, particularmente en las horas picos del procesamiento, como fin de mes
			Manejo de cambios en los servicios de terceros	Comprobar los procedimientos de emergencia y respaldo, incluyendo los procedimientos y responsabilidades para abortar y recuperarse de cambios fallidos y eventos inesperados.	
			Gestión de la capacidad	Comprobar la definición y documentación de las reglas para la transferencia de software del estado de desarrollo al operacional	
			Aceptación del sistema	Examinar que los software de desarrollo y operacional corran en sistemas o procesadores de cómputo, y en diferentes dominios o directorios	
			Controles contra códigos maliciosos	Confirmar que los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no sean accesibles desde los sistemas operacionales cuando no se requieran	
			Controles contra códigos móviles	Verificar que el ambiente del sistema de prueba debiera emular el ambiente del sistema operacional lo más estrechamente posible	
			Respaldo o Back-Up	Demostrar que los usuarios debieran utilizar perfiles de usuario diferentes para los sistemas operacionales y de prueba, y los menús debieran mostrar los mensajes de identificación apropiados para reducir el riesgo de error Evidenciar que la data confidencial no este copiada en el ambiente del sistema de prueba	
			Controles de redes	Verificar el desempeño y los requerimientos de capacidad de la computadora	
			Seguridad de los servicios de la red	Demostrar procedimientos para la recuperación tras errores y reinicio, y planes de contingencia Revisar la preparación y prueba de los procedimientos	

				de operación rutinarios para estándares definidos	
			Gestión de medios removibles	Examinar el conjunto de controles de seguridad acordados y aceptados Examinar la existencia de capacitación para la operación o uso de los sistemas nuevos	
			Procedimientos para el manejo de información	Confirmar la existencia de una política formal que prohíbe el uso de software no-autorizado	Verificar la identificación y registro de cambios significativos
			Seguridad de la documentación del sistema	Revisar la existencia de una política formal para proteger contra riesgos asociados con la obtención de archivos, ya sea a través de redes externas o cualquier otro medio, indicando las medidas de protección a tomarse	Revisar la facilidad de uso del sistema, ya que esto afecta el desempeño del usuario y evita el error humano.
			Políticas y procedimientos de intercambio de información	Verificar que la instalación y actualización regular de software para la detección o reparación de códigos maliciosos para de las computadoras incluyan: 1) chequeo de cualquier archivo en medios electrónico u ópticos, y los archivos recibidos a través de la red para detectar códigos maliciosos antes de utilizarlo	Revisar regularmente el software y contenido de data de los sistemas que sostienen los procesos comerciales críticos; se debe investigar formalmente la presencia de cualquier activo no-aprobado o enmiendas no-autorizadas;
			Acuerdos de intercambio	2) chequeo de los adjuntos y descargas de los correos electrónicos para detectar códigos maliciosos antes de utilizarlos, este chequeo se debe de llevar a cabo en lugares diferentes; por ejemplo, servidores de correo electrónico,	Revisar la extensión (por ejemplo, respaldo completo o diferencial) y la frecuencia de los respaldos los cuales deben de reflejar los requerimientos comerciales de la organización, los requerimientos de seguridad de la información involucrada, y el grado crítico de la información para la operación continua de la organización
			Medios físicos en tránsito	computadoras desktop y cuando se ingresa a la red de la organización; 3) chequeo de las páginas Web para detectar códigos maliciosos	Probar regularmente para asegurar que se puedan confiar en ellos para usarlos cuando sea necesaria en caso de emergencia
			Mensajes electrónicos	Probar la definición, gestión, procedimientos y responsabilidades para lidiar con la protección de códigos maliciosos en los sistemas, capacitación en su uso, reporte y recuperación de ataques de códigos maliciosos	Chequear y probar regularmente los procedimientos de restauración para asegurar que sean efectivos y que pueden ser completados dentro del tiempo asignado en los procedimientos operacionales para la recuperación;
			Sistemas de información comercia l	Confirmar la existencia de planes apropiados para la	Revisar los registros de ingreso y monitoreo apropiados para permitir el registro de las

			Comercio electrónico	continuidad del negocio para recuperarse de ataques de códigos maliciosos, incluyendo toda la data y respaldo (back-up) de software y procesos de recuperación	acciones de seguridad relevantes;
			Transacciones en-línea	Demostrar la implementación de procedimiento para la recolección regular de información, como suscribirse a listas de correos y/o chequear Web sites que dan información sobre códigos maliciosos nuevos	Revisar las características de seguridad de los servicios de red los cuales pueden ser: a) la tecnología aplicada para la seguridad de los servicios de red; como controles de autenticación, codificación y conexión de red; b) parámetros técnicos requeridos para una conexión segura con los servicios de red en concordancia con las reglas de seguridad y conexión de red c) cuando sea necesario, procedimientos para la utilización del servicio de red para restringir el acceso a los servicios de red o aplicaciones.
			Información públicamente disponible	Verificar la implementación de procedimientos para verificar la información relacionada con el código malicioso y para asegurar que los boletines de advertencia sean exactos e informativos, los gerentes debieran asegurar que se utilicen fuentes calificadas	Revisar muchas organizaciones ofrecen servicios de recolección y eliminación de papeles, equipo y medios; se debiera tener cuidado al seleccionar el contratista adecuado con los controles y la experiencia adecuados.
			Registro de auditoría	Demostrar que se cuenta con las siguientes consideraciones para evitar que el código móvil realice acciones no-autorizadas: a) ejecutar el código móvil en un ambiente aislado lógicamente; b) bloquear cualquier uso del código móvil;	Revisar el manipuleo y etiquetado de todos los medios en su nivel de clasificación indicado
			Uso del sistema de monitoreo	c) bloquear lo recibido del código móvil: d) activar las medidas técnicas conforme estén disponibles en un sistema específico para asegurar el manejo del código móvil;	Inspeccionar las restricciones de acceso para evitar el acceso de personal no-autorizado
			Protección del registro de información	e) control de los recursos disponibles para el acceso del código móvil; f) controles criptográficos para autenticar singularmente el código móvil.	Controlar que el input de data esté completo, que el proceso se complete apropiadamente y que se aplique la validación del output
			Registros del administrador y operador	Verificar la definición del nivel necesario de respaldo de la información y la producción de registros exactos y completos de las copias de respaldo y procedimientos documentados de la restauración	Revisar la seguridad para el comercio electrónico Revisar el sistemas de publicación electrónica, especialmente aquellos que permiten retroalimentación y el ingreso directo de información
			Registro de fallas	Probar que las copias de respaldo se debieran almacenar en un lugar apartado, a la distancia suficiente como para escapar de cualquier daño por un desastre en el local principal	Revisar los registros de auditoría
			Sincronización de	Confirmar que la información de respaldo tenga el nivel de protección física y ambiental apropiado consistente	

			relojes	con los estándares aplicados en el local principal; los controles aplicados a los medios en el local principal se debiera extender para cubrir la ubicación de la copia de respaldo Demostrar que en situaciones cuando la confidencialidad es de importancia, las copias de respaldo deben ser protegidas por medios de una codificación Verificar que. cuando sea apropiado, la responsabilidad operacional para las redes se debe de separar de las operaciones de cómputo Comprobar que se establecen las responsabilidades y procedimientos para la gestión del equipo remoto, incluyendo el equipo en las áreas del usuario Comprobar la existencia de controles especiales para salvaguardar la confidencialidad y la integridad de la data que pasa a través de las redes públicas o a través de las redes inalámbricas y la disponibilidad de los servicios de la red Probar que las actividades de gestión deben estar estrechamente coordinadas para optimizar el servicio a la organización y para asegurar que los controles sean aplicados consistentemente a través de la infraestructura de procesamiento de la información. Verificar la existencia de los procedimientos para identificar los medios removibles que podrían requerir de una eliminación segura Comprobar que, cuando sea posible se debe de registrar la eliminación de los medios removibles confidenciales para mantener un rastro de auditoría. Verificar que la documentación del sistema este almacenada de una manera segura Comprobar que la lista de acceso para la documentación del sistema se mantenga en un nivel	

				mínimo y autorizado por el propietario de la aplicación	
				Confirmar que la documentación del sistema mantenido en una red pública, o suministrada a través de una red pública, este adecuadamente protegida. Constatar que los procedimientos y controles a seguirse cuando se utilizan medios de comunicación electrónicos para el intercambio de información consideren lo siguiente: a) los procedimientos diseñados para proteger el intercambio de información de la intercepción, copiado, modificación, routing equivocado y destrucción; b) los procedimientos para la detección y protección contra códigos maliciosos que pueden ser transmitidos a través del uso de comunicaciones electrónicas c) los procedimientos para proteger la información electrónica confidencial comunicada que está en la forma de un adjunto; d) política o lineamientos delineando el uso aceptable de los medios de comunicación electrónicos e) los procedimientos para el uso de comunicación inalámbrica, tomando en cuenta los riesgos particulares involucrados; f) las responsabilidades del usuario empleado, contratista y cualquier otro para que no comprometan a la organización; por ejemplo, a través de la difamación, hostigamiento, suplantación, reenvío de cadenas de cartas, compras no autorizadas, etc. g) uso de técnicas de codificación; por ejemplo, para proteger la confidencialidad, integridad y autenticidad de la información h) lineamientos de retención y eliminación de toda la correspondencia del negocio, incluyendo mensajes, en concordancia con la legislación y regulaciones nacionales y locales relevantes; i) no dejar la información confidencial o crítica en	

				medios impresos; por ejemplo, copiadoras, impresoras y máquinas de fax; ya que personal no-autorizado puede tener acceso a ellas; j) los controles y restricciones asociados con el reenvío de los medios de comunicación; por ejemplo, reenvío automático de correo electrónico a direcciones externas; k) recordar al personal que debiera tomar las precauciones apropiadas; por ejemplo, no revelar información confidencial cuando realiza una llamada telefónica para evitar ser escuchado o interceptado por: 1) personas alrededor suyo, particularmente cuando se utilizan teléfonos móviles; 2) intervención de teléfonos y otras formas de escucha no-autorizada a través del acceso físico al teléfono o la línea telefónica, o el uso de escáners receptores 3) personas en el otro lado de la línea, en el lado del receptor; l) no dejar mensajes conteniendo información confidencial en máquinas contestadoras dado que estos pueden ser escuchados por personas no autorizadas, ni almacenados en sistemas comunitarios o almacenados incorrectamente como resultado de un equívoco al marcar; m) recordar al personal el problema de utilizar máquinas de fax, principalmente por: 1) acceso no autorizado al almacén de mensaje incorporado para recuperar los mensajes; 2) programación deliberada o accidental de las máquinas para enviar mensajes a números específicos 3) enviar documentos al número equivocado, ya se por marcar un número equivocado o usando un número erróneamente almacenado; n) recordar al personal no registrar data demográfica, como la dirección de correo electrónico u otra información personal, en ningún software para evitar que sea utilizada sin autorización; o) recordar al personal que las máquinas de fax y	

