NOTA IMPORTANTE:

ININ/ Oficina Nacional de Normalización

NORMA CUBANA

NC

ISO/IEC 20000-1: 2010
(Publicada por la ISO en 2005)

TECNOLOGÍA DE LA INFORMACIÓN — GESTIÓN DEL SERVICIO — PARTE 1: ESPECIFICACIONES (ISO/IEC 20000-1: 2005, IDT)

Information technology — Service management — Part 1: Specification

ICS: 03.080.99; 35.020

1. Edición Marzo 2010

Oficina Nacional de Normalización (NC) Calle E No. 261 Vedado, Ciudad de La Habana. Cuba. Teléfono: 830-0835 Fax: (537) 836-8048; Correo electrónico: nc@ncnorma.cu; Sitio Web: www.nc.cubaindustria.cu

Cuban National Bureau of Standards

Prefacio

La Oficina Nacional de Normalización (NC), es el Organismo Nacional de Normalización de la República de Cuba y representa al país ante las organizaciones internacionales y regionales de normalización.

La elaboración de las Normas Cubanas y otros documentos normativos relacionados se realiza generalmente a través de los Comités Técnicos de Normalización. Su aprobación es competencia de la Oficina Nacional de Normalización y se basa en las evidencias del consenso.

Esta Norma Cubana:

- Ha sido elaborada por el Comité Técnico de Normalización NC/CTN 18 de Tecnología de la Información, integrado por representantes de las siguientes entidades:

  - Ministerio de la Informática y las Comunicaciones
  - Instituto de Investigaciones en Normalización
  - Instituto Superior Politécnico José A. Echeverría
  - Universidad de las Ciencias Informáticas
  - Universidad de Villa Clara
  - Ministerio de Ciencia Tecnología y Medio Ambiente (CITMATEL y CUBAENERGIA)
  - Ministerio de Salud Pública (Centro de Control Estatal de Equipos Médicos, Centro de Diseño de Sistemas, Centro de Computación Aplicada a la Medicina)
  - Oficina de Seguridad de las Redes Informáticas
  - SEGURMATICA
  - Oficina Nacional de Normalización

- Es una adopción idéntica por el método de traducción de la Norma Internacional ISO/IEC *20000-1:2005 Information technology. Service management. Part 1: Specification.*

- Incorpora a la norma adoptada el Anexo A, que contiene conceptos metodológicos ampliamente adoptados, en cuanto a la provisión de los servicios a los clientes internos, a fin de su empleo a modo de información complementaria para la implantación de la norma en las entidades, propiciando el control, inspección y auditoría a las mismas.

Oficina Nacional de Normalización (NC)
Calle E No. 261, Vedado, Ciudad de La Habana, Habana 4, Cuba.

Impreso en Cuba.

Índice

Página

PRÓLOGO DE LA NORMA INTERNACIONAL

ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización a nivel mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de normas internacionales a través de comités técnicos establecidos por las organizaciones respectivas para realizar acuerdos en los campos específicos de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, públicas y privadas, en coordinación con ISO e IEC, también participan en el trabajo. En el campo de tecnologías de la información, ISO e IEC han establecido un comité técnico conjunto, el denominado ISO/IEC JTC 1

Las normas internacionales se redactan de acuerdo con las reglas establecidas en la Parte 2 de las Directivas ISO/IEC.

La tarea principal de los comités técnicos es preparar normas internacionales. Los proyectos de normas internacionales adoptados por los comités técnicos se envían a los organismos miembros para su votación. La publicación como norma internacional requiere la aprobación por al menos el 75% de los organismos miembros con derecho a voto.

Se llama la atención sobre la posibilidad de que algunos de los elementos de esta norma internacional puedan estar sujetos a derechos de patente. ISO e IEC no asumen la responsabilidad por la identificación de cualquiera o todos los derechos de patente.

La Norma Internacional ISO/IEC 20000-1 fue elaborada por el British Standards Institution (como BS 15000-1) y fue adoptada por el procedimiento especial de "fast-track", por el Comité Técnico Conjunto ISO/IEC JTC 1, Tecnologías de la Información, en paralelo con la aprobación de los organismos nacionales miembros de ISO e IEC.

A nivel nacional el comité espejo de éste es el CTN 18 Tecnologías de la Información y que ha sido el encargado de elaborar esta Norma NC ISO/IEC 20000-1:2009 que es idéntica a la Norma Internacional ISO/IEC 20000-1:2005.

ISO/IEC 20000 está formada de dos partes bajo el mismo título de Tecnologías de la Información. Gestión del servicio:

Parte 1: Especificaciones

Parte 2: Código de buenas prácticas

INTRODUCCIÓN

- Esta parte de la Norma ISO/IEC 20000 promueve la adopción de un enfoque de procesos integrados, para una provisión eficaz de servicios gestionados que satisfaga los requisitos del negocio y de los clientes. Para que una organización funcione de forma eficiente debe identificar y gestionar numerosas actividades relacionadas entre sí. Se puede considerar que un proceso es una actividad que usa recursos y que es gestionada de manera que permite la transformación de entradas en salidas. A menudo las salidas de un proceso conforman las entradas de otro.

- La integración e implantación coordinada de los procesos de gestión del servicio proporcionan el control continuo, una mayor eficacia y mayores oportunidades para la mejora continua. La ejecución de las actividades y procesos requieren una buena organización y coordinación entre los grupos de soporte y operación del servicio, provisión del servicio y el servicio de soporte al usuario. Asimismo, es necesario disponer de las herramientas adecuadas para asegurar la efectividad y la eficiencia de los procesos.

- Se asume que la ejecución de las estipulaciones de esta norma ISO/IEC 20000 ha de ser encargada a personas competentes y debidamente cualificadas para esta tarea.

- Una norma internacional no pretende describir todas las provisiones necesarias de un contrato. Los usuarios de normas internacionales son responsables de su correcta aplicación.

- La conformidad con una norma internacional, no otorga por sí misma ninguna clase de inmunidad frente a las obligaciones legales.

TECNOLOGÍA DE LA INFORMACIÓN — GESTIÓN DEL SERVICIO — PARTE 1: ESPECIFICACIONES

1 OBJETO Y CAMPO DE APLICACIÓN

Esta parte de la Norma ISO/IEC 20000 define los requisitos para que un proveedor del servicio proporcione servicios gestionados de una aceptable calidad a sus clientes. Puede ser usada:

- por negocios que están yendo a ofertar sus servicios;

NOTA 1 El término "negocio" en esta norma internacional debería interpretarse en un sentido amplio, abarcando aquellas actividades que son esenciales para alcanzar los fines que persigue la organización.

- por negocios que requieren de un enfoque consistente por parte de todos sus proveedores de servicio en la cadena de suministro;

- por proveedores del servicio para medir y comparar su gestión del servicio de TI;

- como base de una evaluación independiente;

- por una organización que necesite demostrar su capacidad para proveer servicios que cumplan con los requisitos de los clientes; y

- por una organización que busque mejorar los servicios, mediante la aplicación efectiva de los procesos para monitorizar y mejorar la calidad de los servicios.

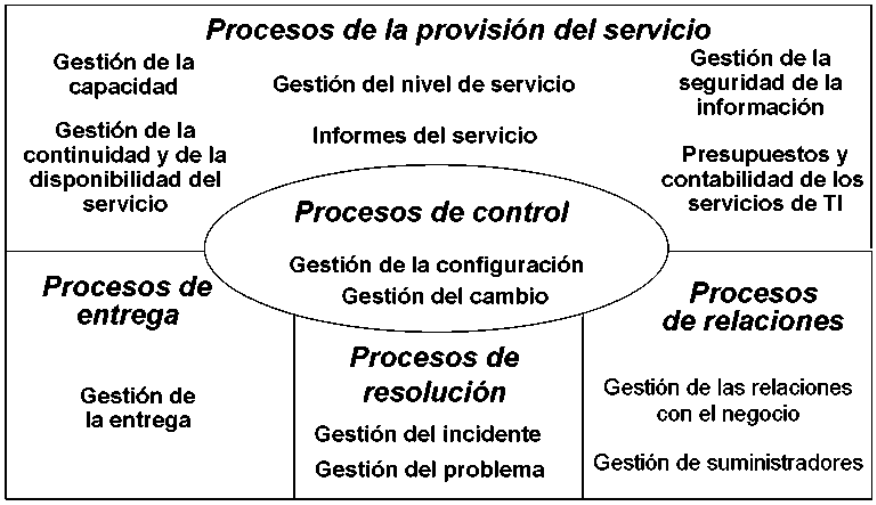

Figura 1 - Procesos de gestión del servicio

Esta parte de la Norma ISO/IEC 20000 especifica un conjunto de procesos de gestión del servicio que están estrechamente relacionados, tal como se muestra en la figura 1.

Las relaciones entre los procesos dependen de su aplicación dentro de una organización y, generalmente son demasiado complejas para modelarlas en un diagrama, por ello, no se muestran en éste.

La lista de objetivos y controles contenida en esta parte de la Norma ISO/IEC 20000 no es exhaustiva, y una organización puede considerar que son necesarios objetivos y controles adicionales para cumplir con sus necesidades particulares de negocio. La naturaleza de la relación de negocio, entre el proveedor del servicio y el negocio, determinará cómo se implementarán los requisitos en esta parte de la Norma ISO/IEC 20000, para cumplir el objetivo global.

Por ser una norma basada en procesos, esta parte de la Norma ISO/IEC 20000 no pretende servir para una evaluación de producto. Sin embargo, aquellas organizaciones que desarrollen herramientas, productos y sistemas de gestión del servicio, pueden usar ambas partes, esta parte de la Norma ISO/IEC 20000 y el código de práctica como ayuda para desarrollar herramientas, productos y sistemas que soporten las mejores prácticas de la gestión del servicio.

2 TÉRMINOS Y DEFINICIONES

Para los fines de este documento, son de aplicación los siguientes términos y definiciones:

2.1 disponibilidad *(availability)*:
Capacidad de un componente o un servicio para realizar la función requerida en un instante determinado o a lo largo de un período de tiempo determinado.

NOTA La disponibilidad se expresa normalmente como una relación entre el tiempo en que el servicio está disponible realmente para su uso por el negocio y el número de horas de servicio acordadas.

2.2 línea de referencia *(baseline)*:
La foto del estado de un servicio o un elemento de configuración individual en un momento dado (véase 2.4).

2.3 registro de cambio *(change record)*:
Registro que contiene los detalles de aquellos elementos de configuración (véase 2.4) que están afectados y como estos son afectados por un cambio autorizado.

2.4 elemento de configuración (CI) *[Configuration Item (CI)]*:
Un componente de una infraestructura o un elemento que está o estará bajo el control de la gestión de la configuración.

NOTA Los elementos de configuración pueden variar ampliamente en complejidad, tamaño y tipo, comprendiendo desde un sistema completo (incluyendo todo el hardware, el software y la documentación), hasta un módulo aislado o un componente de hardware menor.

2.5 base de datos de gestión de la configuración (CMDB) *[Configuration Management DataBase (CMDB)]*:
Base de datos que contiene todos los detalles relevantes de cada elemento de configuración y los detalles de las relaciones importantes entre ellos.

2.6 documento *(document)*:
Información y el medio que la contiene.

NOTA 1 En esta norma se diferencian los documentos de los registros de los documentos (véase 2.9) por el hecho de que los registros tienen como función proporcionar la evidencia de actividades, en lugar de la evidencia de intenciones.

NOTA 2 Ejemplos de documentos son: políticas, planes, procedimientos, acuerdos de nivel de servicio y contratos.

2.7 incidente *(incident)*:
Cualquier evento que no es parte del funcionamiento normal de un servicio y que causa, o puede causar, una interrup-ción de dicho servicio o una disminución de la calidad del mismo.

NOTA Esto puede incluir peticiones de consultas tales como llamadas de "¿cómo hago...?"

2.8 problema *(problem)*:
Causa subyacente desconocida de uno o más incidentes.

2.9 registro *(record)*:
Documento que establece los resultados alcanzados o que proporciona la evidencia de las actividades.

NOTA 1 En esta norma se diferencian los registros de los documentos por el hecho de que los registros tienen como función proporcionar la evidencia de actividades, en lugar de la evidencia de intenciones.

NOTA 2 Son ejemplos de registros los informes de auditoría, las solicitudes de cambio, los informes de incidentes, los registros de formación individual y las facturas enviadas a clientes.

2.10 entrega *(release)*:
Conjunto de elementos de configuración, nuevos o modificados, que están probados y se introducen de forma conjunta en el entorno real.

NOTA En el contexto de esta norma, el término *release* se ha traducido como entrega y difiere del utilizado en otras normas de ingeniería del software (liberación) ya publicadas por NC ISO.

2.11 solicitud de cambio *(request for change)*:
Formulario, en forma impresa o en pantalla, utilizado para registrar los detalles de una solicitud de un cambio en cual-quier elemento de configuración perteneciente a un servicio o a una infraestructura.

2.12 centro de servicio al usuario *(service desk)*:
Grupo de soporte de cara al cliente o al usuario que realiza una alta proporción del total del trabajo de soporte.

2.13 acuerdo del nivel de servicio (SLA) *[Service Level Agreement (SLA)]*:
Acuerdo escrito entre un proveedor del servicio y un cliente en el que se documentan los servicios y los niveles de servicio acordados.

2.14 gestión del servicio *(service management)*:
Gestión de los servicios para cumplir con los requisitos del negocio.

2.15 proveedor del servicio *(service provider)*:
La organización que quiere cumplir con la Norma ISO/IEC 20000.

NOTA En este contexto el proveedor del servicio puede pertenecer tanto a la propia organización cliente, como ser una organización externa.

3 REQUISITOS DE UN SISTEMA DE GESTIÓN

Objetivo: Proveer un sistema de gestión que incluye las políticas y el marco de trabajo para hacer posible una efectiva gestión e implementación de todos los servicios de TI.

3.1 Responsabilidad de la dirección

La alta dirección debe proveer, a través del liderazgo y de acciones, evidencias de su compromiso para desarrollar, implementar y mejorar sus capacidades de gestión del servicio dentro del contexto de los requisitos de negocio de la organización y de los requisitos de los clientes.

La dirección debe:

a) establecer la política de la gestión del servicio, sus objetivos y planes;

b) comunicar la importancia de cumplir con los objetivos de gestión del servicio y la necesidad de la mejora continua;

c) asegurar que los requisitos del cliente se determinan y se cumplen con el objetivo de mejorar la satisfacción del cliente;

d) designar un miembro de la dirección como responsable para la coordinación y gestión de todos los servicios;

e) determinar y proveer recursos para planificar, implementar, monitorizar, revisar y mejorar la provisión y la gestión de los servicios, por ejemplo, contratando el personal apropiado o gestionando la rotación de personal;

f) gestionar los riesgos para la organización de la gestión del servicio y para los servicios; y

g) llevar a cabo revisiones de la gestión del servicio, a intervalos planificados, para asegurar la continuidad de su idoneidad, su adecuación y su efectividad.

3.2 Requisitos de la documentación

Los proveedores del servicio deben facilitar documentos y registros para asegurar una planificación, operación y control de la gestión del servicio efectiva. Esto debe incluir:

a) políticas y planes de la gestión del servicio documentados;

b) acuerdos del nivel de servicio documentados

c) procesos y procedimientos documentados requeridos por esta norma; y

d) registros requeridos por esta norma.

Deben establecerse los procedimientos y las responsabilidades para la creación, revisión, aprobación, mantenimiento, eliminación y control de los diferentes tipos de documentos y registros.

NOTA La documentación puede estar en cualquier forma o tipo de soporte.

3.3 Competencia, concienciación y formación

Se deben definir y mantener todos los roles y responsabilidades de la gestión del servicio, junto con las competencias que sean requeridas para su ejecución efectiva.

Las competencias y necesidades de formación del personal deben revisarse y gestionarse para permitir al personal llevar a cabo sus roles de forma efectiva.

La alta dirección debe asegurar que sus empleados son conscientes de la relevancia e importancia de sus actividades y de cómo deben contribuir a la consecución de los objetivos de la gestión del servicio.

4 PLANIFICACIÓN E IMPLEMENTACIÓN DE LA GESTIÓN DEL SERVICIO

NOTA La metodología conocida como Planificar-Hacer-Verificar-Actuar (PDCA, del inglés *Plan-Do-Check-Act*) puede aplicarse a todos los procesos. La metodología PDCA puede describirse del modo siguiente:

a) Planificar: Establecer los objetivos y los procesos necesarios para proporcionar resultados de acuerdo con las necesidades del cliente y con las políticas de la empresa.

b) Hacer: Implementar los procesos.

c) Verificar: Monitorizar y medir los procesos y los servicios contrastándolos con las políticas, los objetivos y los requisitos, e informar sobre los resultados.

d) Actuar: Emprender las acciones necesarias para mejorar continuamente el rendimiento y comportamiento del proceso.

El modelo que se muestra en la figura 2 ilustra el proceso y las relaciones de los procesos presentados en los capítulos 4 a 10.

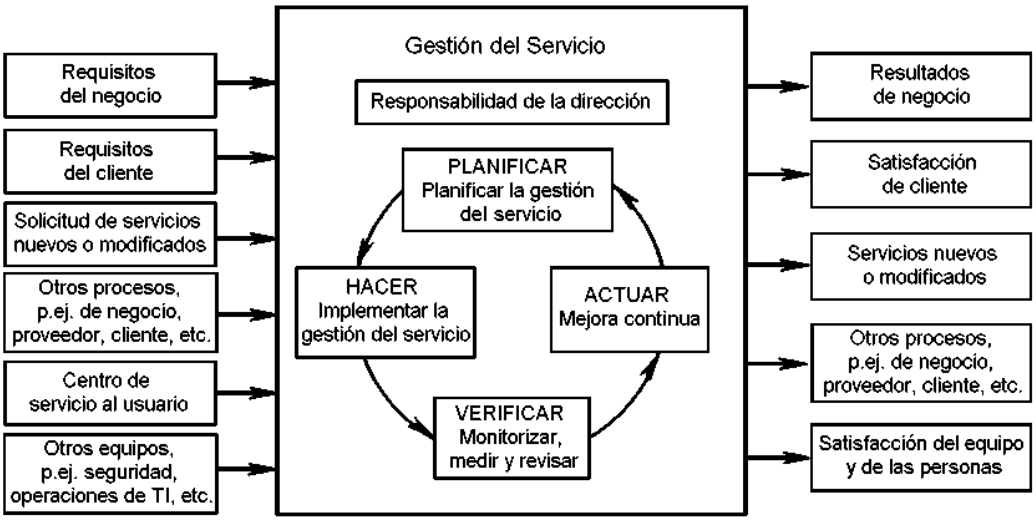

Figura 2 - La metodología PDCA-Planificar-Hacer-Verificar-Actuar para los procesos de gestión del servicio

Objetivo: Planificar la implementación y la provisión de la gestión del servicio.

Se debe planificar la gestión del servicio. Como mínimo, el plan debe definir lo siguiente:

a) el alcance de la gestión del servicio del proveedor del servicio;

b) los objetivos y los requisitos que se tienen que alcanzar por la gestión del servicio;

c) los procesos que se van a ejecutar;

d) el marco de los roles y responsabilidades de la dirección, incluyendo al directivo de alto nivel responsable directo, al propietario del proceso y a la dirección de la gestión la dirección de los suministradores;

e) las interfases entre los procesos de gestión del servicio y el modo en que tienen que coordinarse las actividades;

f) el enfoque que hay que dar a la identificación, la evaluación y la gestión de actividades y de los riesgos para la consecución de los objetivos definidos;

g) el enfoque para la relación con proyectos que estén creando o modificando los servicios;

h) los recursos, el equipamiento y los presupuestos necesarios para alcanzar los objetivos definidos;

i) las herramientas adecuadas para dar soporte a los procesos; y

j) cómo se va gestionar, auditar y mejorar la calidad del servicio.

Deben estar claramente definidas tanto la orientación de la gestión como las responsabilidades documentadas para revisar, autorizar, comunicar, implementar y mantener los planes. Cualquier plan específico de un proceso que se elabore debe ser compatible con este plan de gestión del servicio.

4.2 Implementación de la gestión del servicio y provisión de los servicios (hacer)

Objetivo: Implementar los objetivos y el plan de gestión del servicio.

El proveedor del servicio debe implementar el plan de gestión del servicio para proveer y gestionar los servicios, incluyendo:

a) la asignación de presupuestos y fondos;

b) la asignación de roles y responsabilidades;

c) la documentación y el mantenimiento de políticas, planes, procedimientos y definiciones para cada proceso o conjunto de procesos;

d) la identificación y la gestión de riesgos para el servicio;

e) la gestión de los equipos de trabajo, por ejemplo, la contratación y el desarrollo del personal adecuado y la gestión de continuidad del personal;

f) la gestión del equipamiento y el presupuesto;

g) la gestión de los equipos o grupos de personas, incluidos los del centro de servicio al usuario y los de operaciones;

h) informar del progreso en comparación con los planes; y

i) la coordinación de los procesos de gestión del servicio.

4.3 Monitorear, medir y revisar (verificar)

Objetivo: Monitorear, medir y revisar que los objetivos y el plan de gestión del servicio se están cumpliendo.

El proveedor del servicio debe aplicar métodos adecuados para monitorear y, cuando sea necesario, realizar la medición de los procesos de gestión del servicio. Estos métodos deben demostrar la capacidad de los procesos para alcanzar los resultados planificados. La dirección debe realizar revisiones a intervalos planificados para determinar si los requisitos de gestión del servicio:

a) son conformes con el plan de gestión del servicio y los requisitos de esta norma, y

b) se implementan y se mantienen de manera eficaz.

Se debe planificar un programa de auditorías, teniendo en cuenta el estado y la importancia de los procesos y las áreas a auditar, así como, los resultados de las auditorías anteriores. Se deben definir en un procedimiento los criterios, el alcance, la frecuencia y los métodos de la auditoría. La selección de los auditores y la realización de las auditorías deben garantizar la objetividad y la imparcialidad del proceso de auditoría. Los auditores no deben auditar su propio trabajo.

El objetivo de las revisiones, evaluaciones y auditorías de la gestión del servicio se debe registrar junto con las conclusiones de dichas auditorías, sus revisiones y las acciones correctivas que se hayan identificado. Se debe comunicar a las partes correspondientes la existencia de cualquier área significativa con alguna no conformidad u otra discrepancia.

4.4 Mejora continua (actuar)

Objetivo: Mejorar la eficacia y la eficiencia de la entrega y de la gestión del servicio.

4.4.1 Política

Debe haber una política publicada sobre la mejora del servicio. Se debe corregir cualquier no conformidad con la norma o con los planes de gestión del servicio. Se deben definir claramente los roles y las responsabilidades para las actividades de mejora del servicio.

4.4.2 Gestión de las mejoras del servicio

Se deben evaluar, registrar, priorizar y autorizar todas las propuestas de mejora del servicio. Se debe utilizar un plan para controlar la actividad.

El proveedor del servicio debe disponer de un proceso para identificar, medir y gestionar las actividades de mejora e informar de dichas actividades de manera continua. Este proceso debe incluir:

a) las mejoras de un proceso aislado que el propietario del proceso pueda implementar con los recursos de personal habituales, por ejemplo, la realización de acciones correctivas y preventivas; y

b) las mejoras en toda la organización o en más de un proceso.

4.4.3 Actividades

El proveedor del servicio debe realizar actividades para:

a) recopilar y analizar los datos para delimitar y medir la capacidad del proveedor del servicio para gestionar y proveer el servicio junto con los procesos de gestión del mismo;

b) identificar, planificar e implementar mejoras;

c) consultar a todas las partes implicadas;

c) establecer objetivos de mejora en cuanto a la calidad, los costes y la utilización de recursos;

d) tener en cuenta las aportaciones importantes, referentes a mejoras, que se realicen desde todos los procesos de gestión del servicio;

e) medir, informar y comunicar las mejoras en el servicio;

g) revisar las políticas, los planes y los procedimientos de gestión del servicio, siempre que sea necesario; y

h) asegurar que todas las acciones aprobadas se llevan a cabo y que se alcanzan los objetivos deseados.

5 PLANIFICACIÓN E IMPLEMENTACIÓN DE NUEVOS SERVICIOS O DE SERVICIOS MODIFICADOS

Objetivo: Asegurar que, tanto los servicios nuevos, como las modificaciones a los existentes, se pueden gestionar y proveer con los costes y la calidad acordados.

En las propuestas de nuevos servicios o modificaciones en los existentes, se deben considerar los costes y el impacto a nivel organizativo, técnico y comercial que pudiera derivar de su entrega y gestión.

La implementación de nuevos servicios o modificaciones en los existentes, incluyendo la eliminación de un servicio, debe ser planificada y aprobada a través de un proceso formal de gestión del cambio.

La planificación e implementación deben incluir los fondos y recursos adecuados para llevar a cabo los cambios necesarios para la provisión y la gestión del servicio.

Los planes deben incluir:

a) los roles y responsabilidades para implementar, operar y mantener los nuevos servicios o modificaciones en los existentes, incluyendo las actividades a llevar a cabo por clientes y suministradores;

b) los cambios en el marco de trabajo existente de gestión del servicio y en los propios servicios;

c) la comunicación a las partes afectadas;

d) los nuevos contratos y acuerdos, o modificaciones a los contratos y acuerdos existentes, para estar alineados con las necesidades del negocio;

e) los requisitos de mano de obra y contratación;

f) los requisitos de perfiles y formación, por ejemplo usuarios, soporte técnico;

g) los procesos, medidas, métodos y herramientas que han de usarse con relación a los nuevos servicios o modificaciones en los existentes, por ejemplo gestión de la capacidad, gestión financiera;

h) los presupuestos y plazos de tiempo

i) los criterios de aceptación del servicio; y

j) los resultados esperados al operar con el nuevo servicio, expresados en términos medibles.

Los nuevos servicios, o las modificaciones en los existentes, deben ser aceptados por el proveedor del servicio antes de ser implementados en el entorno de producción real.Tras la implementación, el proveedor del servicio debe informar de los resultados alcanzados por el servicio nuevo, o por el servicio modificado, comparándolos con los resultados previstos. Se debe realizar una revisión posterior a la implementación, que compare los resultados reales con los planificados a través del proceso de gestión del cambio.

6 PROCESOS DE LA PROVISIÓN DEL SERVICIO

6.1 Gestión de nivel de servicio

Objetivo: Definir, acordar, registrar y gestionar los niveles de servicio.

Se deben acordar por las partes, y registrar, el conjunto total de los servicios a ser provistos, junto a los correspondientes objetivos de nivel de servicio y las características de la carga de trabajo que deben soportar.