				fotocopiadoras modernas tienen páginas cache y almacenan páginas en caso de una falla en la transmisión o papel, las cuales se imprimirán una vez que la falla se aclare. Demostrar que el acuerdo de intercambio de información considera las siguientes condiciones de seguridad: a) manejo de las responsabilidades para el control y notificación de la transmisión, despacho y recepción; b) procedimientos para notificar al remitente de la transmisión, despacho y recepción; c) procedimientos para asegurar el rastreo y no-repudio d) estándares técnicos mínimos para el empaque y la transmisión e) acuerdos de depósitos f) estándares de identificación del mensajero; g) responsabilidades y obligaciones en el evento de incidentes de seguridad de la información, como la pérdida de data; h) uso de un sistema de etiquetado acordado para la información confidencial o crítica, asegurando que el significado de las etiquetas sea entendido inmediatamente y que la información sea adecuadamente protegida; i) propiedad y responsabilidades de la protección de data, derechos de autor, licencias de software y consideraciones similares j) estándares técnicos para grabar y leer la información y software; k) cualquier control especial que se pueda requerir para proteger los ítems confidenciales, como claves criptográficas. Comprobar la consideración de los siguientes lineamientos para proteger los medios de información transportados entre diferentes ubicaciones: a) se debieran utilizar transportes o mensajerías confiables; b) se debiera acordar con la gerencia una lista de mensajerías autorizadas;	

				c) se debieran desarrollar procedimientos para chequear la identificación de las mensajeros; d) el empaque debiera ser suficiente para proteger los contenidos de cualquier daño que pudiera surgir durante el tránsito y en concordancia con las especificaciones de cualquier fabricante (por ejemplo, para software), por ejemplo protegiendo de cualquier factor ambiental que pudiera reducir la efectividad de la restauración de medios, tales como la exposición al calor, humedad o campos electromagnéticos; e) donde sea necesario, se debieran adoptar controles para proteger la información confidencial de la divulgación o modificación no-autorizada, los ejemplos incluyen: 1) uso de contenedores cerrados con llave; 2) entrega en la mano; 3) empaque que haga evidente si ha sido manipulado (el cual revela cualquier intento por obtener acceso); 4) en casos excepcionales, dividir el envío en más de una entrega y despacharlo por rutas diferentes. Verificar que las consideraciones de seguridad para los mensajes electrónicos incluyan lo siguiente: a) proteger los mensajes del acceso no-autorizado, modificación o negación del servicio; b) asegurar la correcta dirección y transporte del mensaje; c) confiabilidad y disponibilidad general del servicio; d) consideraciones legales, por ejemplo los requerimientos para firmas electrónicas; e) obtener la aprobación antes de utilizar los servicios públicos externos como un mensaje instantáneo o intercambio de archivos; f) niveles mayores de autenticación controlando el acceso de las redes de acceso público. Verificar que las consideraciones de seguridad para el comercio electrónico incluyan lo siguiente: a) el nivel de confianza que cada parte requiere de la identidad de la otra; por ejemplo, a través de la autenticación;	

				b) los procesos de autorización asociados con aquellos que pueden establecer precios, emitir o firmar documentos de comercialización; c) asegurar que los socios comerciales estén totalmente informados de sus autorizaciones; d) determinar y cumplir con los requerimientos para la confidencialidad, integridad, prueba de despacho y recepción de documentos claves, y el no-repudio de los contratos; por ejemplo, asociado con procesos de licitación y contratos; e) el nivel de confianza requerido para la integridad de las listas de precios publicitadas; f) la confidencialidad de cualquier data o información confidencial; g) la confidencialidad e integridad de cualquier transacción, información de pago, detalles de la dirección de entrega y la confirmación de la recepción; h) el grado de verificación apropiado para chequear la información de pago suministrada por un cliente; i) seleccionar la forma de liquidación más apropiada del pago para evitar el fraude; j) el nivel de protección requerido para mantener la confidencialidad e integridad de la información de la orden; k) evitar la pérdida o duplicación de la información de la transacción; l) la responsabilidad asociada con cualquier transacción fraudulenta; m) requerimientos de seguro. Revisar que las consideraciones de seguridad para las transacciones en-línea incluyan lo siguiente: a) el uso de firmas electrónicas por cada una de las partes involucradas en la transacción; b) todos los aspectos de la transacción; es decir, asegurando que: 1) las credenciales de usuario de todas las partes sean válidas y verificadas;	

				2) que la transacción permanezca confidencial, y 3) que se mantenga la privacidad asociada con todas las partes involucradas; c) el camino de las comunicaciones entre las partes involucradas debiera ser codificado; d) los protocolos utilizados para comunicarse entre todas las partes involucradas sean seguros; e) asegurar que el almacenaje de los detalle de la transacción se localice fuera de cualquier ambiente público accesible; por ejemplo, en una plataforma de almacenaje existente en el Intranet organizacional, y no se mantenga y exponga en un medio de almacenaje directamente accesible desde el Internet; f) cuando se utilice una autoridad confiables (por ejemplo, para propósitos de emitir y mantener firmas digitales y/o certificados digitales) la seguridad es integrada e introducida durante todo el proceso de gestión de firma/certificado de principio a fin. Verificar el control de los sistemas de publicación electrónica, especialmente aquellos que permiten retroalimentación y el ingreso directo de información de manera que: a) la información se obtenga cumpliendo con la legislación de protección de data b) el input de información para, y procesado por, el sistema de publicación será procesado completa y exactamente de una manera oportuna: c) se protegerá la información confidencial durante la recolección, procesamiento y almacenaje; d) el acceso al sistema de publicación no permite el acceso involuntario a las redes con las cuales se conecta el sistema. Constatar que los registros de auditoría del sistema incluyan, cuando sea relevante: a) utilizar IDs;	

				b) fechas, horas y detalles de eventos claves; por ejemplo, ingreso y salida; c) identidad o ubicación de la identidad, si es posible; d) registros de intentos de acceso fallidos y rechazados al sistema; e) registros de intentos de acceso fallidos y rechazados a la data y otros recursos; f) cambios en la configuración del sistema; g) uso de privilegios; h) uso de las utilidades y aplicaciones del sistema; i) archivos a los cuales se tuvo acceso y los tipos de acceso; j) direcciones y protocolos de la red; k) alarmas activadas por el sistema de control de acceso; l) activación y desactivación de los sistemas de protección; como sistemas anti-virus y sistemas de detección de intrusiones. Comprobar que los factores de riesgo a considerarse incluyen: a) grado crítico de los procesos de aplicación; b) valor, sensibilidad y grado crítico de la información involucrada; c) antecedentes de infiltración y mal uso del sistema, y la frecuencia con la que se explotan las vulnerabilidades; d) extensión de la interconexión del sistema (particularmente las redes públicas); e) desactivación del medio de registro. Verificar que los controles del sistema deben tener el objetivo de proteger contra cambios no autorizados y problemas operacionales, y el medio de registro deben incluir: a) las alteraciones registradas a los tipos de mensajes; b) los archivos de registro que se editan o borran; c) capacidad de almacenamiento del medio de archivos de registro que se está excediendo, resultando en una falla en el registro de eventos o la escritura encima de los eventos registrados en el pasado.	

				Probar que los log de seguridad incluyan: a) la hora en la cual ocurre un evento (éxito o falla); b) la información sobre el evento (por ejemplo, archivos manejados) o falla (por ejemplo, el error ocurrido y la acción correctiva); c) cuál cuenta y cuál operador o administrador está involucrado; d) cuáles procesos están involucrados. Confirmar la existencia de reglas claras para manejar las fallas reportadas incluyendo: a) revisión de los registros de fallas para asegurar que las fallas se hayan resuelto satisfactoriamente; b) revisión de las medidas correctivas para asegurar que los controles no se hayan visto comprometidos, y que la acción tomada haya sido completamente autorizada	
Información	Control de accesos		Política de control del acceso Registro del usuario Gestión de privilegios Gestión de las claves secretas de los usuarios Revisión de los derechos de acceso del usuario	Verificar que la política de control de accesos tome en cuenta lo siguiente: a) los requerimientos de seguridad de las aplicaciones comerciales individuales b) identificación de toda la información relacionada con las aplicaciones comerciales y los riesgos que enfrenta la información; c) las políticas para la divulgación y autorización de la información; por ejemplo, la necesidad de conocer el principio y los niveles de seguridad, y la clasificación de la información d) consistencia entre el control del acceso y las políticas de clasificación de la información de los diferentes sistemas y redes e) legislación relevante y cualquier obligación contractual relacionada con la protección del acceso a la data o los servicios f) los perfiles de acceso de usuario estándar para puestos de trabajo comunes en la organización; g) gestión de los derechos de acceso en un ambiente distribuido y en red que reconoce todos los tipos de conexiones disponibles; h) segregación de roles del control del acceso; por ejemplo, solicitud de acceso,	Examinar que los usuarios firmen un enunciado para mantener confidenciales las claves secretas y mantener las claves secretas grupales sólo dentro de los miembros el grupo; este enunciado firmado se puede incluir en los términos y condiciones de empleo Comprobar, cuando se requiere, que los usuarios mantengan sus propias claves secretas, inicialmente se les debe proporcionar una clave secreta temporal segura la cual están obligados a cambiar inmediatamente Corroborar que se establezca procedimientos para verificar la identidad de un usuario antes de proporcionar una clave secreta nuevo, sustituta o temporal Verificar que las claves secretas temporales debieran ser proporcionadas a los usuarios de una manera segura, se debe evitar el uso de mensajes de correo electrónico de terceros o no protegidos Comprobar que las claves secretas temporales

			Uso de claves secretas Equipo del usuario desatendido Política de escritorio y pantalla limpios Política sobre el uso de los servicios de la red Autenticación del usuario para las conexiones externas Identificación del equipo en las redes Protección del puerto de diagnóstico y configuración remoto Segregación en redes	autorización de acceso, administración del acceso; i) requerimientos para la autorización formal de las solicitudes de acceso; j) requerimientos para la revisión periódica de los controles de acceso k) revocación de los derechos de acceso Comprobar que el procedimiento de control del acceso para el registro y des-registro del usuario incluya: a) utilizar IDs de usuarios únicos para permitir a los usuarios vincularse y ser responsables de sus acciones; sólo se debiera permitir el uso de IDs grupales cuando son necesarios por razones comerciales u operacionales, y debieran ser aprobados y documentados; b) chequear que el usuario tenga la autorización dada por el propietario del sistema para el uso del sistema o servicio de información; también puede ser apropiado una aprobación separada de la gerencia para los	deben ser únicas para la persona y no deberán ser fáciles de adivinar; Examinar que los usuarios deban reconocer la recepción de las claves secretas y estas nunca deben ser almacenadas en los sistemas de cómputo de una forma desprotegida Corroborar que las claves secretas predeterminadas por el vendedor deben ser cambiadas después de la instalación de sistemas o software.

				derechos de acceso	
			Control de conexión a la red	c) chequear que el nivel de acceso otorgado sea apropiado para el propósito comercial y que sea consistente con la política de seguridad de la organización; por ejemplo, no compromete la segregación de los deberes	
			Control de routing de la red	d) proporcionar a los usuarios un enunciado escrito de sus derechos de acceso	
				e) requerir a los usuarios que firmen los enunciados indicando que entienden las condiciones de acceso	
			Procedimientos para un registro seguro	f) asegurar que los proveedores del servicio no proporcionen acceso hasta que se hayan completado los procedimientos de autorización	
				g) mantener un registro formal de todas las personas registradas para usar el servicio	
				h) eliminar o bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de puesto o trabajo o han dejado la organización	
			Identificación y autenticación del usuario	i) chequeo periódico para eliminar o bloquear los IDs de usuario y cuentas redundantes	
				j) asegurar que no se emitan IDs de usuario redundantes a otros usuarios.	
			Sistema de gestión de claves secretas	Confirmar que los sistemas multi-usuario que requieren protección contra el acceso no autorizado debieran controlar la asignación de privilegios a través de un proceso de autorización formal, por lo tanto deben de considerar los siguientes pasos:	
			Uso de las utilidades del sistema	a) los privilegios de acceso asociados con cada producto del sistema; por ejemplo, sistema de operación, sistema de gestión de base de datos y cada aplicación, y se debieran identificar los usuarios a quienes se les necesita asignar privilegios;	
			de una sesión por inactividad	b) los privilegios se debieran asignar a los usuarios sobre la base de “sólo lo que necesitan saber” y sobre una base de evento-por-evento en línea con la política de control del acceso; es decir, los requerimientos mínimos para su rol funcional, sólo cuando se necesitan	
			Limitación del tiempo de conexión	c) se debiera mantener un proceso de autorización y un registro de todos los privilegios asignados. No se debieran otorgar privilegios hasta que se complete el	

			Control de acceso a la aplicación y la información Restricción del acceso a la información Aislar el sistema confidencia l Computación y comunicaciones móviles Tele-trabajo	proceso de autorización. d) Se debiera promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios; e) se debiera promover el desarrollo y uso de los programas que evitan la necesidad de correr con privilegios; f) los privilegios se debieran asignar a un ID de usuario diferente de aquellos utilizados para el uso normal del negocio. Probar que los derechos de acceso consideran los siguientes lineamientos: a) los derechos de acceso de los usuarios debieran ser revisados a intervalos regulares; por ejemplo, un período de 6 meses, y después de cualquier cambio, como un ascenso, democión o terminación del empleo b) los derechos de acceso del usuario se debieran revisar y re-asignar cuando se traslada de un empleo a otro dentro de la misma organización c) las autorizaciones para derechos de acceso privilegiados especiales se debieran revisar a intervalos más frecuentes; por ejemplo, un período de 3 meses; d) se debiera chequear la asignación de privilegios a intervalos regulares para asegurar que no se hayan obtenido privilegios no autorizados e) se debieran registrar los cambios en las cuentas privilegiadas para una revisión periódica. Comprobar que todos los usuarios fueron advertidos sobre: a) mantener confidenciales las claves secretas; b) evitar mantener un registro (por ejemplo, papel, archivo en software o dispositivo manual) de las claves secretas, a no ser que este se pueda mantener almacenado de manera segura y el método de almacenaje haya sido aprobado c) cambio de claves secretas cuando haya el menor indicio de un posible peligro en el sistema o la clave secreta d) seleccionar claves secretas de calidad con el largo mínimo suficiente que sean:	

				1) fáciles de recordar; 2) no se basen en nada que otro pueda adivinar fácilmente u obtener utilizando la información relacionada con la persona; por ejemplo, nombres, números telefónicos y fechas de nacimiento, etc. 3) no sean vulnerables a los ataques de diccionarios (es decir, que no consista de palabras incluidas en los diccionarios); 4) libre de caracteres consecutivos idénticos, todos numéricos o todos alfabéticos; e) cambio de las claves secretas a intervalos regulares o en base al número de accesos (las claves secretas para las cuentas privilegiadas se debieran cambiar con mayor frecuencia que las claves secretas normales), y evitar el re-uso de reciclaje de clave secretas antiguas; f) cambiar la clave secreta temporal en el primer registro de ingreso; g) no incluir las claves secretas en ningún proceso de registro automatizado; por ejemplo, almacenado en un macro o función clave; h) no compartir las claves secretas individuales; i) no usar la misma clave personal para propósitos comerciales y no-comerciales Confirmar que se comunico a los usuarios que deben: a) cerrar las sesiones activas cuando se termina, a no ser que puedan asegurarse con un mecanismo de cierre apropiado; por ejemplo, protector de pantalla asegurado mediante clave secreta; b) salir de las computadoras mainframe, servidores y PCs de oficina cuando se termina la sesión (es decir, no sólo apagar la pantalla de la PC o Terminal); c) asegurar las PCs o terminales contra un uso no autorizado mediante un seguro con clave o un control equivalente; por ejemplo, acceso con clave secreta, cuando no está en uso Verificar que se consideran los siguientes lineamientos: a) la información comercial confidencial o crítica; por ejemplo, en papel o medios de almacenamiento electrónicos; debiera ser guardada bajo llave (idealmente en una caja fuerte o archivador u otra	

				forma de mueble seguro) cuando no está siendo utilizada, especialmente cuando la oficina está vacía; b) cuando se dejan desatendidas, las computadoras y terminales debieran dejarse apagadas o protegidas con mecanismos para asegurar la pantalla y el teclado, controlados mediante una clave secreta, dispositivo o un mecanismo de autenticación de usuario similar y se debieran proteger con llave, claves secretas u otros controles cuando no están en uso; c) se debieran proteger los puntos de ingreso y salida de correo y las máquinas de fax desatendidas; d) se debiera evitar el uso no autorizado de fotocopiadoras y otra tecnología de reproducción (por ejemplo, escáners, cámaras digitales); e) los documentos que contienen información confidencial o clasificada debieran Verificar que los sistemas tengan la capacidad para: a) autenticar a los usuarios autorizados, en concordancia con una política de control de acceso definida; b) registrar los intentos exitosos y fallidos de autenticación del sistema; c) registrar el uso de los privilegios especiales del sistema; d) emitir alarmas cuando se violan las políticas de seguridad del sistema; e) proporcionar los medios de autenticación apropiados; f) cuando sea apropiado, restringir el tiempo de conexión de los usuarios. Comprobar que el procedimiento de registro debe de: a) no mostrar identificadores del sistema o aplicación hasta que se haya completado satisfactoriamente el proceso de registro; b) mostrar la advertencia general que a la computadora sólo pueden tener acceso los usuarios autorizados; c) no proporcionar mensajes de ayuda durante el procedimiento de registro que ayuden al usuario no-autorizado; d) sólo validar la información del registro después de	

				completar todo el input de data. Si surge una condición de error, el sistema deberá indicar qué parte de la data es correcta o incorrecta; e) limitar el número de intentos de registro infructuosos permitidos; por ejemplo, tres intentos; y deberá considerar: 1) registrar los intentos exitosos y fallidos; 2) forzar un tiempo de espera antes de permitir más intentos de registro o rechazar cualquier otro intento sin una autorización específica; 3) desconectar las conexiones de vínculo a la data; 4) establecer el número de re-intentos de clave secreta en conjunción con el largo mínimo de la clave secreta y el valor del sistema que se está protegiendo; f) limitar el tiempo máximo y mínimo permitido para el procedimiento de registro. Si se excede este tiempo, el sistema deberá terminar el registro g)mostrar la siguiente información a la culminación de un registro satisfactorio: 1) fecha y hora del registro satisfactorio previo; 2) detalles de cualquier intento infructuoso desde el último registro satisfactorio; h) no mostrar la clave secreta que se está ingresando o considerar esconder los caracteres de la clave secreta mediante símbolos i) no transmitir claves secretas en un texto abierto a través de la red. Verificar la existencia de un sistema de gestión de claves secretas que debe de: a) aplicar el uso de IDs de usuarios individuales y claves secretas para mantener la responsabilidad; b) permitir a los usuarios seleccionar y cambiar sus propias claves secretas e incluir un procedimiento de confirmación para permitir errores de input; c) aplicar la elección de claves secretas adecuadas y los cambios de estas d) obligar a los usuarios a cambiar las claves secretas temporales en su primer ingreso o registro e) mantener un registro de claves de usuario previas y evitar el re-uso; f)no mostrar las claves secretas en la pantalla en el momento de ingresarlas;	

				g) almacenar los archivos de claves secretas separadamente de la data del sistema de aplicación h) almacenar y transmitir las claves secretas en un formato protegido (por ejemplo, codificado o indexado). Comprobar si se considera los siguientes lineamientos para el uso de las utilidades del sistema: a) uso de los procedimientos de identificación, autenticación y autorización para las utilidades del sistema b) segregación de las utilidades del sistema del software de la aplicación; c) limitar el uso de las utilidades del sistema a un número práctico mínimo de usuarios autorizados y confiables d) autorización para el uso ad hoc de las utilidades del sistema; e) limitación de la disponibilidad de las utilidades del sistema; por ejemplo, por la duración de un cambio autorizado; f) registro de todo uso de las utilidades del sistema; g) definir y documentar los niveles de autorización de las utilidades del sistema; h) eliminación o inutilizar todas las utilidades innecesarias basadas en software, así como los software del sistema que sean innecesarios; i) no poner las utilidades a disposición de los usuarios que tienen acceso a las aplicaciones en los sistemas donde se requiere la segregación de los deberes Corroborar la existencia de restricciones como: a) utilizar espacios de tiempo predeterminados; por ejemplo, para transmisiones de archivos en lotes, o sesiones interactivas regulares de corta duración; b) restringir los tiempos de conexión a los horarios laborales normales, si no existe ningún requerimiento para sobre-tiempo o una operación de horario extendido; c) considerar la re-autenticación cada cierto intervalo de tiempo.	

				Constatar que los sistemas de aplicación deben: a) controlar el acceso del usuario a la información y las funciones del sistema de aplicación, en concordancia con una política de control de acceso definida; b) proporcionar protección contra un acceso no autorizado de cualquier utilidad, software del sistema de operación y software malicioso que sea capaz de superar o pasar los controles del sistema o la aplicación; c) no comprometer a otros sistemas con los cuales se comparten recursos de información. Verificar la consideración de aplicar los siguientes lineamientos para reforzar los requerimientos de restricción del acceso al sistema: a) proporcionar menús para controlar el acceso a las funciones del sistema de aplicación; b) controlar los derechos de acceso de los usuarios; por ejemplo, lectura, escritura, eliminar y ejecutar; c) controlar los derechos de acceso de otras aplicaciones; d) asegurar que los outputs de los sistemas de aplicación que manejan información confidencial sólo contengan la información relevante para el uso del output y sólo sea enviada a las terminales y ubicaciones autorizadas; esto debiera incluir revisiones periódicas de dichos outputs para asegurar que se descarte la información redundante. Examinar la consideración de los siguientes lineamientos para aislar el sistema sensible o confidencial: a) el propietario de la aplicación debiera identificar y documentar explícitamente la sensibilidad o confidencialidad del sistema de aplicación; b) cuando una aplicación confidencial va a correr en un ambiente compartido, el propietario de la aplicación confidencial debiera identificar y aceptar los sistemas de aplicación con los cuales va a compartir recursos y los riesgos correspondientes.	