Cada servicio ofrecido se debe definir, acordar y documentar en uno o más acuerdos de nivel de servicio (SLAs).

Se deben acordar y registrar por todas las partes relevantes los SLAs, junto con los acuerdos de servicios de soporte, los contratos con suministradores y los correspondientes procedimientos.

Los SLAs deben estar bajo el control de la gestión del cambio.

Los SLAs se deben revisar periódicamente por las partes, para asegurar que se encuentran actualizados y continúan siendo eficaces con el transcurso del tiempo.

Los niveles de servicio se deben monitorear y se deben generar informes de dichos niveles con relación a los objetivos, mostrando tanto la información actual como las tendencias. Las razones para las no-

conformidades se deben comunicar y revisar. Las acciones de mejora definidas durante este proceso se deben registrar y constituyen una entrada al plan de mejora del servicio.

6.2 Generación de informes del servicio

Objetivo: Generar en plazo los informes acordados, fiables y precisos, para informar de la toma de decisiones y para una comunicación eficaz.

Se debe describir claramente cada informe de servicio, incluyendo su identificador, el propósito, la audiencia y los detalles del origen de los datos.

Los informes de servicio se deben generar para verificar si se cumplen los requisitos y necesidades de los usuarios. Los informes de servicio deben incluir:

a) el rendimiento y comportamiento frente a los objetivos de nivel de servicio;

b) las no-conformidades y problemas relacionados, por ejemplo con los SLAs o agujeros de seguridad;

c) las características de la carga de trabajo, por ejemplo volumen o utilización de recursos;

d) los informes de los resultados de los principales eventos, por ejemplo los principales incidentes y cambios;

e) la información sobre tendencias;

f) el análisis de satisfacción.

g) Las decisiones de gestión y las acciones correctivas deben tener en cuenta los aspectos destacados en los informes de servicio y deben comunicarse a las partes afectadas.

6.3 Gestión de la continuidad y disponibilidad del servicio

Objetivo: Asegurar que los compromisos de continuidad y disponibilidad acordados con los clientes pueden cumplirse bajo todas las circunstancias.

Se deben identificar los requisitos de disponibilidad y de continuidad del servicio sobre la base de los planes de negocio, los SLAs y las evaluaciones del riesgo. Los requisitos deben incluir los derechos de acceso y los tiempos de respuesta, así como, la disponibilidad extremo a extremo de los componentes del sistema.

Los planes de disponibilidad y continuidad del servicio se deben desarrollar y revisar al menos una vez al año, para asegurar que los requisitos cumplen lo acordado bajo todas las circunstancias, desde la normalidad hasta la pérdida grave del servicio. Estos planes se deben mantener para asegurar que reflejan los cambios acordados, requeridos por el negocio.

Los planes de disponibilidad y de continuidad del servicio se deben probar de nuevo cuando se produzca un cambio importante en el entorno del negocio.

El proceso de gestión del cambio debe evaluar el impacto de cualquier cambio sobre los planes de disponibilidad y de continuidad del servicio.

La disponibilidad se debe medir y registrar. Se debe investigar la no-disponibilidad no planeada y se deben llevar a cabo las acciones necesarias.

NOTA Cuando sea posible, se deben predecir problemas potenciales y tomar medidas preventivas.

Los planes de continuidad del servicio, la lista de contactos y la base de datos de gestión de la configuración deben estar disponibles incluso en el caso de que no sea posible el acceso normal a las oficinas. El plan de continuidad del servicio debe incluir la actividad de vuelta a la normalidad.

El plan de continuidad del servicio debe probarse de acuerdo a las necesidades del negocio.

Todas las pruebas de continuidad se deben registrar y tras las pruebas fallidas se deben elaborar planes de acción.

6.4 Elaboración del presupuesto y contabilidad de los servicios de TI

Objetivo: Presupuestar y contabilizar los costes de la provisión del servicio.

NOTA Esta sección cubre la elaboración de presupuestos y de la contabilidad del los servicios de TI. En la práctica, muchos proveedores del servicio estarán involucrados en facturar por tales servicios. Sin embargo, dado que la facturación es una actividad opcional, no está cubierta por la norma. Se recomienda a los proveedores que si hacen uso de la facturación, el mecanismo para hacerlo esté plenamente definido y entendido por las partes. Todas las prácticas contables en uso se deberían alinear con las prácticas contables más amplias de la organización del proveedor del servicio.

Debe haber políticas y procedimientos claros para:

a) presupuestar y contabilizar todos los componentes, incluyendo los activos de tecnologías de la información, recursos compartidos, gastos generales, servicios suministrados externamente, personas, seguros y licencias;

b) la repercusión de costes indirectos y la asignación de costes directos a servicios;

c) el control económico efectivo y la autorización.

Los costes se deben presupuestar con suficiente detalle para permitir el control económico efectivo y la toma de decisiones.

El proveedor del servicio debe monitorizar e informar de los costes contra el presupuesto, revisar las previsiones económicas y gestionar los costes en consonancia.

Los costes de los cambios en el servicio se deben valorar y aprobar a través del proceso de gestión del cambio.

6.5 Gestión de la capacidad

Objetivo: Asegurar que el proveedor del servicio tiene, en todo momento, la capacidad suficiente para cubrir la demanda acordada, actual y futura, de las necesidades del negocio del cliente.

La gestión de la capacidad debe elaborar y mantener un plan de capacidad.

La gestión de la capacidad debe estar dirigida a las necesidades del negocio y debe incluir:

a) los requisitos de capacidad, rendimiento y comportamiento, actuales y previstos;

b) la identificación de plazos, umbrales y costes para las actualizaciones del servicio;

c) la evaluación de los efectos sobre la capacidad de actualizaciones anticipadas del servicio, peticiones de cambio, y nuevas tecnologías y técnicas;

d) la previsión del impacto de cambios externos, por ejemplo cambios legislativos;

e) los datos y los procesos para poder realizar análisis predictivos.

Se deben identificar métodos, procedimientos y técnicas para monitorear la capacidad del servicio, el ajuste del comportamiento y de las prestaciones del servicio y la provisión de la adecuada capacidad.

6.6 Gestión de la seguridad de la información

Objetivo: Gestionar la seguridad de la información de manera eficaz para todas las actividades del servicio.

NOTA ISO/IEC 27000 Tecnologías de la Información. Código de prácticas para la gestión de la seguridad de la información, proporciona una guía para la gestión de la seguridad de la información.

La dirección, con la autoridad apropiada, debe aprobar una política de seguridad de la información, que debe comunicarse a todo el personal implicado y, cuando sea adecuado, a los clientes.

Los adecuados controles de seguridad deben ayudar a:

a) implementar los requisitos de la política de seguridad de la información;

b) gestionar los riesgos asociados al acceso al servicio o a los sistemas.

Los controles de seguridad deben estar documentados. La documentación debe describir los riesgos a los que están asociados los controles, la manera de utilizarlos y el mantenimiento de los mismos.

El impacto de los cambios sobre los controles se debe evaluar antes de que los cambios sean implementados.

Los servicios que impliquen el acceso de organizaciones externas a los sistemas de información y a los servicios, deben estar basados en un acuerdo formal que defina todos los requisitos de seguridad necesarios.

Los incidentes de seguridad se deben comunicar y registrar tan pronto como sea posible de acuerdo a los procedimientos de gestión del incidente. Se deben poner en marcha procedimientos para asegurar que todos los incidentes de seguridad son investigados, y que se toman medidas al respecto.

Se deben poner en marcha mecanismos para poder cuantificar y monitorear los tipos, volúmenes e impacto de los incidentes y el mal funcionamiento de la seguridad. Las acciones de mejora identificadas durante este proceso se deben registrar y servir como información de entrada al plan de mejora del servicio.

7 PROCESOS DE RELACIONES

7.1 Generalidades

Los procesos de relación describen los dos aspectos relacionados con la gestión de suministradores y con la gestión de las relaciones con el negocio.

7.2 Gestión de las relaciones con el negocio

Objetivo: Establecer y mantener una buena relación entre el proveedor del servicio y el cliente, basándose en el entendimiento del cliente y de los fundamentos de su negocio.

El proveedor del servicio debe identificar y documentar quienes son los actores principales y los clientes de los servicios.

El proveedor del servicio y los clientes se deben reunir, al menos una vez al año, para la revisión del servicio y para discutir cualquier cambio en el alcance del mismo, en el SLA, en el contrato (si existe) o en las necesidades del negocio. Se deben mantener reuniones a intervalos acordados para discutir el comportamiento y las prestaciones, los cumplimientos, asuntos varios y planes de acción. Estas reuniones se deben documentar.

A las reuniones puede invitarse a otros actores relacionados con el servicio.

Los cambios al contrato(s), si existen, y al SLA(s) deben ser el resultado de las reuniones mencionadas, cuando sea apropiado. Estos cambios deben estar sujetos al proceso de gestión del cambio.

El proveedor del servicio debe permanecer al tanto de las necesidades del negocio y de los principales cambios en el mismo para preparar una respuesta a dichas necesidades.

Debe existir un proceso de reclamaciones. La definición de la reclamación formal sobre el servicio debe estar acordada con el cliente. Todas las reclamaciones formales sobre el servicio son registradas por el proveedor del servicio, investigadas, controladas emprendiendo acciones sobre ellas, informadas y formalmente cerradas. Cuando una reclamación no sea resuelta mediante los canales normales, el cliente debe disponer de un mecanismo de escalado.

El proveedor del servicio debe tener una o varias personas asignadas como responsable(s) de gestionar la satisfacción del cliente y todo el proceso de gestión de relaciones con el negocio. Debe existir un proceso de medición periódica de la satisfacción del cliente para obtener información y comentarios, y actuar en consecuencia. Las acciones de mejora que se identifiquen durante este proceso se deben registrar y utilizar como información de entrada para un plan de mejora del servicio.

7.3 Gestión de suministradores

Objetivo: Gestionar los suministradores para garantizar la provisión sin interrupciones de servicios de calidad.

NOTA 1 El ámbito de esta norma excluye la selección de suministradores.

NOTA 2 Los suministradores pueden ser utilizados por el proveedor del servicio para el suministro de alguna parte del servicio. Es el proveedor del servicio quien debe demostrar el cumplimiento de estos procesos de gestión de suministradores. Pueden existir relaciones complejas, como demuestra el siguiente diagrama utilizado a modo de ejemplo:

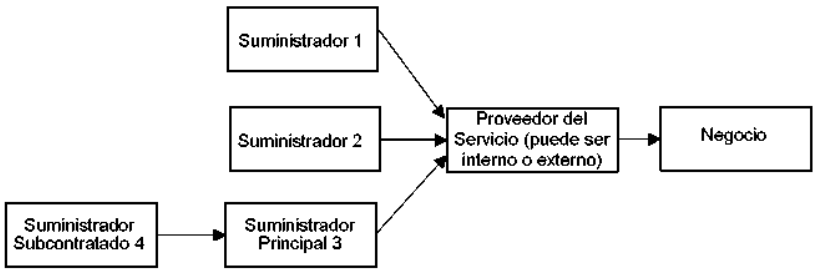

Figura 3 - Ejemplo de relaciones entre el proveedor del servicio y los suministradores

El proveedor del servicio debe tener documentados los procesos de gestión de suministradores y debe designar un gestor responsable del contacto con cada suministrador.

Los requisitos, alcance, nivel de servicio y procesos de comunicación a ser proporcionados por el suministrador(es) se deben acordar por todas las partes y documentar en los SLA(s) u otros documentos.

Los SLAs con los suministradores se deben alinear con los SLAs con el negocio.

Las interfases entre los procesos utilizados por cada parte deben ser acordadas y documentadas.

Todos los roles y relaciones entre suministradores principales y subcontratados deben estar claramente documentados. Los suministradores principales deben ser capaces de demostrar que tienen procesos para garantizar que los subcontratistas cumplen con los requisitos contractuales.

Se debe disponer de un proceso para la revisión detallada del contrato o del acuerdo formal, con periodicidad mínima anual, que garantice que las necesidades y obligaciones contractuales del negocio se siguen cumpliendo.

Los cambios al contrato(s), si existen, y los SLAs deben ser el resultado de estas revisiones o de aquellas requeridas en cualquier otro momento. Cualquier cambio debe estar sujeto al proceso de gestión del cambio.
Debe existir un proceso para tratar los desacuerdos contractuales.

Debe existir un proceso para gestionar la finalización normal o anticipada de un servicio, o la transferencia del mismo a un tercero.

Se debe monitorear y revisar el comportamiento y las prestaciones frente a los objetivos de nivel de servicio. Las acciones de mejora identificadas durante este proceso se deben registrar y utilizar como información de entrada al plan de mejora del servicio.

8 PROCESOS DE RESOLUCIÓN

8.1 Antecedentes

La gestión del incidente y la gestión del problema son procesos separados, aunque ambos están fuertemente relacionados.

Se deben registrar todos los incidentes.

Se deben adoptar procedimientos para gestionar el impacto de los incidentes.

Los procedimientos deben definir el registro, la priorización, el impacto en el negocio, la clasificación, la actualización, el escalado, la resolución y el cierre formal de todos los incidentes.

Se debe mantener informado al cliente del progreso del incidente sobre el que haya informado o de su solicitud de servicio, y se le debe alertar por adelantado sobre si sus niveles de servicio no se pueden satisfacer, acordando con él las acciones a tomar.

Todo el personal implicado en la gestión del incidente debe tener acceso a información relevante como, por ejemplo errores conocidos, resoluciones de problemas y la base de datos de gestión de la configuración.