Información	Desarrollo y mantenimiento de sistemas		Análisis y especificación de los requerimientos de seguridad Validación de la input data Control del procesamiento interno Integridad del mensaje Validación de la output data Política sobre el uso de controles criptográficos Gestión de claves Control del software operacional Protección de la	Verificar que se realicen chequeos del input de las transacciones comerciales, la data fija (por ejemplo nombres y direcciones, límites de crédito, números de referencia de los clientes), y tablas de parámetros (por ejemplo; precios de venta, moneda, tasas de cambio, tasa tributaria). Se deberán considerar los siguientes lineamientos a) input dual u otros chequeos de data; tales como chequeo de límites o limitar los campos a los rangos específicos de la input data; para detectar los siguientes errores: 1) valores fuera de rango; 2) caracteres inválidos en los campos de data; 3) data incompleta o faltante; 4) exceder los límites superiores e inferiores del volumen de data; 5) data de control no autorizada o inconsistente; b) revisión periódica del contenido de los campos claves o archivos de data para confirmar su validez e integridad; c) inspeccionar los documentos de input de la copia impresa en caso de cambios no autorizados (todos los cambios a los documentos de input debieran ser autorizados); d) procedimientos para responder a los errores de validación; e) procedimientos para probar la plausibilidad de la input data; f) definir las responsabilidades de todo el personal involucrado en el proceso de input de data; g) crear un registro de las actividades involucradas en el proceso de input de data Verificar que la validación del output incluya: a) chequeos de plausibilidad para comprobar si el output data es razonable; b) conteo de control de conciliación para asegurar el procesamiento de toda la data; c) proporcionar la información suficiente para un lector o el sistema de procesamiento subsiguiente para determinar la exactitud, integridad,	Revisar periódicamente lo siguiente: a) controles de sesión o lote, para conciliar los saldos del archivo de data después de las actualizaciones de la transacción; b) controles de saldos, para chequear los saldos de apertura comparándolos con los saldos de cierre anteriores; específicamente: 1) controles corrida-a-corrida; 2) totales de actualización del archivo; 3) controles programa-a-programa; c) validación de la input data generada por el sistema d) chequeos de la integridad, autenticidad y cualquier otro dispositivo de seguridad de la data o software cargado o descargado, entre la computadora central y las remotas; e) totales hash de registros y archivos; f) chequeos para asegurar que los programas se corran en el momento adecuado; g) chequeos para asegurar que los programas sean corridos en el orden correcto y terminados en caso de una falla, y que se detenga el procesamiento hasta que se resuelva el problema; h) crear un registro de las actividades involucradas en el procesamiento Revisar el output del sistema Revisar el sistema de gestión de claves Revisar, que cuando sea posible, no se mantenga las bibliotecas de fuentes del programa en los sistemas operacionales Revisar que el código fuente del programa y las bibliotecas de fuentes del programa debieran ser manejadas de acuerdo con los procedimientos establecidos Revisar los procedimientos de control e integridad de la aplicación para asegurar que no se hayan visto comprometidos por los cambios en el

			data del sistema	precisión y clasificación de la información; d) procedimientos para responder a las pruebas de validación de output;	sistema de operación
			Control de acceso al código fuente del programa	e) definir las responsabilidades de todo el personal involucrado en el proceso de output de data; f) crear un registro de las actividades en el proceso de validación del output de data	Asegurar que el plan y el presupuesto de soporte anual abarque las revisiones y pruebas del sistema resultantes de los cambios en el sistema de operación
			Procedimientos del control del cambio	Verificar que cuando se desarrolla una política criptográfica se considere lo siguiente: a) el enfoque gerencial sobre el uso de los controles criptográficos a través de la organización, incluyendo los principios generales bajo los cuales se debiera proteger la información comercial	Asegurar que la notificación de los cambios en el sistema de operación sea provista con tiempo para permitir realizar las pruebas y revisiones apropiadas antes de la implementación
			Revisión técnica de la aplicación después de cambios en el sistema	b) en base a la evaluación del riesgo, se debe identificar el nivel de protección requerido tomando en cuenta el tipo, fuerza y calidad del algoritmo criptográfico requerido; c) el uso de codificación para la protección de la información confidencial transportada por los medios y dispositivos móviles o removibles o a través de las líneas de comunicación	Asegurar que se realicen los cambios apropiados en los planes de continuidad del negocio
			Restricciones sobre los cambios en los paquetes de software	d) el enfoque de la gestión de claves, incluyendo los métodos para lidiar con la protección de las claves criptográficas y la recuperación de la información codificada en el caso de claves pérdidas, comprometidas o dañadas; e) roles y responsabilidades; por ejemplo, quién es responsable de:	Revisar, dependiendo de la urgencia con que se necesita tratar la vulnerabilidad técnica, que la acción a tomarse debe realizarse de acuerdo a los controles relacionados con la gestión de cambios o siguiendo los procedimientos de respuesta ante
			Filtración de información	1) la implementación de la política; 2) la gestión de claves, incluyendo la generación de claves	incidentes de seguridad de la información
			Desarrollo de software abastecido externamente	f) los estándares a adoptarse para la implementación efectiva en toda la organización (cuál solución se utiliza para cuáles procesos comerciales); g) el impacto de utilizar información codificada sobre los controles que se basan en la inspección del contenido(por ejemplo, detección de virus);	
			Control de las vulnerabilidades técnicas	Comprobar que el sistema de gestión de claves este basado en un conjunto de estándares, procedimientos y métodos seguros acordados para	

				a) generar claves para los diferentes sistemas criptográficos y las diversas aplicaciones b) generar y obtener certificados de claves públicas c) distribuir claves a los usuarios planeados, incluyendo cómo se debieran activar las claves una vez recibidas d) almacenar claves, incluyendo cómo los usuarios autorizados obtienen acceso a las claves e) cambiar o actualizar las claves incluyendo las reglas sobre cuándo se debieran cambiar las claves y cómo se realiza esto f) lidiar con las claves comprometidas g) revocar las claves incluyendo cómo se debieran retirar o desactivar las claves por ejemplo, cuando las claves se han visto comprometidas o cuando el usuario deja la organización (en cuyos casos las claves también debieran ser archivadas); h) recuperar las claves cuando han sido perdidas o corrompidas como parte de la continuidad y gestión del negocio; por ejemplo, para recuperar la información codificada; i) archivar las claves; por ejemplo, para la información archivada o respaldada; j) destruir las claves; k) registrar y auditar las actividades relacionadas con la gestión de claves. Corroborar que para minimizar el riesgo de corrupción de los sistemas operacionales, se debe considerar los siguientes lineamientos para controlar los cambios: a) la actualización del software operacional, aplicaciones y bibliotecas de programas sólo debiera ser realizada por administradores capacitados con la apropiada autorización gerencial b) los sistemas operacionales sólo debieran mantener códigos ejecutables aprobados, y no códigos de desarrollo o compiladores c) el software de las aplicaciones y el sistema de operación sólo se debiera implementar después de una prueba extensa y satisfactoria; las pruebas debieran incluir pruebas de utilidad, seguridad, efectos sobre los sistemas y facilidad para el usuario; y se debieran llevar a cabo en sistemas separados; se debiera	

				asegurar que se hayan actualizado todas las bibliotecas fuente correspondientes del programa; d) se debiera utilizar un sistema de control de configuración para mantener el control de todo el software implementado, así como la documentación del sistema; e) se debiera establecer una estrategia de "regreso a la situación original" (rollback) antes de implementar los cambios; f) se debiera mantener un registro de auditoría de todas las actualizaciones a las bibliotecas del programa operacional; g) se debieran mantener las versiones previas del software de aplicación como una medida de contingencia; h) se debieran archivar las versiones antiguas del software, junto con toda la información requerida y los parámetros, procedimientos, detalles de configuración y software de soporte durante todo el tiempo que se mantengan la data en archivo. Comprobar que cuando se utiliza la data operacional para propósitos de prueba se aplique los siguientes lineamientos para protegerla: a) procedimientos de control de acceso, los cuales se aplican a los sistemas de aplicación operacional, y también se debieran aplicar a los sistemas de aplicación de prueba; b) debe existir una autorización separada para cada vez que se copia información operacional en un sistema de aplicación de prueba; c) la información operacional debe ser borrada de los sistemas de aplicación de prueba inmediatamente después de haber completado la prueba; d) se debe registrar el copiado y uso de la información operacional para proporcionar un rastro de auditoria Verificar que el personal de soporte no debe tener acceso irrestricto a las bibliotecas de fuentes del programa Comprobar que la actualización de las bibliotecas de fuentes del programa y los ítems asociados, y la	

				emisión de las fuentes del programa para los programadores sólo se realizará después de haber recibido la apropiada autorización Verificar la existencia de un registro de auditoría de todos los accesos a las bibliotecas de fuentes del programa Comprobar que el mantenimiento y copiado de las bibliotecas fuentes del programa estén sujeto a procedimientos estrictos de control de cambios Corroborar que los procedimientos de cambio incluyan: a) mantener un registro de los niveles de autorización acordados; b) asegurar que los cambios sean presentados por los usuarios autorizados; c) revisar los procedimientos de control e integridad para asegurar que no se vean comprometidos por los cambios; d) identificar todo el software, información, entidades de base de datos y hardware que requieran enmiendas; e) obtener la aprobación formal para propuestas detalladas antes de comenzar el trabajo; f) asegurar que los usuarios autorizados acepten a los cambios antes de la implementación; g) asegurar que el conjunto de documentación del sistema esté actualizado al completar cada cambio y que la documentación antigua se archive o se elimine; h) mantener un control de la versión para todas las actualizaciones del software; i) mantener un rastro de auditoría para todas las solicitudes de cambio; j) asegurar que la documentación de operación y procedimientos de usuarios sean cambiados conforme sean necesarios para seguir siendo apropiados; k) asegurar que la implementación de los cambios se realicen en el momento adecuado y no disturbe los procesos comerciales involucrados. Verificar que cuando se necesita modificar un paquete de software se debe considerar los siguientes puntos:	

				a) el riesgo de comprometer los controles incorporados y los procesos de integridad; b) si se debiera obtener el consentimiento del vendedor; c) la posibilidad de obtener del vendedor los cambios requeridos como actualizaciones del programa estándar; d) el impacto de si como resultado de los cambios, la organización se hace responsable del mantenimiento futuro del software. Comprobar que se consideran los siguientes puntos para limitar la filtración de la información; por ejemplo, a través del uso y explotación de los canales encubiertos (covert channels): a) escanear el flujo de salida de los medios y las comunicaciones en busca de información escondida; b) enmascarar y modular la conducta del sistema y las comunicaciones para reducir la probabilidad de que una tercera persona pueda deducir la información a partir de dicha conducta; c) hacer uso de los sistemas y el software considerados de la más alta integridad; por ejemplo, utilizando productos evaluados d) monitoreo regular de las actividades del personal y del sistema, cuando sea permitido bajo la legislación o regulación existente; e) monitorear la utilización del recurso en los sistemas de cómputo. Corroborar que cuando un software es abastecido externamente, se debieran considerar los siguientes puntos: a) contratos de licencias, propiedad de códigos, derechos de propiedad intelectual b) certificación de la calidad y exactitud del trabajo llevado a cabo c) contratos de depósito en custodia en el evento de la falla de una tercera persona d) derechos de acceso para a auditoría de la calidad y seguridad del trabajo realizado e) requerimientos contractuales para la funcionalidad	

				de calidad y seguridad del código f) prueba antes de la instalación para detectar códigos maliciosos y Troyanos. Comprobar que se sigue el siguiente lineamiento para establecer un proceso de gestión efectivo para las vulnerabilidades técnicas:la organización debiera definir y establecer los roles y responsabilidades asociadas con la gestión de la vulnerabilidad técnica; incluyendo el monitoreo de la vulnerabilidad, evaluación del riesgo de la vulnerabilidad, monitoreo de activos y cualquier responsabilidad de coordinación requerida Verificar la identificación de los recursos de información que se utilizarán para identificar las vulnerabilidades técnicas relevantes y mantener la conciencia sobre ellas para el software y otras tecnologías (en base a la lista de inventario de activos; estos recursos de información debieran actualizarse en base a los cambios en el inventario, o cuando se encuentran recursos nuevo o útiles Comprobar la definición una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas potencialmente relevantes Verificar que se evalúen los riesgos asociados con instalar el parche del sistema (los riesgos impuestos por la vulnerabilidad se debieran comparar con el riesgo de instalar el parche del sistema) Examinar que los parches son probados y evaluados antes de instalarlos para asegurar que sean efectivos y no resulten efectos secundarios que no se puedan tolerar; si el parche no está disponible, se pueden considerar otros controles: 1) desconectar los servicios o capacidades relacionadas con la vulnerabilidad; 2) adaptar o agregar controles de acceso; por ejemplo, firewalls en los límites de la red 3) mayor monitoreo para detectar o evitar ataques	

				reales 4) elevar la conciencia acerca de la vulnerabilidad; 5) mantener un registro de auditoría de todos los procedimientos realizados; 6) el proceso de gestión de vulnerabilidad técnica debiera ser monitoreado y evaluado regularmente para asegurar su efectividad y eficacia; 7) se debieran tratar primero los sistemas en alto riesgo.	
Información	Gestión de continuidad del negocio		Incluir la seguridad de la información en el proceso de gestión de continuidad del negocio Continuidad del negocio y evaluación del riesgo Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información Marco Referencial de la planeación de la continuidad del negocio Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio	Verificar que la gestión de continuidad del negocio incluya: a) entender los riesgos que enfrenta la organización en términos de la probabilidad y el impacto en el tiempo, incluyendo la identificación y priorización de los procesos comerciales críticos b) identificar todos los activos involucrados en los procesos comerciales críticos c) entender el impacto que probablemente tendrán las interrupciones causadas por incidentes en la seguridad de la información en el negocio (es importante encontrar las soluciones que manejen los incidentes que causan el menor impacto, así como los incidentes serios que pueden amenazar la viabilidad de la organización), y establecer los objetivos comerciales de los medios de procesamiento de la información; d) considerar la compra de un seguro adecuado que pueda formar parte de un proceso general de la continuidad del negocio, y que también sea parte de la gestión del riesgo operacional; e) identificar y considerar la implementación de controles preventivos y atenuantes adicionales; f) identificar los recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los requerimientos de seguridad de la información identificados; g) garantizar la seguridad del personal y la protección de los medios de procesamiento de la información y la propiedad organizacional h) formular y documentar los planes de continuidad del negocio tratando los requerimientos de seguridad de la información en línea con la estrategia acordada para la continuidad del negocio	Revisar cada elemento del(los) plan(es) de continuidad de negocio mediante los siguientes métodos: a) prueba flexible de simulación (table-top testing) de varios escenarios (discutiendo los acuerdos de recuperación comercial utilizando ejemplos de interrupciones) b) simulaciones (particularmente para capacitar a las personas en sus papeles en la gestión post-incidente/crisis) c) prueba de recuperación técnica (asegurando que los sistemas de información puedan restaurarse de manera efectiva d) prueba de recuperación en el local alternativo (corriendo los procesos comerciales en paralelo con las operaciones de recuperación lejos del local principal) e) pruebas de los medios y servicios del proveedor (asegurando que los servicios y productos provistos externamente cumplan con el compromiso contraído) f) ensayos completos (probando que la organización, personal, equipo, medios y procesos puedan lidiar con las interrupciones).

				i) pruebas y actualizaciones regulares de los planes y procesos j) asegurar que la gestión de la continuidad del negocio se incorpore a los procesos y estructura de la organización; se debiera asignar la responsabilidad del proceso de la gestión de la continuidad del negocio en el nivel apropiado dentro de la organización Probar que el proceso de planeación de la continuidad del negocio considere lo siguiente: a) identificar y acordar todas las responsabilidades y los procedimientos de continuidad del negocio; b) identificar la pérdida aceptable de la información y los servicios c) implementación de los procedimientos para permitir la recuperación y restauración de las operaciones comerciales y la disponibilidad de la información en las escalas de tiempo requeridas; se debiera prestar particular atención a la evaluación de las dependencias comerciales internas y externas y el establecimiento de los contratos debidos d) los procedimientos operacionales a seguir dependiendo de la culminación de la recuperación y restauración; e) documentación de los procesos y procedimientos acordados; f) educación apropiada del personal en los procedimientos y procesos acordados, incluyendo la gestión de crisis; g) prueba y actualización de los planes. Examinar que la planeación de continuidad del negocio trate los requerimientos de seguridad de la información y considere lo siguiente: a) las condiciones para activar los planes que describen el proceso a seguirse (por ejemplo, cómo evaluar la situación, quién va a participar) antes de activar cada plan b) los procedimientos de emergencia que describen las acciones a realizarse después del incidente que pone en riesgo las operaciones comerciales	

				c) procedimientos de contingencia que describen las acciones tomadas para trasladar las actividades comerciales esenciales de los servicios de soporte a locales temporales alternativos, y regresar los procesos comerciales a la operación en las escalas de tiempo requeridas d) procedimientos operacionales temporales a seguirse hasta la culminación de la recuperación y restauración; e) procedimientos de reanudación que describen las acciones a tomarse para regresar a las operaciones comerciales normales f) un programa de mantenimiento que especifica cómo y cuándo se va a probar el plan, y el proceso para mantener el plan g) las actividades de conciencia, educación y capacitación diseñadas para crear el entendimiento de los procesos de continuidad del negocio y asegurar que los procesos continúen siendo efectivos; h) las responsabilidades de las personas, describiendo quién es el responsable de ejecutar cuál componente del plan. Se debieran nombrar alternativas conforme sea necesario. i) los activos y recursos críticos necesitan ser capaces de realizar los procedimientos de emergencia, de respaldo y reanudación.	
Información	Cumplimiento		Identificación de la legislación aplicable Derechos de propiedad intelectual Protección de registros organizacionales Protección de la data y privacidad de la información personal Prevención del mal uso de los medios	Verificar que se considere los siguientes lineamientos para proteger cualquier material que se considere de propiedad intelectual: a) una política de cumplimiento de los derechos de propiedad intelectual y publicación que defina el uso legal de los productos de software e información; b) sólo adquirir software a través de fuentes conocidos y acreditados para asegurar que no sean violados los derechos de autor c) mantener el conocimiento de las políticas para proteger los derechos de propiedad intelectual, y notificar de la voluntad de tomar una acción disciplinaria contra el personal que los viole d) monitorear los registros de activos apropiados, e identificar todos los activos con los requerimientos para proteger los derechos de propiedad intelectual e) mantener prueba y evidencia de la propiedad de las	

			de procesamiento de la información Regulación de controles criptográficos Cumplimiento con las políticas y estándares de seguridad Chequeo del cumplimiento técnico Controles de auditoría de los sistemas de información Protección de las herramientas de auditoría de los sistemas de información	licencias, discos maestros, manuales, etc. f) implementar controles para asegurar que no se exceda el número máximo de usuarios permitidos g) llevar a cabo chequeos para que sólo se instalen software autorizados y productos con licencia h) proporcionar una política para mantener las condiciones de licencias apropiadas i) proporcionar una política para eliminar o transferir el software a otros j) utilizar las herramientas de auditoría apropiadas k) cumplir con los términos y condiciones del software e información obtenida de redes públicas l) no duplicar, convertir a otro formato o extraer de registros comerciales (audio, vídeo), aparte de los permitidos por la ley de derechos de autor; m) no copiar; completamente o en parte; libros, artículos, reportes u otros documentos; aparte de aquellos permitidos por la ley de derechos de autor. Comprobar la existencia de los siguientes pasos dentro de una organización para cumplir con el cumplimiento legal: a) emitir lineamientos sobre la retención, almacenaje, manipuleo y eliminación de registros e información; b) diseñar un programa de retención para identificar los registros y el período de tiempo durante el cual se debieran retener; c) mantener un inventario de fuentes de información clave d) se debieran implementar los controles apropiados para proteger los registros y la información de pérdida, destrucción y falsificación. Probar la existencias de los siguientes ítems para el cumplimiento con los acuerdos, leyes y regulaciones relevantes: a) las restricciones sobre la importación y/o exportación de hardware y software de cómputo para realizar funciones criptográficas;	

				b) las restricciones sobre la importación y/o exportación de hardware y software de cómputo diseñado para agregarle funciones criptográficas; c) restricciones sobre la utilización de la codificación; d) métodos obligatorios o voluntarios para que las autoridades de los países tengan acceso a la información codificada por hardware o software para proporcionar confidencialidad del contenido. Corroborar la existencia de los siguientes lineamientos: a) acordar los requerimientos de auditoría con la gerencia apropiada; b) acordar y controlar el alcance de los chequeos; c) los chequeos debieran limitarse a un acceso sólo-de-lectura al software y data; d) sólo se debiera permitir un acceso diferente al sólo-de-lectura para copias aisladas de los archivos del sistema, los cuales se pueden borrar cuando termina la auditoría, o se les puede dar la protección apropiada si existe la obligación de mantener dichos archivos en concordancia con los requerimientos de la documentación de auditoría; e)identificar explícitamente los recursos para realizar los chequeos y debieran estar disponibles; f)identificar y acordar los requerimientos de procesamiento especial o adicional; g)monitorear y registrar todos los accesos para producir un rastro de referencia; se debiera considerar el uso de rastros de referencia con la hora impresa para la data o sistemas críticos; h) se debieran documentar todos los procedimientos, requerimientos y responsabilidades; i) la(s) personas(s) que llevan a cabo la auditoría debieran ser independientes a las actividades auditadas.	
Información	Definir la arquitectura de la información		Modelo de arquitectura de información empresarial Diccionario de	Garantizar la exactitud de la arquitectura de información y del modelo de datos Asignar propiedad de datos Clasificar el uso de la información utilizando un	Revisar: Frecuencia de actualizaciones al modelo empresarial de datos

			datos empresarial y reglas de sintaxis de datos Esquema de clasificación de datos Administración de la integridad	esquema de clasificación acordado Asegurar la consistencia entre los componentes de la arquitectura TI (arquitectura de información, diccionario de datos, aplicaciones sintaxis de datos, esquemas de clasificación y niveles de seguridad) Mantener integridad de datos Establecer un modelo de datos empresarial Reducir la redundancia de los datos Dar soporte efectivo a la administración de información Optimizar el uso de la información Garantizar la integración transparente de las aplicaciones hacia los procesos de negocio Responder a los requisitos de negocio en de manera alineada con la estrategia del negocio Crear agilidad de TI	% de elementos de datos que no tienen propietario Frecuencia de actividades de validación de datos Nivel de participación de la comunidad de usuarios % de elementos de datos que no son parte del modelo de datos empresarial % de falta de cumplimiento del esquema de clasificación de datos % de aplicaciones que no cumplen con las arquitecturas de información El % de satisfacción de los usuarios respecto al modelo de información (esto es, ¿el modelo de datos es fácil de usar?) % de elementos de datos redundantes / duplicados
Información	Administrar la calidad		Sistema de administración de calidad Estándares y prácticas de calidad Estándares de desarrollo y de adquisición IT Enfoque en el cliente	Definir estándares y prácticas de calidad Monitorear y revisar el desempeño interno y externo contra los estándares y prácticas de calidad definidos Establecer estándares y cultura de calidad para los procesos de TI Establecer una función de aseguramiento de la calidad para una TI eficiente y efectiva Monitorear la efectividad de los procesos y proyectos de TI Garantizar la satisfacción de los usuarios finales con oferta de servicios y niveles de servicio Reducir los defectos y repeticiones de trabajo en la prestación de servicios y soluciones Entregar proyectos a tiempo y dentro del presupuesto, satisfaciendo estándares de calidad	Revisar: % de proyectos que reciben revisiones de aseguramiento de calidad % de personal de TI que recibe entrenamiento administrativo / concientización % de proyectos y procesos de TI con participación activa en el aseguramiento de calidad por parte de los participantes % de procesos que reciben revisiones de aseguramiento de calidad Porcentaje de interesados que participan en encuestas de calidad % de defectos no descubiertos antes de entrar en producción % de reducción en el número de incidentes de alta severidad por usuario por mes