Los incidentes graves se deben clasificar y gestionar de acuerdo con un proceso.

8.3 Gestión del problema

Objetivo: Minimizar los efectos negativos sobre el negocio de interrupciones del servicio, mediante la identificación y el análisis proactivos de la causa de los incidentes y la gestión de los problemas para su cierre.

Se deben registrar todos los problemas identificados.

Se deben adoptar procedimientos para identificar, minimizar y evitar el impacto de los incidentes y de los problemas. Estos procedimientos deben definir el registro, la clasificación, la actualización, el escalado, la resolución y el cierre de todos los problemas.

Se deben llevar a cabo acciones preventivas para reducir los problemas potenciales, por ejemplo las derivadas de análisis de tendencias de volúmenes y tipos de incidentes.

Se deben remitir al proceso de gestión del cambio los cambios necesarios para corregir la causa subyacente de problemas.

Para que resulte eficaz la resolución de problemas, se debe supervisar, revisar y elaborar informes sobre ella.

El equipo de gestión del problema debe ser responsable de garantizar que esté disponible, para la gestión de incidentes, la información actualizada sobre errores conocidos y problemas corregidos.

Las acciones de mejora identificadas durante este proceso se deben registrar e incluir en el plan de mejora del servicio.

9 PROCESOS DE CONTROL

9.1 Gestión de la configuración

Objetivo: Definir y controlar los componentes del servicio y de la infraestructura, y mantener información precisa sobre la configuración.

Debe existir una visión integrada para la planificación de la gestión del cambio y de la configuración.

El proveedor del servicio debe definir la interfaz con los procesos de contabilidad financiera de activos.

NOTA La contabilidad financiera de los activos queda fuera del ámbito de esta sección.

Debe existir una política que defina qué se considera como elemento de configuración y qué componentes lo constituyen.

Se debe definir la información que se debe registrar para cada elemento, y se deben incluir las relaciones y la documentación necesaria para la gestión efectiva del servicio.

La gestión de la configuración debe proporcionar los mecanismos para identificar, controlar y hacer el seguimiento de las versiones de los componentes identificables del servicio y de la infraestructura. Se debe asegurar que el grado de control es suficiente para cubrir las necesidades del negocio, los riesgos de fallo y la criticidad del servicio.

La gestión de la configuración debe proporcionar información al proceso de gestión del cambio sobre el impacto de un cambio solicitado sobre la configuración del servicio y de la infraestructura. Los cambios en los elementos de configuración deben ser fáciles de identificar y auditables cuando sea apropiado, por ejemplo para cambios y movimientos en el software y el hardware.

Los procedimientos de control de configuración deben asegurar que se mantiene la integridad de los sistemas, servicios y componentes de servicio.

Antes de un paso al entorno real, debe establecerse una línea de referencia de los elementos de configuración correspondientes.

Deben estar controladas, en una biblioteca física o electrónica segura, las copias maestras de los elementos de configuración digitales, con referencias a los registros de configuración, por ejemplo software, productos de prueba, documentos de soporte.

Todos los elementos de configuración deben ser identificables, de manera única, y registrados en la base de datos de gestión de la configuración, cuyo acceso para actualizaciones se debe controlar de manera estricta. La base de datos de gestión de la configuración se debe gestionar y verificar activamente para asegurar su fiabilidad y precisión. El estado de los elementos de configuración, sus versiones, ubicación, cambios y problemas relacionados, así como la documentación asociada deben estar visibles para quienes lo requieran.

Los procedimientos de auditoría de la configuración deben incluir el registro de deficiencias, el lanzamiento de acciones correctivas y la comunicación de su resultado.

9.2 Gestión del cambio

Objetivo: Asegurar que todos los cambios son evaluados, aprobados, implementados y revisados de una manera controlada.

Los cambios en los servicios y la infraestructura deben tener un alcance claramente definido y documentado.

Todas las peticiones de cambio se deben registrar y clasificar, por ejemplo en urgentes, de emergencia, importantes, menores. Se debe evaluar el riesgo, el impacto y los beneficios para el negocio de las peticiones de cambio.

El proceso de gestión del cambio debe incluir la forma en que puede darse marcha atrás o corregir cada cambio si no se realiza con éxito.

Los cambios se deben aprobar y tras ello deben ser comprobados, y deben ser implementados de una forma controlada.

Se debe revisar el éxito de todos los cambios y, en caso contrario, se deben decidir y llevarse a cabo acciones correctivas tras la implementación.

Deben existir políticas y procedimientos para controlar la autorización e implementación de cambios de emergencia.

Las fechas planificadas para la implementación de los cambios se deben utilizar como base para la planificación de cambios y entregas. Se debe mantener y comunicar a las partes correspondientes la planificación que contenga los detalles de todos los cambios aprobados para su implementación y las fechas propuestas.

Los registros de cambios se deben analizar regularmente para detectar incrementos en el volumen de cambios, tipos recurrentes frecuentemente, tenencias emergentes y cualquier otra información relevante. Los resultados y conclusiones obtenidos a partir del análisis de los cambios se deben registrar.

Las acciones de mejora identificadas para la gestión del cambio se deben registrar y debe proporcionar información de entrada al plan de mejora del servicio.

10 PROCESO DE ENTREGA

10.1 Proceso de gestión de la entrega

Objetivo: Entregar, distribuir y realizar el seguimiento de uno o más cambios en la entrega en el entorno de producción real.

NOTA El proceso de gestión de la entrega se debería integrar con los procesos de gestión de la configuración y de gestión del cambio.

Se debe documentar y acordar la política de entrega que establezca la frecuencia y el tipo de las entregas.

El proveedor del servicio debe planificar con el negocio la entrega de los servicios, sistemas, software y hardware. Los planes sobre cómo desplegar una entrega se deben acordar y autorizar por todas las partes pertinentes, por ejemplo clientes, usuarios, personal de operaciones y de soporte.

El proceso debe incluir la forma en que se dé marcha atrás o se corrija la entrega si no se realiza con éxito.

Los planes deben registrar los entregables y las fechas de la entrega, y hacer referencia a las peticiones de cambio, errores conocidos y problemas relacionados. El proceso de gestión de la entrega debe proporcionar la información adecuada al proceso de gestión del incidente.

Las peticiones de cambio se deben evaluar en cuanto a su impacto en los planes de entregas. Los procedimientos de gestión de la entrega deben incluir la actualización y el cambio de la información de configuración y los registros de cambio. Las entregas de emergencia se deben gestionar de acuerdo a un proceso definido que realice la interfaz con el proceso de gestión del cambio de emergencia.

Se debe establecer un entorno controlado de pruebas de aceptación para construir y probar todas las entregas previamente a su distribución.

Las entregas y su distribución se deben diseñar e implementar de forma que la integridad del hardware y del software se mantenga a lo largo de la instalación, la manipulación, el empaquetado y la provisión.

Se debe medir el éxito y el fallo de las entregas. Las mediciones deben incluir los incidentes relacionados con una entrega en el periodo siguiente a su despliegue. Los análisis deben incluir la evaluación del impacto en el negocio y en el personal de operación y soporte de TI, y deben proporcionar información de entrada al plan para la mejora del servicio.

BIBLIOGRAFÍA

[I] ISO/IEC 20000-2 *Tecnología de la Información. Gestión del servicio. Parte 2: Código de buenas prácticas.*

[2] ISO/IEC 17799 *Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información.*

[3] ISO/IEC 12207 *Tecnología de la información. Procesos del ciclo de vida del software.*

[4] ISO/IEC TR 15271 *Tecnología de la información. Directrices para la aplicación de la Norma ISO/IEC 12207 (Procesos del ciclo de vida del software).*

[5] ISO/IEC TR 16326 *Ingeniería de sistemas. Directrices para la aplicación de la Norma ISO/IEC 12207 a la gestión de proyectos.*

[6] ISO/IEC 15288 *Ingeniería de sistemas. Procesos del sistema de ciclo de vida.*

[7] ISO/IEC TR 19760 *Ingeniería de sistemas. Guía para la aplicación de la Norma ISO/IEC 15288 (Procesos del sistema de ciclo de vida).*

[8] ISO/IEC 15504-1 *Tecnología de la información. Evaluación del proceso. Parte 1: Conceptos y vocabulario.*

[9] ISO/IEC 15504-2 *Tecnología de la información. Evaluación del proceso. Parte 2: Interpretación de la evaluación.*

[10] ISO/IEC 15504-3 *Tecnología de la información. Evaluación del proceso. Parte 3: Directrices para la interpretación de la evaluación.*

[11] ISO/IEC 15504-4 *Tecnología de la información. Evaluación del proceso. Parte 4: Guía de uso para la mejora del proceso y la determinación de la capacidad del proceso.*

[12] ISO/IEC 15504-5 *Tecnología de la información. Evaluación del proceso. Parte 5: Un modelo de evaluación del proceso.*

[13] ISO 10007 *Sistemas de gestión de la calidad. Directrices para la gestión de la configuración.*

[14] ISO 9000 *Sistemas de gestión de la calidad. Fundamentos y vocabulario.*

[15] ISO 9001 *Sistemas de gestión de la calidad. Requisitos.*

[16] ISO/IEC 90003 *Ingeniería del software. Guía de aplicación de la ISO 9001:2000 al software.*

ANEXO A

DIRECTIVAS GENERALES PARA LA PLANIFICACIÓN, IMPLANTACIÓN, MONITOREO Y PROVISION DE LOS SERVICIOS INTERNOS DE TECNOLOGÍAS DE LA INFORMACIÓN

1. PLANIFICACIÓN

1.1 DEFINICIÓN DE UN PLAN ESTRATÉGICO DE TECNOLOGÍA DE INFORMACIÓN

1.1.1 Tecnología de Información como parte del Plan de la Organización a corto y largo plazo.
La alta dirección será la responsable de desarrollar e implementar planes a largo y corto plazo que satisfagan la misión y las metas de la organización y deberá asegurar que los problemas de tecnología de información, así como las oportunidades, sean evaluados y reflejados adecuadamente en los planes a largo y corto plazo de la organización.

1.1.2 Plan a largo plazo de Tecnología de Información
El responsable para la coordinación y gestión de los servicios de TI será responsable de desarrollar regularmente planes a largo plazo de tecnología de información que apoyen el logro de la misión y las metas generales de la organización. De la misma manera, deberá implementar un proceso de planeación a largo plazo, adoptar un enfoque estructurado y determinar la estructura para el plan.

1.1.3 Plan a largo plazo de Tecnología de Información - Enfoque y Estructura
El responsable para la coordinación y gestión de los servicios de TI deberá establecer y aplicar un enfoque estructurado al proceso de planeación a largo plazo. Esto deberá traer como resultado un plan de alta calidad que cubra las preguntas básicas de qué, quién y cuándo. Los aspectos que necesitan ser tomados en cuenta y ser cubiertos adecuadamente durante el proceso de planeación son el modelo de organización y sus cambios, la distribución geográfica, la evolución tecnológica, los costos, los requisitos legales y regulatorios, requerimientos de terceras partes o del mercado, el horizonte de planeación, reingeniería de procesos del negocio, la asignación de personal, la designación de fuentes internas o externas, etc. El plan mismo deberá hacer referencia a otros planes tales como el plan de calidad de la organización y el plan de manejo de riesgos de información.

1.1.4 Cambios al Plan a largo plazo de Tecnología de Información
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que se establezca un proceso para modificar oportunamente y con precisión el plan a largo plazo de tecnología de información con el fin de adaptar los cambios al plan a largo plazo de la organización y los cambios en las condiciones de la tecnología de información.

1.1.5 Planeación a corto plazo para la Función de Servicios de Información
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que el plan a largo plazo de tecnología de información sea traducido regularmente a planes a corto plazo de tecnología de información. Estos planes a corto plazo deberán asegurar que se asignen los recursos apropiados de la función de servicios de tecnología de información con una base consistente con el plan a largo plazo de tecnología de información. Los planes a corto plazo deberán ser reevaluados y modificados periódicamente según se considere necesario respondiendo a las condiciones de cambios en el negocio y en la tecnología de información. La

realización oportuna de estudios de factibilidad deberá asegurar que la ejecución de los planes a corto plazo sea iniciada adecuadamente.

1.1.6 Evaluación de Sistemas Existentes
En forma previa al desarrollo o modificación del Plan Estratégico de TI, el responsable para la coordinación y gestión de los servicios debe evaluar los sistemas existentes en términos de: nivel de automatización de negocio, funcionalidad, estabilidad, complejidad, costo y fortalezas y debilidades, con el propósito de determinar el nivel de soporte que reciben los requerimientos del negocio de los sistemas existentes.

1.2 DEFINICIÓN DE LA ARQUITECTURA DE INFORMACIÓN

1.2.1 Modelo de la Arquitectura de Información
La información deberá conservar consistencia con las necesidades y deberá ser identificada, capturada y comunicada en una forma y dentro de períodos de tiempo que permitan a los responsables llevar a cabo sus tareas eficiente y oportunamente. Asimismo, la función de sistemas de información deberá crear y actualizar regularmente un modelo de arquitectura de información, abarcando el modelo de datos corporativo y los sistemas de información asociados. El modelo de arquitectura de información deberá conservar consistencia con el plan a largo plazo de tecnología de información.

1.2.2 Diccionario de Datos y Reglas de Sintaxis de Datos de la Corporación
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar la creación y la continua actualización de un diccionario de datos corporativo que incorpore las reglas de sintaxis de datos de la organización.