			Medición, monitoreo y revisión de la calidad		% de proyectos de TI revisados y autorizados por aseguramiento de calidad que satisfacen las metas y objetivos de calidad % de procesos de TI revisados de manera formal por aseguramiento de calidad de manera periódica que cumplen las metas y objetivos de calidad % de interesados satisfechos con la calidad de TI (ponderado por importancia)
Información	Educar y entrenar a los usuarios		Identificación de necesidades de entrenamiento y educación Impartición de entrenamiento y educación Evaluación del entrenamiento recibido	Establecer plan de entrenamiento Organizar el entrenamiento Impartir el entrenamiento Monitorear y reportar la efectividad del entrenamiento Establecer un programa de capacitación para usuarios a todos los niveles utilizando los métodos con mejor rentabilidad. Transferir el conocimiento a los usuarios de las aplicaciones y soluciones tecnológicas. Incrementar la conciencia sobre los riesgos y las responsabilidades involucrados en el uso de soluciones y aplicaciones tecnológicas. Garantizar la satisfacción de los usuarios finales con ofrecimiento de servicios y niveles de servicio. Garantizar el uso apropiado y el desempeño de las aplicaciones y soluciones tecnológicas. Optimizar la infraestructura, los recursos y las capacidades de TI.	Revisar: Frecuencia de actualizaciones del programa de capacitación. Lapso de tiempo entre la identificación de la necesidad de capacitación y la impartición de la misma. # de llamadas de soporte para capacitación o para responder preguntas % de satisfacción de los interesados a quienes se les brindó capacitación % de empleados capacitados. Mejoras en la productividad de los empleados como resultado de un mejor entendimiento de los sistemas. Aumento de la satisfacción del usuario con la introducción de servicios, sistemas o nuevas tecnologías.
Información	Administrar la información		Requerimientos del negocio para administración de	Respaldo de datos y prueba de restauración. Administración de almacenamiento de datos en sitio y fuera del sitio.	

			datos	Desecho seguro de datos y equipo.	Revisar:
			Acuerdos de almacenamiento y conservación Sistema de administración de librerías de medios Respaldo y restauración Requerimientos de seguridad para la administración de datos	Mantener la completitud, exactitud, validez y accesibilidad de los datos almacenados. Asegurar los datos durante el desecho de medios Administrar de manera efectiva el almacenamiento de medios. Optimizar el uso de información. Garantizar que la información crítica y confidencial se mantiene oculta contra quienes no deben tener acceso a ella. Garantizar que TI cumpla con las leyes y regulaciones.	Frecuencia de las prueba de los medios de respaldo. Tiempo promedio del tiempo de restauración de datos. % de restauraciones de datos exitosas. # de incidentes en los que se recuperaron datos de medios y equipos ya desechados. # de incidentes de falta de servicio o de integridad de información causados por falta de capacidad de almacenamiento. Número de eventos donde se presente incapacidad para recuperar información crítica para el proceso de negocio Satisfacción del usuario con la disponibilidad de la información. Incidentes de incumplimiento de las leyes debido a problemas con la administración del almacenamiento.
Información	Monitorear y evaluar el control interno		marco de trabajo de control interno Revisiones de Auditoría Excepciones de control Auto-evaluación de control Control interno para terceros Acciones	Definir un sistema de controles internos integrado al marco de trabajo de procesos de TI Monitorear y reportar la efectividad de los controles internos sobre TI Reportar las excepciones de control a la gerencia para tomar acciones Monitorear el logro de los objetivos de control interno establecidos para los procesos de TI Identificar las acciones de mejoramiento para el control interno Garantizar que los servicios y la infraestructura de TI pueden resistir y recuperarse apropiadamente de fallas debidas a error, ataque deliberado o desastre. Proteger el logro de los objetivos de TI	Revisar: # y cobertura de auto-evaluaciones de control # y cobertura de controles internos sujetos a revisiones de auditoría Tiempo transcurrido entre la ocurrencia de una deficiencia de control interno y el reporte de ésta # frecuencia y cobertura de reportes de cumplimiento interno Frecuencia de incidentes de control interno

			correctivas	Garantizar el cumplimiento de TI con las leyes y regulaciones Proteger y registrar todos los activos de TI	# de debilidades identificadas por reportes externos de calificación y certificación #de iniciativas para mejorar el control # de eventos regulatorios o legales que no cumplen. # de acciones oportunas sobre problemas de control interno Índice de satisfacción y confort de la alta dirección con los reportes de vigilancia del control interno # de brechas importantes de control interno
Información	Garantizar el cumplimiento regulatorio		leyes y regulaciones con impacto potencial sobre TI cumplimiento con requerimientos regulatorios Reportes integrados.	Identificar los requisitos legales y regulatorios relacionados con TI Entrenar al personal de TI sobre su responsabilidad de cumplimiento Evaluar el impacto de los requisitos regulatorios Monitorear y reportar el cumplimiento de los requerimientos regulatorios Identificar todas las leyes y regulaciones aplicables e identificar el nivel de cumplimiento de TI Procurar la alineación de las políticas, estándares y procedimientos de TI para manejar de forma eficiente los riesgos de no cumplimiento Minimizar el impacto al negocio de los eventos de cumplimiento identificados dentro de TI Garantizar el cumplimiento de TI con las leyes y regulaciones	Revisar: Demora promedio entre la identificación de los eventos externos de cumplimiento y su resolución Retraso de tiempo promedio entre la publicación de una nueva ley o regulación y el inicio de la revisión de cumplimiento Días de entrenamiento por empleado de TI por año, referentes al cumplimiento # de problemas críticos de no cumplimiento identificados por año Frecuencia de revisiones de cumplimiento Costo del no cumplimiento de TI, incluyendo arreglos y multas # de problemas de no cumplimiento reportados al consejo directivo , o que hayan causado comentarios o vergüenza pública
Información	Mantenimiento de		Análisis del impacto	Verificar si el tipo de respaldo elegido es:	

	la seguridad, integridad y respaldo de la data		del negocio Plan de contingencia del sistema de información de una LAN	1)Full 2)Incremental 3)Diferencial Comprobar que se tomaron en consideración los siguientes criterios para seleccionar la mejor solución de respaldo de data: 1)Equipo de interoperabilidad 2)Volumen de almacenamiento 3)Vida media 4)Software de respaldo	
Información	Identificación de almacenamiento alternativo e instalaciones de procesamiento		Análisis del impacto del negocio Plan de contingencia del sistema de información de una LAN	Verificar si las instalaciones alternativas de procesamiento corresponden con el nivel de preparación para funcionar como una instalación de operaciones del sistema, dichos niveles son: 1)lugares fríos 2)lugares cálidos 3)lugares calientes	
Información	Uso de la alta disponibilidad de los procesos		Análisis del impacto del negocio Plan de contingencia del sistema de información de una LAN	Verificar la existencia de la alta disponibilidad de los procesos para maximizar el tiempo de actividad y su disponibilidad Comprobar la construcción de redundancia y flexibilidad en la arquitectura	Revisar que el sistema este activo el 99.9% o más durante un año
Comunicación	Definir un plan estratégico de TI		Administración del valor de TI Alineación de TI con el negocio Evaluación del desempeño actual Plan estratégico de TI	Involucrarse con la alta gerencia y la gerencia del negocio para alinear los planes estratégicos de TI con las necesidades del negocio actuales y futuras Entender las capacidades actuales de TI Traducir el plan estratégico de TI a planes tácticos Brindar un esquema de prioridades para los objetivos del negocio que cuantifiquen los requisitos del negocio Definir cómo los requisitos de negocio se traducen en ofertas de servicio	Revisar; Rastrear lo retrasos existentes entre las actualizaciones del plan estratégico/táctico del negocio y las actualizaciones del plan estratégico/táctico de TI % de reuniones de planeación estratégica/táctica de TI donde los representantes del negocio participaron de forma activa Retraso entre actualizaciones de planes estratégicos de TI y actualizaciones de planes tácticos de TI

			Planes tácticos de TI Administración del portafolio de TI	Definir la estrategia para la entrega de las ofertas de servicio Contribuir a la gestión del portafolio de inversiones de negocio de TI Establecer claridad del impacto de los riesgos en los objetivos y en los recursos Proporcionar transparencia y entendimiento de costos, beneficios, estrategias, políticas y niveles de servicio de TI Responder a los requerimientos del negocio en alineación con la estrategia del negocio Responder a los requerimientos de gobierno alineados con la dirección del consejo directivo	% de planes tácticos de TI con el contenido/estructura predefinida de esos planes % de iniciativas/proyectos TI dirigidos por propietarios del negocio % de objetivos de TI en el plan estratégico de TI que dan soporte al plan estratégico del negocio % de iniciativas de TI en el plan táctico de TI que da soporte al plan táctico del negocio % de proyectos de TI en el portafolio de proyectos de TI que se pueden rastrear de forma directa al plan táctico de TI Grado de aprobación de los propietarios del negocio de los planes estratégicos/tácticos de TI Grado de cumplimiento de requisitos de gobierno y de negocio Nivel de satisfacción del negocio con el estado actual del portafolio de proyectos y aplicaciones (número, alcance, etc.)
Comunicación	Determinar la dirección tecnológica		Planeación de la dirección tecnológica Plan de infraestructura tecnológica Monitoreo de tendencias y regulaciones futuras Estándares tecnológicos Consejo de	Definir los estándares de la infraestructura técnica con base en los requisitos de la arquitectura de la información Establecer el plan de la infraestructura técnica equilibrado contra los costos, riesgos y requerimientos Establecer un foro para orientar la arquitectura y verificar el cumplimiento Reconocer y aprovechar las oportunidades tecnológicas Desarrollar e implantar el plan de infraestructura tecnológica Definir los estándares tecnológicos y de arquitectura para la infraestructura de la TI	Revisar: Frecuencia de las reuniones sostenidas por el foro tecnológico Frecuencia de las reuniones sostenidas por el consejo de arquitectura de TI Frecuencia de la revisión / actualización del plan de infraestructura tecnológica % de incumplimiento de los estándares tecnológicos # de plataformas tecnológicas por función a lo largo de toda la empresa # y tipo de desviaciones con respecto al plan de

			arquitectura	Optimizar la infraestructura, los recursos y las capacidades de TI Adquirir y mantener integrados y estandarizados los sistemas de aplicación	infraestructura tecnológica
Comunicación	Definir los procesos, organización y relaciones de TI		Marco de trabajo del proceso Ubicación organizacional de la función de TI Estructura organizacional Roles y responsabilidades Responsabilidad de aseguramiento de calidad de TI Responsabilidad sobre el riesgo, la seguridad y el cumplimiento Propiedad de datos y de sistemas Segregación de funciones Políticas y procedimientos para personal contratado	Definir un marco de trabajo de procesos para TI Establecer organismos y estructuras organizacionales apropiadas Establecer estructuras y relaciones organizacionales para TI, que sean flexibles y responsables Definir propietarios, roles y responsabilidades de forma clara para todos los procesos TI y para todas las relaciones con los interesados Responder a los requisitos de gobierno de acuerdo con las directivas del consejo directivo Responder a los requisitos de negocio de acuerdo con la estrategia del negocio Crear la agilidad de TI	Revisar: % de roles con puestos documentados y descripciones de autoridad % de funciones / procesos operativos de TI que se conectan con las estructuras operativas del negocio Frecuencia de reuniones de los comités estratégicos y de dirección # de responsabilidades conflictivas en vista de la segregación de funciones # de escalamientos o problemas sin resolver debido a la carencia o insuficiencia de asignaciones de responsabilidad % de stakehokders satisfechos con el nivel de respuesta de TI Satisfacción de participantes (encuestas) # de iniciativas de negocio retrasadas debido a la inercia operativa de TI o a la falta de disponibilidad de las capacidades necesarias # de procesos de negocio que no reciben soporte por parte de TI que lo deberían recibir de acuerdo a la estrategia # de actividades esenciales de TI fuera de TI que no están aprobadas o que no están sujetas a los estándares de TI

Comunicación	Comunicar las aspiraciones y la dirección de la gerencia		Ambiente de políticas y de control Riesgo Corporativo y Marco de Referencia de Control Interno de TI Administración de políticas para TI Implantación de políticas de TI	Definir un marco de control para TI Elaborar e implantar políticas de TI Reforzar las políticas de TI Elaborar un marco de control para TI, que sea común e integral Elaborar un conjunto de políticas de TI que sea común e integral Comunicar la estrategia, políticas y el marco de control de TI Asegurarse de la transparencia y el entendimiento de los costos, beneficios, estrategia, políticas y niveles de servicio de TI. Asegurarse de que se puede confiar en las transacciones automatizadas y en los intercambios de información del negocio Asegurarse de que la información crítica y confidencial no esté disponible a quienes no deben verla Asegurar un impacto mínimo en el evento de una interrupción o cambio del servicio de TI Asegurar el uso y desempeño adecuados de las aplicaciones y de las soluciones tecnológicas Garantizar que los servicios e infraestructura de TI pueden resistir y recuperarse de fallas debidas a errores, ataques o desastres.	Revisar: Frecuencia de revisiones / actualizaciones de las políticas Tiempo entre la aprobación de las políticas y la comunicación a los usuarios. % de interesados que entienden las políticas de TI % de interesados que entienden el marco de control de TI % de interesados que no cumplen las políticas # de ocasiones en que se puso en riesgo la información confidencial # de interrupciones al negocio debidas a interrupciones en el servicio de TI Nivel de entendimiento de los costos, beneficios, estrategia, políticas y niveles de servicio de TI
Comunicación	Administrar los recursos humanos de TI		Reclutamiento y Retención del Personal	Contratar y entrenar al personal de TI para apoyar los planes tácticos de TI Mitigar el riesgo de la sobre-dependencia en individuos clave	Revisar: % de personal de TI que hayan completado sus planes profesionales y de desarrollo

			Competencias del personal Asignación de roles Entrenamiento del personal de TI Dependencia sobre los individuos Procedimientos de Investigación del personal Evaluación del desempeño del empleado Cambios y terminación de trabajo	Revisión del desempeño del personal Elaborar prácticas administrativas profesionales para RH de TI Utilizar a todo el personal de TI de forma efectiva mientras que al mismo tiempo se minimiza la dependencia de personal clave. Adquirir y mantener habilidades de TI que respondan a la estrategia de TI Crear la agilidad de la TI	% de personal con revisiones de desempeño oportunas, documentadas y validadas % de puestos con descripciones y calificaciones de contratación # promedio de días de entrenamiento y desarrollo (incluyendo adiestramiento) por persona por año Rotación de personal de TI % de personal de TI certificado de acuerdo a las necesidades del puesto Número promedio de días para ocupar los roles vacantes de TI % de personal de TI que satisfacen el perfil de habilidades para los roles requeridos como se describe en la estrategia % de roles de TI ocupados Número de días perdidos debido a ausencias no planeadas % de personal de TI que terminó el plan de entrenamiento anual de TI Proporción real de contratistas vs. personal, comparado con la proporción planeada % de empleados de TI que se han sometido a verificación de antecedentes % de roles de TI con personal calificado de respaldo Nivel de satisfacción de participantes respecto a la experiencia y habilidades del personal % de personal de TI satisfecho (métrica compuesta) Rotación de personal de TI
Comunicación	Facilitar la operación y el uso		Plan para soluciones de	Desarrollar y hacer disponible la documentación de transferencia del conocimiento	Revisar: Nivel de asistencia a entrenamiento de usuarios y

			operación	Participar y entrenar a usuarios y a la gerencia del negocio, personal de soporte y personal de operación Generar materiales de entrenamiento Proporcionar manuales efectivos de usuario y de operación y materiales de entrenamiento para aplicaciones y soluciones técnicas. Transferir el conocimiento necesario para la operación exitosa del sistema. Garantizar el uso y desempeño apropiado de aplicaciones y de soluciones de tecnología. Garantizar la satisfacción de usuarios finales con ofrecimientos de servicio y niveles de servicio. Integrar en forma transparente las aplicaciones y las soluciones de tecnología dentro de los procesos del negocio. Reducir defectos y correcciones en la entrega de soluciones y servicios.	operadores para cada aplicación Lapso de tiempo entre modificaciones y actualizaciones de materiales de entrenamiento, procedimientos y documentación Disponibilidad, integridad y exactitud de la documentación de usuario y de operación # de aplicaciones con entrenamiento de apoyo adecuado para el usuario y la operación # de incidentes provocados por deficiencias en la documentación y entrenamiento de usuario y de operación # de solicitudes de entrenamiento manejada por el servicio a usuarios Puntajes satisfactorios para entrenamiento y documentación en relación con el usuario y los procedimientos de operación Reducción de costos para producir/mantener documentación del usuario, procedimientos de operación y materiales de entrenamiento # de aplicaciones en las que los procedimientos de TI se integran de forma continua dentro de los procesos del negocio % de propietarios de negocios satisfechos con el entrenamiento de aplicaciones y materiales de apoyo
			Transferencia de conocimiento a la gerencia del negocio Transferencia de conocimiento a usuarios finales Transferencia de conocimiento al personal de operaciones y soporte		
Comunicación	Instalar y acreditar soluciones y cambios		Entrenamiento Plan de prueba Plan de implantación	Establecer una metodología de prueba que garantice pruebas de aceptación suficientes antes de liberar Rastrear cambios a todos los componentes de la configuración Realizarla planeación de la liberación Ejecutar y aprobar los resultados de las pruebas por parte de la administración del negocio Verificar y confirmar que las aplicaciones y soluciones de tecnología se ajustan al propósito deseado	Revisar: Grado de involucramiento del stakeholder en el proceso de instalación y acreditación % de proyectos con plan de prueba documentado y aprobado # de lecciones aprendidas de la revisión posterior a la implantación % de errores encontrados durante la revisión de aseguramiento de calidad en las funciones de instalación y acreditación

			Ambiente de prueba Prueba de cambios Prueba final de aceptación Transferencia a producción Liberación de software Distribución del sistema Registro y rastreo de cambios Revisión posterior a la implantación	Liberar y distribuir apropiadamente las aplicaciones aprobadas y las soluciones de tecnología. Preparar a los usuarios y operadores del negocio para el uso de aplicaciones y soluciones de tecnología. Garantizar que las nuevas aplicaciones de negocio y los cambios a las aplicaciones existentes estén libres de error. Garantizar que las transacciones automatizadas de negocio y los intercambios de información sean confiables. Reducir los defectos y revisiones de trabajo en la entrega de soluciones y servicios. Responder a los requerimientos del negocio de acuerdo con la estrategia de negocio. Integrar las aplicaciones y soluciones de tecnología de forma transparente a los procesos de negocio. Garantizar el uso y desempeño apropiado de las aplicaciones y soluciones de tecnología. Garantizar que los servicios y la infraestructura de TI pueden resistir apropiadamente y recuperarse de fallas por errores, ataques deliberados o desastres.	# de cambios sin la autorizaciones requeridas de la gerencia antes de la implantación # de errores encontrados durante auditorías internas o externas con respecto al proceso de instalación y acreditación Repetición del trabajo después de la implantación debida a las pruebas inadecuadas de aceptación. Llamadas de usuarios servicio de usuarios debidas a entrenamiento inadecuado Tiempo perdido de aplicación o reparaciones de datos provocadas por pruebas inadecuadas % de participantes satisfechos con la integridad de los datos de los nuevos sistemas % de sistemas que satisfacen los beneficios esperados tal como se midieron en el proceso posterior a la implantación
Comunicación	Definir y administrar los niveles de servicio		Marco de trabajo de la administración de los niveles de servicio Definición de	Definición de servicios. Formalización de convenios internos y externos alineados con los requerimientos y las capacidades de entrega. Notificación del cumplimiento de los niveles de servicio (reportes y reuniones). Asegurar que los reportes están hechos a la medida de la audiencia que los recibe.	Revisar: Número de reuniones formales de revisión de los SLAs con los responsables de negocio por año % de niveles de servicio reportados % de niveles de servicio reportados de forma automatizada

			servicios		Número de días de trabajo transcurridos para ajustar un nivel de servicio después del acuerdo con el cliente.
			Acuerdos de niveles de servicio	Retroalimentar requerimientos de servicio, nuevos y actualizados, al proceso de planeación estratégica. Establecer un entendimiento común de los niveles de servicio requeridos. Formalizar y monitorear los convenios de niveles de servicio y los criterios de desempeño.	% de servicios entregados que no están en el catálogo. % de servicios que cumplen con los niveles de servicio.
			Acuerdos de niveles de operación	Alinear los servicios entregados con los niveles de servicio acordados. Crear un catálogo de servicios actualizado alineado con las metas del negocio.	% de niveles de servicio que se miden. % de participantes del negocio satisfechos de que los servicios entregados cumplen con los niveles de servicio acordados.
			reporte del cumplimento de los niveles de servicio	Asegurar la satisfacción de los usuarios finales con ofertas de servicio y niveles de servicio. Responder a los requerimientos de negocio alineados con la estrategia de negocio. Asegurar transparencia y entendimiento de los costos, beneficios, estrategia, políticas y niveles de servicio de TI.	% de usuarios satisfechos de que los servicios entregados cumplen con los niveles de servicio acordados.
	Garantizar la seguridad de los sistemas		Administración de la seguridad de TI	Entendimiento de los requerimientos, vulnerabilidades y amenazas de seguridad. Administración de las identidades y autorizaciones de los usuarios de manera estándar.	Revisar: Frecuencia y revisión del tipo de eventos de seguridad a ser monitoreados. # y tipo de cuentas obsoletas
			Plan de seguridad de TI	Definición de incidentes de seguridad. Pruebas de seguridad regulares.	# de direcciones IP no autorizadas, puertos y tipos de tráfico denegados % de llaves criptográficas comprometidas y revocadas
			Administración de identidad	Permitir el acceso a información crítica y sensible solo a usuarios autorizados. Identificar, monitorear y reportar vulnerabilidades e incidentes de seguridad.	# de derechos de acceso autorizados, revocados, restaurados o cambiados.
			Administración de cuentas del usuario	Detectar y resolver accesos no autorizados a la información, aplicaciones e infraestructura. Minimizar el impacto de las vulnerabilidades y de los incidentes de seguridad.	# y tipo de violaciones de acceso reales y sospechadas. # de violaciones en la segregación de funciones