1.2.3 Esquema de Clasificación de Datos
Deberá establecerse un marco de referencia de clasificación general relativo a la ubicación de datos en clases de información (por ejemplo, categorías de seguridad), así como a la asignación de propiedad. Las reglas de acceso para las clases deberán definirse apropiadamente.

1.2.4 Niveles de Seguridad
El responsable para la coordinación y gestión de los servicios de TI deberá definir, implementar y mantener niveles de seguridad para cada una de las clasificaciones de datos identificadas con un nivel superior al de "no requiere protección". Estos niveles de seguridad deberán representar el conjunto de medidas de seguridad y de control apropiado (mínimo) para cada una de las clasificaciones.

1.3 DETERMINACIÓN DE LA DIRECCIÓN TECNOLÓGICA

1.3.1 Planeación de la Infraestructura Tecnológica
El responsable para la coordinación y gestión de los servicios de TI deberá crear y actualizar regularmente un plan de infraestructura tecnológica que concuerde con los planes a largo y corto plazo de tecnología de información. Dicho plan deberá abarcar aspectos tales como arquitectura de sistemas, dirección tecnológica y estrategias de migración.

1.3.2 Monitoreo de Tendencias y Regulaciones Futuras
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar el continuo monitoreo de tendencias futuras y condiciones regulatorias, de tal manera que estos factores

puedan ser tomados en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.

1.3.3 Contingencias en la Infraestructura Tecnológica
El plan de infraestructura tecnológica deberá ser evaluado sistemáticamente en cuanto a aspectos de contingencia (por ejemplo, redundancia, resistencia, capacidad de adecuación y evolución de la infraestructura).

1.3.4 Planes de Adquisición de Hardware y Software
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que los planes de adquisición de hardware y software sean establecidos y que reflejen las necesidades identificadas en el plan de infraestructura tecnológica.

1.3.5 Estándares de Tecnología
Tomando como base el plan de infraestructura tecnológica, el responsable para la coordinación y gestión de los servicios de TI deberá definir normas de tecnología con la finalidad de fomentar la estandarización.

1.4 DEFINICIÓN DE LA ORGANIZACIÓN Y DE LAS RELACIONES DE TI

1.4.1 Comité de planeación o dirección de la función de servicios de información
La alta dirección de la organización deberá designar un comité de planeación o dirección para monitorear las TI y sus actividades. Entre los miembros del comité deberán encontrarse el responsable para la coordinación y gestión de los servicios de TI, un representante de la dirección usuaria y de la función de servicios de información. El comité deberá reunirse regularmente y reportar a la alta dirección.

1.4.2 Ubicación de los servicios de información en la organización
Al ubicar al responsable para la coordinación y gestión de los servicios de TI en la estructura organizacional general, la alta dirección deberá asegurar la existencia de autoridad, actitud crítica e independencia de la unidades organizativas usuarias con un grado tal que sea posible garantizar soluciones de tecnología de información efectivas y progreso suficiente al implementarlas, así como establecer una relación con la alta dirección para incrementar la capacidad de previsión, la comprensión y las habilidades para identificar y resolver problemas de tecnología de información.

1.4.3 Revisión de Logros Organizacionales
Deberá establecerse un marco de referencia con el propósito de revisar que la estructura organizacional cumpla continuamente con los objetivos y se adapte a las cambiantes circunstancias.

1.4.4 Funciones y Responsabilidades
La dirección deberá asegurar que todo el personal en la organización conozca sus funciones y responsabilidades en relación con los sistemas de información. Todo el personal deberá contar con la autoridad suficiente para llevar a cabo las funciones y responsabilidades que le hayan sido asignadas. Todos deberán estar conscientes de que tienen una cierta responsabilidad con especto a la seguridad y al control interno. Consecuentemente, deberán organizarse y emprenderse campañas regulares para aumentar la conciencia y la disciplina.

1.4.5 Responsabilidad del aseguramiento de la calidad
El responsable para la coordinación y gestión de los servicios de TI deberá asignar la responsabilidad de la ejecución de la función de gestión de calidad a miembros del personal de TI y asegurar que existan sistemas de gestión de calidad apropiados, controles y experiencia en comunicación dentro del grupo de gestión de calidad de la función de servicios de información. La ubicación de la función dentro del área de servicios de información, las responsabilidades y el tamaño del grupo de gestión de calidad deberán satisfacer los requisitos de la empresa.

1.4.6 Responsabilidad de la Seguridad Lógica y Física
La alta dirección deberá asignar formalmente la responsabilidad de la seguridad lógica y física de los activos de información de la organización a un responsable de seguridad de la información, quien reportará a la alta dirección. Como mínimo, la responsabilidad de la seguridad deberá establecerse a todos los niveles de la organización para manejar los problemas generales de seguridad en la organización. En caso necesario, deberán asignarse responsabilidades de seguridad adicionales a niveles específicos con el fin de resolver los problemas de seguridad relacionados con ellos.

1.4.7 Propiedad y Custodia
El responsable para la coordinación y gestión de los servicios de TI deberá crear una estructura para designar formalmente a los propietarios y custodios de los datos. Sus funciones y responsabilidades deberán estar claramente definidas.

1.4.8 Propiedad de Datos y Sistemas
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que todos los activos de información (sistemas y datos) cuenten con un propietario asignado que tome decisiones sobre la clasificación y los derechos de acceso. Los propietarios del sistema normalmente delegarán la custodia diaria al grupo de liberación/operación de sistemas y las responsabilidades de seguridad a un administrador de la seguridad. Los Propietarios, sin embargo, permanecerán como responsables del mantenimiento de medidas de seguridad apropiadas.

1.4.9 Supervisión
La alta dirección deberá implementar prácticas de supervisión adecuadas en la organización de servicios de información para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente, para evaluar si todo el personal cuenta con suficiente autoridad y recursos para llevar a cabo sus tareas y responsabilidades, y para revisar de manera general los indicadores clave de desempeño.

1.4.10 Segregación de Funciones
La alta dirección deberá implementar una división de funciones y responsabilidades que excluya la posibilidad de que un solo individuo resuelva un proceso crítico. El responsable para la coordinación y gestión de los servicios de TI deberá asegurar también que el personal lleve a cabo únicamente aquellas tareas estipuladas para sus respectivos puestos. En particular, deberá mantenerse una segregación de funciones entre las siguientes funciones: uso de sistemas de información; entrada de datos; operación de cómputo; administración de redes; administración de sistemas; desarrollo y mantenimiento de sistemas administración de cambios; administración de seguridad; y auditoria de seguridad

1.4.11 Asignación de Personal para Tecnología de Información
Las evaluaciones de los requisitos de asignación de personal deberán llevarse a cabo regularmente para asegurar que TI cuente con un número suficiente de personal competente de

tecnología de información. Los requisitos de asignación de personal deberán ser evaluados por lo menos anualmente o al presentarse cambios mayores en el negocio, en el ambiente operacional o de tecnología de información. Deberá actuarse oportunamente tomando como base los resultados de las evaluaciones para asegurar una asignación de personal adecuada en el presente y en el futuro.

1.4.12 Descripción de Puestos para el Personal de la Función de Servicios de Información
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que las descripciones de los puestos para el personal de TI sean establecidos y actualizados regularmente. Estas descripciones de puestos deberán delinear claramente tanto la responsabilidad como la autoridad, incluir las definiciones de las habilidades y la experiencia necesarias para el puesto, y ser adecuadas para su utilización en evaluaciones de desempeño.

1.4.13 Personal Clave de TI
El responsable para la coordinación y gestión de los servicios de TI deberá definir e identificar al personal clave de tecnología de información.

1.4.14 Procedimientos para personal por contrato
El responsable para la coordinación y gestión de los servicios de TI deberá definir e implementar procedimientos relevantes para controlar las actividades de consultores y demás personal externo contratado por TI para asegurar la protección de los activos de información de la organización.

1.4.15 Relaciones
El responsable para la coordinación y gestión de los servicios de TI deberá llevar a cabo las acciones necesarias para establecer y mantener una coordinación, una comunicación y un enlace óptimos entre TI y demás elementos interesados dentro y fuera de TI (usuarios, proveedores, responsables de seguridad).

1.5 MANEJO DE LA INVERSIÓN EN TECNOLOGÍA DE INFORMACIÓN

1.5.1 Presupuesto Operativo Anual para la Función de Servicios de Información
La alta dirección deberá implementar un proceso de definición de presupuestos para asegurar que un presupuesto operativo anual para TI sea establecido y probado en línea con los planes a largo y corto plazo de la organización, así como con los planes a largo y corto plazo de tecnología de información. Deberán investigarse alternativas de financiamiento.

1.5.2 Monitoreo de Costo - Beneficios
El responsable para la coordinación y gestión de los servicios de TI deberá establecer un proceso de monitoreo de costos que compare los costos reales contra los presupuestados. Aun más, los posibles beneficios derivados de la actividad de tecnología de información deberán ser identificados y reportados. En cuanto al monitoreo de costos, la fuente de las cifras reales deberá tomar como base el sistema de contabilidad de la organización, mismo que deberá registrar, procesar y reportar rutinariamente los costos asociados con las actividades de la función de servicios de información. Por lo que toca a monitoreo de beneficios, se deberán definir indicadores de medición de desempeño de alto nivel y ser reportados y revisados regularmente para asegurar su adecuación.

1.5.3 Justificación de Costo - Beneficio
Deberá establecerse un control direccional que garantice que la prestación de servicios por parte de TI se justifique en cuanto a costos y se encuentre en línea con la industria. Los beneficios derivados de las actividades de tecnología de información deberán ser analizados en forma similar.

1.6 COMUNICACIÓN DE LA DIRECCIÓN Y ASPIRACIONES DE LA DIRECCION

1.6.1 Ambiente Positivo de Control de la Información
El responsable para la coordinación y gestión de los servicios de TI deberá crear un marco de referencia y un programa de previsión que fomente un ambiente de control positivo a través de toda la organización al aplicar elementos tales como: integridad, valores éticos, competencia del trabajador, filosofía y estilo operativo de la dirección, responsabilidad, atención y dirección proporcionada por el Consejo Directivo. Deberá ponerse especial atención a los aspectos relacionados con tecnología de información.

1.6.2 Responsabilidad de la dirección en cuanto a Políticas
La alta dirección deberá asumir la responsabilidad completa de la formulación, el desarrollo, la documentación, la promulgación y el control de políticas que cubran metas y directrices generales. Deberán llevarse a cabo revisiones regulares de las políticas para asegurar su conveniencia. La complejidad de las políticas y los procedimientos escritos deberán estar siempre en proporción con el tamaño de la organización y el estilo de dirección.

1.6.3 Comunicación de las Políticas de la Organización
La alta dirección deberá asegurar que las políticas organizacionales sean comunicadas y comprendidas por todos los niveles de la organización.

1.6.4 Recursos para la implementación de Políticas
Posterior a la comunicación, la alta dirección deberá destinar recursos para la implementación de sus políticas. La dirección deberá también monitorear la duración de la implementación de sus políticas.

1.6.5 Mantenimiento de Políticas
Las políticas deberán ser ajustadas regularmente para adecuarse a las condiciones cambiantes. Las políticas deberán ser reevaluadas, por lo menos anualmente o al momento de presentarse cambios significativos en el ambiente operacional o del negocio, para evaluar que sean convenientes y apropiadas y deberán ser modificadas en caso necesario. El responsable para la coordinación y gestión de los servicios de TI deberá proporcionar un marco de referencia y un proceso para las revisiones periódicas y la aprobación de estándares, políticas, directrices y procedimientos.

1.6.6 Cumplimiento de Políticas, Procedimientos y Estándares
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que se establezcan procedimientos apropiados para determinar si el personal comprende los procedimientos y políticas implementados, y que éste cumple con dichas políticas y procedimientos. El cumplimiento de las reglas de ética, seguridad y estándares de control interno deberá ser establecido por la alta dirección y promoverse a través del ejemplo.

1.6.7 Compromiso con la Calidad
El responsable para la coordinación y gestión de los servicios de TI deberá definir, documentar y mantener una filosofía de calidad, así como políticas y objetivos que sean consistentes con la

filosofía y las políticas de la corporación a este respecto. La filosofía de calidad, las políticas y los objetivos deberán ser comprendidos, implementados y mantenidos a todos los niveles de la función de servicios de información.

1.6.8 Política sobre el Marco de Referencia para la Seguridad y el Control Interno
La alta dirección deberá asumir la responsabilidad total del desarrollo y mantenimiento de una política sobre el marco de referencia, que establezca el enfoque general de la organización en cuanto a seguridad y control interno. La política deberá cumplir con los objetivos generales del negocio y estar dirigida a la minimización de riesgos a través de medidas preventivas, identificación oportuna de irregularidades, limitación de pérdidas y recuperación oportuna. Estas medidas deberán basarse en análisis costo-beneficio y deberá priorizarse. Además, la alta gerencia deberá asegurar que esta política de seguridad de alto nivel y de control interno especifique el propósito y los objetivos, la estructura gerencial, el alcance dentro de la organización, la definición y asignación de responsabilidades para su implementación a todos los niveles y la definición de multas y de acciones disciplinarias asociadas con la falta de cumplimiento con las políticas de seguridad y control interno.

1.6.9 Derechos de propiedad intelectual
La alta dirección deberá proveer e implementar una política por escrito sobre derechos de propiedad intelectual, que cubra el desarrollo de software, tanto interno como contratado a externos.