			Pruebas, vigilancia y monitoreo de la seguridad Definición de incidente de seguridad Protección de la tecnología de seguridad Administración de llaves criptográficas Prevención, detección y corrección de software malicioso Seguridad de la red Intercambio de datos sensitivos	Garantizar que la información crítica y confidencial esté prohibida a aquellos que no tienen acceso a ella. Garantizar que las transacciones e intercambios de información automatizados del negocio sean confiables. Mantener la integridad de la información y de la infraestructura de procesamiento. Proteger y mantener registro de todos los activos de TI. Garantizar que los servicios y la infraestructura de TI pueden resistir y recuperarse de fallas originadas por un error, ataque deliberado o desastre.	% de usuarios que no cumplen con los estándares de contraseñas . # y tipo de código malicioso prevenido. # de incidentes con impacto al negocio # de sistemas que no cumplen con los requerimientos de seguridad Tiempo para otorgar, cambiar o eliminar privilegios de acceso.
Comunicación	Administrar la mesa de servicio y los incidentes		Registro de consultas de clientes	Instalación y operación de una mes de servicios Monitoreo y reporte de tendencias. Alineación de las prioridades de resolución con las prioridades del negocio. Definición de procedimientos y criterios de	Revisar: % de incidentes y de solicitudes de servicio reportadas y registradas usando herramientas automatizadas

			Escalamiento de incidentes Cierre de incidentes Análisis de tendencias	escalamiento claros. Analizar, documentar y escalar incidentes de manera oportuna. Responder a las consultas de forma precisa y oportuna. Llevar a cabo de manera regular análisis de tendencias de incidentes y consultas. Garantizar la satisfacción de los usuarios finales con ofrecimientos de servicios y niveles de servicio. Garantizar el uso y desempeño apropiados de las aplicaciones y soluciones tecnológicas. Garantizar que los servicios de TI estén disponibles cuando se requieran.	# de días de entrenamiento del personal de la mesa de servicios por año # de llamadas atendidas por el personal de la mesa de servicios por hora % de incidentes que requieren soporte local (en campo, visita personal) Acumulación de consultas sin resolver. % de resoluciones en la primera línea de atención con base en el total de peticiones. % de incidentes reabiertos. Índice de abandono de llamadas. Duración promedio de los incidentes por severidad. Velocidad promedio para responder a peticiones vía teléfono y vía web o e-mail. Satisfacción del usuario con el soporte de primera línea (mesa de servicios o base de conocimientos) % de incidentes resueltos dentro de un período de tiempo aceptable/ acordado.
Comunicación	Administrar los problemas		Identificación y clasificación de problemas Rastreo y resolución de problemas Cierre de	Dar suficiente autoridad al gerente de problemas. Hacer análisis de causa raíz de los problemas reportados. Analizar tendencias. Tomar propiedad de los problemas y del progreso de la resolución de problemas. Registrar y rastrear problemas de operación hasta su resolución. Investigar las causas raíz de todos los problemas significativos. Definir soluciones para los problemas operativos identificados.	Revisar: Duración promedio entre el registro de un problema y la identificación de la causa raíz. % de problemas para los cuales se realizó un análisis de causa raíz. La frecuencia de reportes o actualizaciones de un problema en curso, con base en la severidad del problema. % de problemas registrados y rastreados % de problemas recurrentes (en un periodo de

			problemas		tiempo) por severidad.
			Integración de las administraciones de cambios, configuración y problemas	Garantizar la satisfacción de los usuarios finales con ofrecimientos de servicios y niveles de servicio. Reducir el re-trabajo y los defectos de la solución y de la prestación de servicios. Proteger el logro de los objetivos de TI	% de problemas resueltos en el tiempo requerido. # de problemas abiertos/nuevos/cerrados por severidad. Desviación promedio y estándar del lapso de tiempo entre la identificación del problema y su resolución. Desviación promedio y estándar del lapso de tiempo entre la resolución del problema y su cierre. # de problemas recurrentes con impacto al negocio. # de interrupciones al negocio ocasionadas por problemas operativos.
Comunicación	Administrar las operaciones		Procedimientos e instrucciones de operación Programación de tareas Monitoreo de la infraestructura de TI Documentos sensitivos y dispositivos de salida. Mantenimiento preventivo del	Operación del ambiente de TI de acuerdo con los niveles de servicio acordados, con instrucciones definidas y con supervisión cercana. Mantenimiento preventivo y monitoreo de la infraestructura de TI. Definir procedimientos de operación y alinearlos con los niveles de servicio acordados. Realizar el procesamiento de solicitudes especiales de acuerdo a los niveles de servicio acordados. Brindar resguardos físicos para la información sensible. Garantizar que los servicios y la infraestructura de TI puedan resistir y recuperarse de fallas ocasionadas por errores, ataques deliberados o desastres. Garantizar la satisfacción de los usuarios finales con ofrecimientos de servicios y niveles de servicio. Asegurar que los servicios de TI están disponibles conforme se requieran.	Revisa:; # de días de capacitación por año para el personal de operaciones % de activos de hardware incluidos en los programas de mantenimiento preventivo. % de planes de trabajo automatizados Frecuencia de actualización de los procedimientos operativos. # de incidentes de tiempo sin servicio causados por la desviación de los procedimientos de operaciones % peticiones y trabajos programados que no se cumplen a tiempo. # de incidentes de tiempo sin servicio y de retrasos causados por procedimientos inadecuados. # de niveles de servicio impactados por incidentes operativos

			hardware		Horas de tiempo sin servicio no planeadas causadas por incidentes en la operación.
Comunicación	Monitorear y evaluar el desempeño de TI:		Enfoque del Monitoreo Definición y recolección de datos de monitoreo Método de monitoreo Evaluación del desempeño Reportes al consejo directivo y a ejecutivos Acciones correctivas	Capturar, cotejar y traducir los reportes de desempeño de procesos en reportes gerenciales Comparar el desempeño contra las metas acordadas e iniciar las medidas correctivas necesarias Establecer objetivos, KGIs y KPIs medibles para TI, así como procesos clave Medir, monitorear y reportar métricas de proceso Identificar e implantar acciones de mejoramiento del desempeño Responder a los requerimientos de gobierno de acuerdo a la directriz del consejo de Dirección. Responder a los requerimientos del negocio en alineación con la estrategia del negocio. Garantizar que TI demuestre una calidad de servicio eficiente en costos, mejora continua y preparación para cambios futuros Garantizar la transparencia y el entendimiento de los costos, beneficios, estrategia, políticas y niveles de servicio de TI	Revisar: Demora entre el reporte de la deficiencia y el inicio de la acción Demora en la actualización de mediciones que reflejen los objetivos, las mediciones, las metas y los benchmarks actuales. # de métricas (por proceso) # de relaciones causa efecto identificadas e incorporadas en el monitoreo Esfuerzo requerido para recolectar datos de medición # de problemas no identificados por el proceso de medición % de métricas que se pueden evaluar por comparación contra estándares de la industria y metas establecidas Satisfacción de los interesados con el proceso de medición % de procesos críticos monitoreados # de acciones de mejoramiento impulsadas por las actividades de monitoreo # de metas de desempeño alcanzadas (indicadores en control) # de cambios a las metas para los indicadores de efectividad y eficiencia de los procesos de TI Satisfacción de la gerencia y de la entidad de gobierno con los reportes de desempeño Reducido # de deficiencias de los procesos sobresalientes

Comunicación	Proporcionar Gobierno de TI		marco de trabajo de gobierno para TI Alineamiento estratégico Administración de recursos Administración de riesgos. Medición del desempeño.	Establecer un marco de trabajo para el gobierno de TI integrado al gobierno corporativo Obtener una garantía independiente respecto al estatus del gobierno de TI Integrar el gobierno de TI a los objetivos del gobierno corporativo Elaborar reportes completos y oportunos para el consejo directivo sobre la estrategia, el desempeño y los riesgos de TI Responder a las preocupaciones y consultas del consejo directivo respecto a la estrategia, desempeño y riesgos de TI Procurar aseguramiento independiente respecto al cumplimiento de las políticas, estándares y procedimientos de TI Responder a los requerimientos de gobierno de acuerdo con las directrices del consejo directivo Garantizar la transparencia y el entendimiento de los costos, beneficios, estrategias, políticas y niveles de servicio de TI Garantizar que IT cumpla las leyes y regulaciones Asegurar que TI demuestre una calidad de servicio eficiente en costo, mejora continua y presteza para cambios futuros	Revisar: % del equipo entrenado en gobierno (ej. Códigos de conducta) # de ejecutivos éticos por departamento Frecuencia en que el gobierno de TI es un punto de la agenda en las reuniones estratégicas/de comité de TI % de miembros del consejo directivo con entrenamiento o experiencia en gobierno de TI Obsolescencia de recomendaciones acordadas Frecuencia de reportes al consejo sobre las encuestas de satisfacción a las terceras partes interesadas Frecuencia de reportes provenientes de TI hacia el consejo directivo (incluyendo el nivel de madurez) Número de brechas de gobierno Frecuencia de revisiones independientes del cumplimiento de TI # de veces que TI se encuentra en la agenda del consejo directivo de manera proactiva Frecuencia de reportes del consejo directivo sobre TI a los as terceras partes interesadas (incluyendo el nivel de madurez) # de eventos recurrentes de TI en las agendas del consejo directivo
Comunicación	Desarrollar Consideraciones de contingencia para las telecomunicacione	Coordinador	Análisis del impacto del negocio Plan de	Verificar la identificación de los puntos de fallo que afectan los sistemas o procesos críticos señalados en el Analisis del impacto del negocio. Este análisis podría incluir amenazas para el sistema de cableado, tales como cortes de cables, interferencias	

	s		contingencia del sistema de información de una LAN	electromagnéticas y de radiofrecuencia, y el daño resultante del fuego, el agua y otros peligros. Como solución, los cables redundantes pueden ser instalado cuando sea apropiado. Por ejemplo, podría no ser rentable para instalar cables duplicados para equipos de sobremesa. Sin embargo, podría ser rentable para instalar un cable gigabit entre los pisos para que los hosts en ambas plantas puedan volver a conectarse si el cable primario fue cortado Comprobar que la planificación de contingencia también considere los dispositivos de conexión de red como hubs, switches, routers y puentes Examinar que se debe caracterizar las funciones que cada dispositivo sirve en la red, y una solución de contingencia debe ser desarrollado para cada dispositivo en función de su criticidad en el análisis del impacto del negocio Corroborar si el acceso remoto está establecido como una estrategia de contingencia, los requisitos de ancho de banda de datos deben ser identificadas y utilizadas para escalar la solución de acceso remoto Además, los controles de seguridad como la autenticación multifactor y el cifrado de datos debe llevarse a cabo si las comunicaciones contienen información moderado o alto impacto Verificar que al implementar una red inalámbrica, controles de seguridad, como el cifrado de datos, se debe emplear si el tráfico de comunicaciones contiene información moderado o alto impacto Examinar que los routers inalámbricos proporcionen autenticación de contraseña y cifrado de transmisión	

				como características estándar Probar que si se opta por implementar la conectividad remota, los requisitos de seguridad y las directrices deben ser implementados. Esto incluye la verificación de la identidad de un usuario a través de la autenticación electrónica Verificar que se consideren las siguientes soluciones de contingencia para garantizar la disponibilidad de la WAN: 1) Enlaces de comunicaciones redundantes 2) Redundantes proveedores de servicios de red 3) Redundantes dispositivos de conexión de red 4) Redundancia de proveedor de servicios de Internet	
Comunicación	Desarrollar Consideraciones de contingencia de los servidores		Análisis del impacto del negocio Política de seguridad de la red Controles de seguridad del sistema	Verificar que las siguientes medidas se tomen en cuenta al determinar los requisitos centrales de contingencia de los servidores: 1) medios de copia de seguridad fuera del lugar laboral 2) Configuraciones del sistema de documentos y proveedores 3) Coordinar con la política de seguridad de la red y los controles de seguridad del sistema 4) Utilizar los resultados del análisis del impacto del negocio	