1.6.10 Políticas para Situaciones Específicas
Deberán ponerse en práctica medidas que aseguren el establecimiento de políticas para situaciones específicas con el fin de documentar las decisiones direccionales con respecto al tratamiento de actividades, aplicaciones, sistemas o tecnologías particulares.

1.7 ADMINISTRACIÓN DE RECURSOS HUMANOS

1.7.1 Reclutamiento y Promoción de Personal
El responsable para la coordinación y gestión de los servicios de TI deberá implementar y evaluar regularmente los procesos necesarios para asegurar que las prácticas de reclutamiento y promoción de personal tengan como base criterios objetivos y consideren factores como la educación, la experiencia y la responsabilidad. Estos procesos deberán estar en línea con las políticas y procedimientos generales de la organización a este respecto.

1.7.2 Personal Calificado
El responsable para la coordinación y gestión de los servicios de TI deberá verificar regularmente que el personal que lleva a cabo tareas específicas esté calificado tomando como base una educación, entrenamiento y/o experiencia apropiados, según se requiera. La dirección deberá alentar al personal para que participe como miembro, en organizaciones profesionales.

1.7.3 Entrenamiento de Personal
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que los empleados reciban orientación al ser contratados, así como entrenamiento y capacitación constantes con la finalidad de conservar los conocimientos, habilidades, destrezas y conciencia de seguridad al nivel requerido, para la ejecución efectiva de sus tareas. Los programas de educación y entrenamiento dirigidos a incrementar los niveles de habilidad técnica y administrativa del personal deberán ser revisados regularmente.

1.7.4 Entrenamiento Cruzado o Respaldo de personal
El responsable para la coordinación y gestión de los servicios de TI deberá proporcionar un entrenamiento "cruzado" o contar con suficiente personal de respaldo con la finalidad de solucionar posibles ausencias. El personal encargado de puestos delicados deberá tomar vacaciones ininterrumpidas con una duración suficiente como para probar la habilidad de la organización para manejar casos de ausencia y detectar actividades fraudulentas.

1.7.5 Procedimientos de Acreditación de Personal
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que su personal se sujete a una revisión o acreditación de seguridad antes de ser contratado, transferido o promovido, dependiendo de lo delicado o sensible del puesto. Un empleado que no haya pasado por este procedimiento de revisión o acreditación al ser contratado por primera vez, no deberá ser colocado en un puesto delicado hasta que éste haya obtenido la acreditación de seguridad.

1.7.6 Evaluación de Desempeño de los Empleados
La alta dirección deberá implementar un proceso de evaluación de desempeño de los empleados y asegurar que dicha evaluación sea llevada a cabo regularmente según los estándares establecidos y las responsabilidades específicas del puesto. Los empleados deberán recibir asesoría sobre su desempeño o su conducta cuando esto sea apropiado.

1.7.7 Cambios de Puesto
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que se tomen acciones oportunas y apropiadas con respecto a cambios de puesto y cese de la relación laboral, de tal manera que los controles internos y la seguridad no se vean perjudicados por estos eventos.

1.8 ASEGURAMIENTO DEL CUMPLIMIENTO DE LOS REQUISITOS EXTERNOS

1.8.1 Revisión de Requisitos Externos
La organización deberá establecer y mantener procedimientos para la revisión de requisitos externos y para la coordinación de estas actividades. La investigación continua deberá determinar los requisitos externos aplicables en la organización. Deberán revisarse los requisitos legales, gubernamentales o cualquier otro requisito externo relacionado con las prácticas y controles de tecnología de información. La dirección deberá también evaluar el impacto de cualquier relación externa en las necesidades generales de información de la organización, incluyendo la determinación del grado al cual las estrategias de TI deben soportar o cumplir con los requisitos de terceros.

1.8.2 Prácticas y Procedimientos para el Cumplimiento de Requisitos Externos
Las prácticas organizacionales deberán asegurar que se lleven a cabo oportunamente las acciones correctivas apropiadas para garantizar el cumplimiento de los requisitos externos. Además, deberán establecerse y mantenerse procedimientos adecuados que aseguren el cumplimiento continuo A este respecto la dirección deberá solicitar apoyo legal en caso necesario.

1.8.3 Cumplimiento de Seguridad y Ergonomía
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar el cumplimiento de los estándares ergonómicos y de seguridad física en el ambiente de trabajo de los usuarios y el personal de la función de servicios de información.

1.8.4 Privacidad, propiedad intelectual y flujos de datos
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar el cumplimiento de las regulaciones sobre privacidad o confidencialidad, propiedad intelectual, flujo de datos externos y criptografía aplicables a las prácticas de tecnología de información de la organización.

1.8.5 Comercio Electrónico
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que se establezcan contratos formales para determinar acuerdos entre socios comerciales sobre procesos de comunicación, así como sobre estándares de mensajes de transacción, seguridad y almacenamiento de datos. Cuando se realicen operaciones de intercambio en Internet, El responsable para la coordinación y gestión de los servicios de TI deberá imponer adecuados controles para asegurar el cumplimiento de leyes locales y costumbres en un ámbito mundial.

1.8.6 Cumplimiento con los Contratos de Seguros
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar la identificación y el continuo cumplimiento de los requisitos de los contratos de seguros.

1.9 EVALUACIÓN DE RIESGOS

1.9.1 Evaluación de Riesgos del Negocio
El responsable para la coordinación y gestión de los servicios de TI deberá establecer un marco de referencia de evaluación sistemática de riesgos. Este marco de referencia deberá incorporar una evaluación regular de los riesgos de información relevantes para el logro de los objetivos del negocio, formando una base para determinar la manera en la que los riesgos deben ser manejados a un nivel aceptable. El proceso deberá proporcionar evaluaciones de riesgos tanto a un nivel global como a niveles específicos del sistema (para nuevos proyectos y para casos recurrentes) y deberá asegurar actualizaciones regulares a la información sobre evaluación de riesgos utilizando los resultados de auditorías, inspecciones e incidentes identificados.

1.9.2 Enfoque de Evaluación de Riesgos
El responsable para la coordinación y gestión de los servicios de TI deberá establecer un enfoque general para la evaluación de riesgos que defina el balance y los límites, la metodología a ser adoptada para las evaluaciones de riesgos, las responsabilidades y las habilidades requeridas. La calidad de las evaluaciones de riesgos deberá estar asegurada por un método estructurado y por asesores expertos en riesgos.

1.9.3 Identificación de Riesgos
La evaluación de riesgos deberá enfocarse al examen de los elementos esenciales de riesgo, tales como activos, amenazas, elementos vulnerables, protecciones, consecuencias y probabilidad de amenaza.

1.9.4 Medición de Riesgos
El enfoque de la evaluación de riesgos deberá asegurar que el análisis de la información de identificación de riesgos genere como resultado una medida cuantitativa y/o cualitativa del riesgo al cual está expuesta el área examinada. Asimismo, deberá evaluarse la capacidad de aceptación de riesgos de la organización.

1.9.5 Plan de Acción contra Riesgos
El enfoque de evaluación de riesgos deberá proporcionar la definición de un plan de acción contra riesgos para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continua.

1.9.6 Aceptación de Riesgos
El enfoque de la evaluación de riesgos deberá asegurar la aceptación formal del riesgo residual, dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de qué tan económico resulte implementar protecciones y controles. El riesgo residual deberá compensarse con una cobertura de seguro adecuada.

1.10 GESTION DE PROYECTOS

1.10.1 Marco de Referencia para la Gestión de Proyectos
El responsable para la coordinación y gestión de los servicios de TI deberá establecer un marco de referencia general para la gestión de proyectos que defina el alcance y los límites del mismo, así como la metodología de administración de proyectos a ser adoptada y aplicada para cada proyecto emprendido. La metodología deberá cubrir, como mínimo, la asignación de responsabilidades, la determinación de tareas, la realización de presupuestos de tiempo y recursos, los avances, los puntos de revisión y las aprobaciones.

1.10.2 Participación del Departamento Usuario en la Iniciación de Proyectos
El marco de referencia de la gestión de proyectos de la organización deberá fomentar la participación del departamento usuario afectado en la definición y autorización de cualquier proyecto de desarrollo, implementación o modificación.

1.10.3 Miembros y Responsabilidades del Equipo del Proyecto
El marco de referencia de gestión de proyectos de la organización deberá especificar las bases para asignar a los miembros del personal al proyecto y definir las responsabilidades y autoridades de los miembros del equipo del proyecto.

1.10.4 Definición del Proyecto
El marco de referencia de gestión de proyectos de la organización deberá generar la creación de un estatuto claro por escrito que defina la naturaleza y el alcance de cada proyecto de implementación antes de que los trabajos del mismo sean iniciados.

1.10.5 Aprobación del Proyecto
El marco de referencia de gestión de proyectos de la organización deberá asegurar que, para cada proyecto propuesto, la alta dirección de la organización revise los reportes de los estudios de factibilidad relevantes como una base para fundamentar la decisión de proceder con el proyecto.

1.10.6 Aprobación de las Fases del Proyecto
El marco de referencia de gestión de proyectos de la organización deberá disponer que los Gerentes designados para las funciones del usuario y de los servicios de información aprueben el trabajo realizado en cada fase del ciclo antes de iniciar los trabajos de la siguiente fase.

1.10.7 Plan Maestro del Proyecto
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que, para cada proyecto aprobado, se cree un plan maestro adecuado que mantenga el control del proyecto

a través de todo su desarrollo e incluya un método de monitoreo del tiempo y los costos incurridos durante su vida.

1.10.8 Plan de Aseguramiento de la Calidad de Sistemas

El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que la implementación de un sistema nuevo o modificado incluya la preparación de un plan de calidad que sea integrado posteriormente al plan maestro del proyecto y que sea formalmente revisado y acordado por todas las partes interesadas.

1.10.9 Planeación de Métodos de Aseguramiento

Las tareas de aseguramiento deberán ser definidas durante la fase de planeación del marco de referencia de gestión de proyectos. Las tareas de aseguramiento deberán apoyar la acreditación de sistemas nuevos o modificados y garantizar que los controles internos y los dispositivos de seguridad cumplan con los requisitos necesarios.

1.10.10 Administración Formal de Riesgos de Proyectos

El responsable para la coordinación y gestión de los servicios de TI deberá implementar un programa de administración formal de riesgos de proyectos para eliminar o minimizar los riesgos asociados con proyectos individuales (por ejemplo, identificación y control de áreas o eventos que tengan el potencial de causar cambios no deseados).

1.10.11 Plan de Prueba

El marco de referencia de gestión de proyectos de la organización deberá requerir la creación de un plan de pruebas para cada proyecto de desarrollo, implementación y modificación.

1.10.12 Plan de Entrenamiento

El marco de referencia de gestión de proyectos de la organización deberá requerir la creación de un plan de entrenamiento para cada proyecto de desarrollo, implementación y modificación.

1.10.13 Plan de Revisión Post - Implementación

El marco de referencia de gestión de proyectos de la organización deberá disponer que, como parte integral de las actividades del equipo del proyecto, se desarrolle un plan de revisión post - implementación para cada sistema de información nuevo o modificado, con la finalidad de determinar si el proyecto ha generado los beneficios planeados.

1.11 GESTION DE CALIDAD

1.11.1 Plan General de Calidad

La alta dirección deberá desarrollar y mantener regularmente un plan general de calidad basado en los planes organizacionales y de tecnología de información a largo plazo. El plan deberá promover la filosofía de mejora continua y contestar a las preguntas básicas de qué, quién y cómo.

1.11.2 Enfoque de Gestión de Calidad

El responsable para la coordinación y gestión de los servicios de TI deberá establecer un enfoque estándar con respecto a la gestión de calidad, que cubra tanto las actividades de gestión de calidad generales como las específicas de un proyecto. El enfoque deberá determinar el (los) tipo(s) de actividades de gestión de calidad (tales como revisiones, auditorías, inspecciones, etc.) que deben realizarse para alcanzar los objetivos del plan general de calidad. Asimismo deberá requerir una revisión específica de gestión de calidad.

1.11.3 Planeación de la Gestión de calidad
El responsable para la coordinación y gestión de los servicios de TI deberá implementar un proceso de planeación de gestión de calidad para determinar el alcance y la duración de las actividades de gestión de calidad.

1.11.4 Revisión del Aseguramiento de la Calidad sobre el Cumplimiento de Estándares y Procedimientos de la Función de Servicios de Información
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que las responsabilidades asignadas al personal de gestión de calidad incluyan una revisión del cumplimiento general de los estándares y procedimientos de la función de servicios de información.

1.11.5 Metodología del Ciclo de Vida de Desarrollo de Sistemas
La alta dirección de la organización deberá definir e implementar estándares de sistemas de información y adoptar una metodología del ciclo de vida de desarrollo de sistemas que rija el proceso de desarrollo, adquisición, implementación y mantenimiento de sistemas de información computarizados y tecnología afín. La metodología del ciclo de vida de desarrollo de sistemas elegida deberá ser la apropiada para los sistemas a ser desarrollados, adquiridos, implementados y mantenidos.

1.11.6 Metodología del Ciclo de Vida de Desarrollo de Sistemas para Cambios Mayores a la Tecnología Actual
En el caso de requerirse cambios mayores a la tecnología actual, el responsable para la coordinación y gestión de los servicios de TI deberá asegurar el cumplimiento de la metodología del ciclo de vida de desarrollo de sistemas, como en el caso de adquisición de nueva tecnología.

1.11.7 Actualización de la Metodología del Ciclo de Vida de Desarrollo de Sistemas
La alta dirección deberá implementar una revisión periódica de su metodología del ciclo de vida de desarrollo de sistemas para asegurar que incluya técnicas y procedimientos actuales generalmente aceptados.

1.11.8 Coordinación y Comunicación
El responsable para la coordinación y gestión de los servicios de TI deberá establecer un proceso para asegurar la coordinación y comunicación estrecha entre los clientes de TI y los desarrolladores de sistemas. Este proceso deberá ocasionar que los métodos estructurados que utilicen la metodología del ciclo de vida de desarrollo de sistemas aseguren la provisión de soluciones de tecnología de información de calidad que satisfagan las demandas de negocio. El responsable para la coordinación y gestión de los servicios de TI deberá promover una organización que se caracterice por la estrecha cooperación y comunicación a lo largo del ciclo de vida de desarrollo de sistemas.

1.11.9 Marco de Referencia de Adquisición y Mantenimiento para la Infraestructura de Tecnología
Deberá establecerse un marco de referencia general referente a la adquisición y mantenimiento de la infraestructura de tecnología. Los diferentes pasos que deben ser seguidos con respecto a la infraestructura de tecnología (tales como adquisición; programación, documentación y pruebas; establecimiento de parámetros; mantenimiento y aplicación de correcciones) deberán estar regidos por y mantenerse en línea con el marco de referencia para la adquisición y mantenimiento de la infraestructura de tecnología.

1.11.10 Relaciones con Terceras Partes como Programadores
El responsable para la coordinación y gestión de los servicios de TI deberá implementar un proceso para asegurar las buenas relaciones de trabajo con terceras partes como desarrolladores externos. Dicho proceso deberá disponer que el usuario y el programador estén de acuerdo sobre los criterios de aceptación, el manejo de cambios, los problemas durante el desarrollo, las funciones de los usuarios, las instalaciones, las herramientas, el software, los estándares y los procedimientos.

1.11.11 Estándares para la Documentación de Programas
La metodología del ciclo de vida de desarrollo de sistemas deberá incorporar estándares para la documentación de programas que hayan sido impuestos y comunicados al personal interesado. La metodología deberá asegurar que la documentación creada durante el desarrollo del sistema de información o de los proyectos de modificación coincida con estos estándares.

1.11.12 Estándares para Pruebas de Programas
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe proporcionar estándares que cubran los requisitos de pruebas, verificación, documentación y retención para probar las unidades de software y los programas agregados, creados como parte de cada proyecto de desarrollo o modificación de sistemas de información.

1.11.13 Estándares para Pruebas de Sistemas
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe proporcionar estándares que cubran los requisitos de pruebas, verificación, documentación y retención para probar el sistema total, como parte de cada proyecto de desarrollo o modificación de sistemas de información.

1.11.14 Pruebas Piloto
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe definir las condiciones bajo las cuales deberán conducirse las pruebas piloto (de aceptación, en paralelo) de sistemas nuevos y/o actuales.

1.11.15 Documentación de las Pruebas del Sistema
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe disponer, como parte de cualquier proyecto de desarrollo, implementación o modificación de sistemas de información, que se conserve la documentación de los resultados de las pruebas del sistema.

1.11.16 Evaluación del Aseguramiento de la Calidad sobre el Cumplimiento de Estándares de Desarrollo
El enfoque de gestión de calidad de la organización deberá requerir que una revisión post - implementación de un sistema de información operacional evalúe si el equipo encargado del proyecto, cumplió con las estipulaciones de la metodología del ciclo de vida de desarrollo de sistemas.

1.11.17 Revisión de la Gestión de calidad sobre el Logro de los Objetivos de la Función de Servicios de Información
El enfoque de gestión de calidad deberá incluir una revisión de hasta qué punto los sistemas particulares y las actividades de desarrollo de aplicaciones han alcanzado los objetivos de la función de servicios de información.

1.11.18 Métricas de calidad
El responsable para la coordinación y gestión de los servicios de TI deberá definir y utilizar métricas para medir los resultados de actividades, evaluando si las metas de calidad han sido alcanzadas

1.11.19 Reportes de Revisiones de Gestión de calidad
Los reportes de revisiones de gestión de calidad deberán ser preparados y enviados a los departamentos usuarios y a la función de servicios de información.

2 IMPLANTACION

2.1 IDENTIFICACIÓN DE SOLUCIONES

2.1.1 Definición de requisitos de información
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que los requisitos de la entidad ya satisfechos por el sistema actual y a ser satisfechos por el sistema nuevo propuesto o modificado (programas, datos e infraestructura), estén claramente definidos antes de aprobar cualquier proyecto de desarrollo, implementación o modificación. La metodología del ciclo de vida de desarrollo de sistemas deberá exigir que los requisitos de las soluciones funcionales y operacionales sean especificados, incluyendo desempeño, protección, confiabilidad, compatibilidad, seguridad y legislación.

2.1.2 Formulación de acciones alternativas
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe proveer el análisis de las acciones alternativas que deberán satisfacer los requisitos de la entidad, establecidos para un sistema nuevo o modificado.

2.1.3 Formulación de estrategias de adquisición
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe estipular un plan de estrategia de adquisición, definiendo si el software será “adquirido del mostrador”, desarrollados internamente, a través de contratación o mediante una combinación de estos.

2.1.4 Requisitos de servicios de terceros
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe estipular la evaluación de requisitos y las especificaciones para una Solicitud de Propuesta cuando se negocie con un proveedor de servicios externo.

2.1.5 Estudio de factibilidad tecnológica
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe estipular un examen de factibilidad tecnológica de cada alternativa con la finalidad de satisfacer los requisitos de negocio establecidos para el desarrollo de un proyecto propuesto de cualquier sistema nuevo o modificado.

2.1.6 Estudio de factibilidad económica
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe generar, en cada proyecto de desarrollo, implementación y modificación de sistemas de información propuesto, el análisis de los costos y beneficios asociados con cada alternativa considerada para satisfacer os requisitos de la entidad establecidos.

2.1.7 Arquitectura de información
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que se tome en consideración el modelo de datos de la empresa al definir las soluciones y analizar la factibilidad de las mismas.

2.1.8 Reporte de análisis de riesgos
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar, en cada proyecto de desarrollo, implementación y modificación de sistemas de información propuesto, el análisis y la documentación de las amenazas a la seguridad, puntos de impacto y debilidad y protecciones factibles de seguridad y control interno, con la finalidad de reducir o eliminar el riesgo identificado. Esto deberá llevarse a cabo en línea con el marco de referencia general de evaluación de riesgos.

2.1.9 Controles de seguridad económicos
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que los costos y beneficios de seguridad sean examinados cuidadosamente en términos monetarios y no monetarios, para garantizar que los costos de los controles no excedan a los beneficios. La decisión requerirá la firma de aprobación formal de la alta dirección.

2.1.10 Diseño de trazas de auditoría
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que existan mecanismos adecuados para trazas de auditoría o que dichos mecanismos puedan ser desarrollados para la solución identificada y seleccionada. Los mecanismos deberán proporcionar la capacidad de proteger datos sensitivos (ej. identificación de usuarios contra divulgación o mal uso)

2.1.11 Ergonomía
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que los proyectos de desarrollo, implementación y cambios emprendidos por la función de servicios de información, tomen en consideración los aspectos ergonómicos asociados con la introducción de soluciones automatizadas.

2.1.12 Selección del software del sistema
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que la función de servicios de información cumpla con un procedimiento estándar para identificar todos los programas de software potenciales que deberán satisfacer sus requisitos operacionales.

2.1.13 Control de suministros
El responsable para la coordinación y gestión de los servicios de TI deberá desarrollar e implementar un enfoque central de suministros que describa un conjunto común de procedimientos y estándares a ser seguidos en la adquisición de hardware, software y servicios relacionados con la tecnología de información. Los productos deberán ser revisados y probados antes de su utilización y pago.

2.1.14 Adquisición de productos de software
La adquisición de productos de software deberá seguir las políticas de adquisición de la organización.

2.1.15 Mantenimiento de software de terceras partes
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que, para el software con licencia adquirida a terceras partes, los proveedores cuenten con los procedimientos apropiados para validar, proteger y mantener los derechos de integridad de los productos de software. Deberá tomarse en consideración el soporte del producto en cualquier acuerdo de mantenimiento relacionado con el producto entregado.

2.1.16 Contratos de programación de aplicaciones
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que los servicios de programación contratados estén justificados con una solicitud de servicios por escrito por parte de un miembro designado por el responsable para la coordinación y gestión de los servicios de TI. El contrato deberá estipular que el software, la documentación y otros elementos entregables estén sujetos a pruebas y revisiones antes de ser aceptados. Además, deberá asegurar que los productos finales terminados por los servicios de programación contratados sean revisados y probados de acuerdo con los estándares definidos por el grupo de gestión de calidad de los servicios de TI y otras partes interesadas (como usuarios, admin. de proyectos) antes de pagar y aprobar el producto final. Las pruebas que deberán ser incluidas en las especificaciones del contrato deberán consistir en pruebas del sistema, integración, hardware y componentes, procedimientos, carga y estrés, pruebas de afinación y desempeño, pruebas de regresión, pruebas de aceptación del usuario y, finalmente, pruebas piloto del sistema total, con la finalidad de evitar fallas no esperadas del mismo.

2.1.17 Aceptación de instalaciones
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que, dentro del contrato con el proveedor, se acuerde un plan de aceptación para las instalaciones a ser proporcionadas, el cual defina los procedimientos y criterios de aceptación. Además, deberán llevarse a cabo pruebas de aceptación para garantizar que el acomodo y el medio cumplan con los requisitos especificados en el contrato.

2.1.18 Aceptación de tecnología
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que, dentro del contrato con el proveedor, se acuerde un plan de aceptación para la tecnología específica a ser proporcionada, el cual defina los procedimientos y criterios de aceptación. Además, las pruebas de aceptación establecidas en el plan, deberán incluir inspección, pruebas de funcionalidad y seguimiento de cargas de trabajo.

2.2 DESARROLLO Y MANTENIMIENTO DE SOFTWARE DE APLICACIÓN

2.2.1 Métodos de diseño
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe estipular que sean aplicados a técnicas y procedimientos apropiados, incluyendo una estrecha relación con los usuarios del sistema, en la creación de las especificaciones de diseño para cada nuevo proyecto de desarrollo de sistemas de información, y verificar las especificaciones del diseño contra los requisitos del usuario.

2.2.2 Cambios significativos a sistemas actuales
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que, en caso de presentarse la necesidad de realizar modificaciones significativas a los sistemas actuales, se siga un proceso de desarrollo similar al utilizado en el desarrollo de sistemas nuevos.

2.2.3 Aprobación del diseño
La metodología del ciclo de vida de desarrollo de sistemas de la organización requerirá que las especificaciones de diseño para todos los proyectos de desarrollo y modificación de sistemas de información, sean revisados y aprobados por el responsable para la coordinación y gestión de los servicios de TI, por las unidades organizativas usuarias afectadas y por la alta dirección de la organización, cuando esto sea pertinente.

2.2.4 Definición y documentación de requisitos de archivos
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar la aplicación de un procedimiento apropiado para la definición y documentación del formato de los archivos para cada proyecto de desarrollo y modificación de sistemas de información. Este procedimiento deberá garantizar el respeto a las reglas de diccionario de datos

2.2.5 Especificaciones de programas
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir la preparación de especificaciones detalladas por escrito, de los programas para cada proyecto de desarrollo o modificación de sistemas de información. Además, la metodología deberá garantizar que las especificaciones de los programas correspondan a las especificaciones del diseño del sistema.

2.2.6 Diseño para la recopilación de datos fuente
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir la especificación de mecanismos adecuados, para la recopilación y entrada de datos para cada proyecto de desarrollo y modificación de sistemas de información.

2.2.7 Definición y documentación de requisitos de entrada de datos
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que existan mecanismos adecuados para definir y documentar los requisitos de entrada de datos para cada proyecto de desarrollo o modificación de sistemas de información.

2.2.8 Definición de interfases
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe estipular que se especifiquen, diseñen y documenten apropiadamente todas las interfases internas y externas.

2.2.9 Interfaz usuario-máquina
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar el desarrollo de una interfaz entre el usuario y la máquina fácil de utilizar y que sea capaz de auto-documentarse (por medio de funciones de ayuda en línea).

2.2.10 Definición y documentación de requisitos de procesamiento
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que existan mecanismos adecuados para definir y documentar los requisitos de procesamiento para cada proyecto de desarrollo o modificación de sistemas de información.

2.2.11 Definición y documentación de requisitos de salida de datos
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que existan mecanismos adecuados para definir y documentar los requisitos de salida de datos para cada proyecto de desarrollo o modificación de sistemas de información.

2.2.12 Control interno
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que se especifiquen mecanismos adecuados, para garantizar que se identifiquen los requisitos de seguridad y control internos para cada proyecto de desarrollo o modificación de sistemas de información. La metodología deberá asegurar además que los sistemas de información estén diseñados para incluir controles de aplicación que garanticen que los datos de entrada y salida estén completos, así como su precisión, oportunidad y autorización. Deberá llevarse a cabo una evaluación de sensibilidad durante el inicio del desarrollo o modificación del sistema. Los aspectos básicos de seguridad y control interno de un sistema a ser desarrollado o modificado deberán ser evaluados junto con el diseño conceptual del mismo, con el fin de integrar los conceptos de seguridad en el diseño tan pronto como sea posible.

2.2.13 Disponibilidad como factor clave de diseño
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que la disponibilidad sea considerada en el proceso de diseño de nuevos o modificados sistemas de información en la fase más temprana posible. La disponibilidad debe ser analizada y, en caso necesario, incrementada a través de mejoras de mantenimiento y fiabilidad.

2.2.14 Consideraciones de integridad de tecnología para programas de aplicación
La organización deberá establecer procedimientos para asegurar, cuando esto proceda, que los programas de aplicación contengan estipulaciones que verifiquen sistemáticamente las tareas realizadas por el software, para apoyar el aseguramiento de la integridad de los datos y el cual haga posible la restauración de la integridad a través de procedimientos de recuperación u otros medios.

2.2.15 Pruebas a los programas de aplicación
Deberán aplicarse pruebas unitarias, pruebas de integración, de carga y estrés y finalmente las pruebas de calificación para liberar el sistema, u otras pruebas, de acuerdo con el plan de prueba del proyecto, cumpliendo las normas técnicas de pruebas establecidas, antes de ser aprobado el sistema por el usuario. Se deberán aplicar adecuadas medidas de seguridad para prevenir divulgación de información sensible durante las pruebas.

2.2.16 Materiales de consulta y soporte para usuarios
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que se preparen manuales de referencia y soporte para usuarios adecuados (preferiblemente en formato electrónico) como parte de cada proyecto de desarrollo o modificación de sistemas de información

2.2.17 Reevaluación del diseño del sistema
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que el diseño del sistema sea reevaluado siempre que ocurran discrepancias técnicas y/o lógicas durante el desarrollo o mantenimiento del sistema.

2.3 ADQUISICIÓN Y MANTENIMIENTO DE ARQUITECTURA DE TECNOLOGÍA

2.3.1 Evaluación de nuevo hardware y software
Deberán establecerse procedimientos para evaluar el impacto de nuevo hardware y software sobre el rendimiento del sistema en general.

2.3.2 Mantenimiento preventivo para hardware
El responsable para la coordinación y gestión de los servicios de TI deberá calendarizar el mantenimiento rutinario y periódico del hardware con el fin de reducir la frecuencia y el impacto de fallas de rendimiento.

2.3.3 Seguridad del software del sistema
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que la instalación del software del sistema no arriesgue la seguridad de los datos y programas ya almacenados en el mismo. Deberá ponerse gran atención a la instalación y mantenimiento de los parámetros del software del sistema.

2.3.4 Instalación del software del sistema
Deberán implementarse procedimientos para asegurar que el software del sistema sea instalado de acuerdo al marco de referencia de adquisición y mantenimiento de infraestructura de tecnología. Las pruebas deberán ser llevadas a cabo antes de autorizarse su utilización en ambiente de producción.

2.3.5 Mantenimiento del software del sistema
Deberán implementarse procedimientos para asegurar que el software del sistema sea mantenido de acuerdo al marco de referencia de adquisición y mantenimiento para infraestructura de tecnología.

2.3.6 Controles para cambios del software del sistema

Deberán implementarse procedimientos para asegurar que las modificaciones realizadas al software del sistema sean controladas de acuerdo con los procedimientos de gestión de cambios de la organización.

2.4 DESARROLLO Y MANTENIMIENTO DE PROCEDIMIENTOS RELACIONADOS CON TECNOLOGÍA DE INFORMACIÓN

2.4.1 Requisitos operacionales y niveles de servicios futuros
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar la definición oportuna de requisitos operacionales y niveles de servicios futuros.

2.4.2 Manual de procedimientos para usuario
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que se preparen y actualicen manuales adecuados de procedimientos para los usuarios como parte de cada proyecto de desarrollo o modificación de sistemas de información.

2.4.3 Manual de operaciones
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que se prepare y se mantenga actualizado un manual de operaciones adecuado como parte de cada proyecto de desarrollo o modificación de sistemas de información.

2.4.4 Material de entrenamiento
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar que se desarrollen materiales de entrenamiento adecuados como parte de cualquier proyecto de desarrollo, implementación o modificación de sistemas de información. Estos materiales deberán enfocarse al uso del sistema en la práctica diaria.

2.5 INSTALACIÓN Y ACREDITACIÓN DE SISTEMAS

2.5.1 Entrenamiento
El personal de las unidades organizativas de los usuarios afectados y el grupo de operaciones de los servicios de TI deberá estar entrenado de acuerdo al plan de entrenamiento definido y los materiales relacionados, como parte de cualquier proyecto de desarrollo, implementación o modificación de sistemas de información.

2.5.2 Adecuación del desempeño del software de aplicación
La medición (optimización) del desempeño del software de aplicación deberá establecerse como una parte integral de la metodología del ciclo de vida de desarrollo de sistemas de la organización para predecir los recursos requeridos para operar software nuevo o significativamente modificado.

2.5.3 Conversión
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe asegurar, como parte de cada proyecto de desarrollo, implementación o modificación de sistemas de información, que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo de acuerdo con el plan preestablecido.

2.5.4 Pruebas de Cambios
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que los cambios sean probados por un grupo de prueba independiente (distinto al del equipo de desarrollo, o al programador) de acuerdo con la evaluación de impacto y recursos en un ambiente de prueba separado antes de comenzar su uso en el ambiente de operación regular. También deberán desarrollarse planes de respaldo externo. Las pruebas de aceptación deberán llevarse a cabo en un ambiente representativo del ambiente operacional futuro (por ejemplo, condiciones similares de seguridad, controles internos o cargas de trabajo).

2.5.5 Criterios y desempeño de pruebas piloto y en paralelo
Deben establecerse procedimientos para asegurar que las pruebas piloto o en paralelo sean llevadas a cabo de acuerdo con un plan preestablecido y que los criterios para la terminación del proceso de pruebas sean especificados con anterioridad.

2.5.6 Prueba de aceptación final
Los procedimientos deberán asegurar, como parte de las pruebas de aceptación final o de gestión de calidad de sistemas de información nuevo o modificado, una evaluación y aprobación formal de los resultados de las pruebas por parte de los responsables de las unidades organizativas usuarias afectados y del responsable para la coordinación y gestión de los servicios de TI. Las pruebas deben cubrir todos los componentes del sistema de información (software de aplicación, instalaciones, tecnología, procedimientos de usuario).

2.5.7 Pruebas y acreditación de seguridad
El responsable para la coordinación y gestión de los servicios de TI deberá definir e implementar procedimientos para asegurar que la unidad organizativa de operaciones y la unidad organizativa usuaria aceptan formalmente los resultados de las pruebas de calificación y el nivel de seguridad para los sistemas, junto con el riesgo residual existente.

2.5.8 Prueba operacional
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que, antes de poner el sistema en operación, el usuario o custodio designado (la parte designada para ejecutar el

sistema en nombre del usuario), valide su operación como un producto completo, bajo condiciones similares a las del ambiente de aplicación y en la manera en la que el sistema será operado en un ambiente de producción (validación).

2.5.9 Paso a producción
El responsable para la coordinación y gestión de los servicios de TI deberá definir e implementar procedimientos formales para controlar la entrega del sistema de desarrollo a pruebas de calificación, validación (aceptación) y a operación. Los ambientes respectivos deberán separarse y protegerse apropiadamente.

2.5.10 Evaluación de la satisfacción de los requisitos del usuario
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que se realice una revisión post - implementación de los requisitos operacionales del sistema de información (por ejemplo, capacidad, desempeño de procesamiento a través del sistema) con el fin de evaluar si las necesidades del usuario están siendo satisfechas por el mismo.

2.5.11 Revisión de la Dirección post - implementación
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe requerir que una revisión post - implementación del sistema de información operacional evalúe y reporte si el sistema proporcionó los beneficios esperados de la manera más económica.

2.6 GESTIÓN DE CONFIGURACION

2.6.1 Inicio y control de solicitudes de cambio
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que todas las solicitudes de cambios tanto internos como por parte de proveedores estén estandarizados y sujetos a procedimientos formales de gestión de cambios. Las solicitudes deberán categorizarse, priorizarse y establecerse procedimientos específicos para manejar asuntos urgentes. Los solicitantes de cambios deben permanecer informados acerca del estatus de su solicitud.

2.6.2 Evaluación del impacto
Deberá establecerse un procedimiento para asegurar que todas las solicitudes de cambio sean evaluadas en una forma estructurada en cuanto a todos los posibles impactos sobre el sistema operacional y su funcionalidad.

2.6.3 Control de cambios
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que la gestión de cambios, así como el control y la distribución de software sean integrados apropiadamente en un sistema completo de gestión de configuración.

2.6.4 Documentación y procedimientos
El procedimiento de cambios deberá asegurar que, siempre que se implementen modificaciones a un sistema, la documentación y procedimientos relacionados sean actualizados de manera correspondiente.

2.6.5 Mantenimiento autorizado
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que el personal de mantenimiento tenga asignaciones específicas y que su trabajo sea monitoreado apropiadamente. Además, sus derechos de acceso al sistema deberán ser controlados para evitar riesgos de accesos no autorizados a los sistemas automatizados.

2.6.6 Política de liberación de software
El responsable para la coordinación y gestión de los servicios de TI deberá garantizar que la entrega (liberación) de software esté regida por procedimientos formales asegurando aprobación, empaque, pruebas de regresión, entrega.

2.6.7 Distribución de software
Deberán establecerse medidas de control específicas para asegurar la distribución del elemento de software correcto al lugar correcto, con integridad y de manera oportuna con trazas de auditoría adecuadas.

3. MONITOREO (VERIFICAR)

3.1 MONITOREO DEL PROCESO

3.1.1 Recolección de datos de monitoreo
Para los procesos de tecnología de información y de control interno, la Dirección deberá asegurar que se definan indicadores de desempeño relevantes (ej. comparaciones externas) tanto para actividades internas como las proporcionadas por terceros y que se recolecten datos para la creación de reportes relevantes de desempeño y reportes de excepción relacionados con estos indicadores.

3.1.2 Evaluación de desempeño
Los servicios a ser proporcionados por la función de servicios de información deberán ser medidos (indicadores clave de desempeño y/o factores críticos de éxito) y comparados con los niveles objetivo. Las evaluaciones a la función de servicios de información deberán ser desarrolladas en forma continua.

3.1.3 Evaluación de la satisfacción de clientes
A intervalos regulares, el responsable para la coordinación y gestión de los servicios de TI deberá efectuar mediciones de la satisfacción de los clientes con respecto a los servicios proporcionados por la función de servicios de información, con la intención de identificar deficiencias en los niveles de servicio y establecer objetivos de mejoramiento.

3.1.4 Revisión por la dirección
Deberán proporcionarse informes para ser revisados por la alta Dirección en cuanto al avance de la organización hacia las metas identificadas. Con base en la revisión, el responsable para la coordinación y gestión de los servicios de TI deberá iniciar y controlar las acciones pertinentes.

3.2 EVALUAR LO ADECUADO DEL CONTROL INTERNO

3.2.1 Monitoreo de control interno
El responsable para la coordinación y gestión de los servicios de TI deberá monitorear la efectividad de los controles internos en el curso normal de las operaciones a través de actividades administrativas y de supervisión, comparaciones, reconciliaciones y otras acciones rutinarias. Las desviaciones deberán evocar análisis y acciones correctivas.

3.2.2 Operación oportuna de controles internos
La confiabilidad en los controles internos requiere que los controles operen rápidamente para resaltar errores e inconsistencias y que éstos sean corregidos antes de que impacten a la producción y a la prestación de servicios. La información relacionada con los errores,

inconsistencias y excepciones deberá ser conservada y reportada sistemáticamente a la alta dirección.

3.2.3 Reporte sobre el nivel de control interno
El responsable para la coordinación y gestión de los servicios de TI deberá reportar información sobre niveles de control interno y excepciones a las partes afectadas para asegurar la efectividad continua de su sistema de control interno. Deberán llevarse a cabo acciones para identificar qué información es requerida a un nivel particular de toma de decisiones.

3.2.4 Seguridad de operación y aseguramiento de control interno
La garantía de seguridad operacional y el aseguramiento de control interno deberán ser establecidos a través de una "auto-auditoría" o de una auditoría independiente para examinar si la seguridad y los controles internos se encuentran operando de acuerdo con los requisitos de seguridad y control interno establecidos o implícitos. Las actividades de monitoreo continuo por parte de el responsable para la coordinación y gestión de los servicios de TI deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

3.3 OBTENCIÓN DE EVALUACION INDEPENDIENTE

3.3.1 Certificación / acreditación independiente de control y seguridad de los servicios de TI
La alta dirección deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de implementar nuevos servicios de tecnología de información que resulten críticos y obtener re-certificaciones o re-acreditaciones de estas actividades en forma una cíclica rutinaria después de haber hecho la implementación.

3.3.2 Certificación / acreditación independiente de control y seguridad de proveedores externos de servicios
La Dirección deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de utilizar proveedores de servicios de tecnología de información y obtener re-certificaciones o re-acreditaciones de estas actividades en forma cíclica rutinaria.

3.3.3 Evaluación Independiente de la efectividad de los servicios de TI
La Dirección deberá obtener una evaluación independiente sobre la efectividad de los servicios de tecnología de información en forma cíclica rutinaria.

3.3.4 Evaluación independiente de la efectividad de proveedores externos de servicios
La Dirección deberá obtener una evaluación independiente sobre la efectividad de los proveedores de servicios de tecnología de información en forma cíclica rutinaria.

3.3.5 Evaluación independiente del cumplimiento de leyes y requisitos regulatorios y compromisos contractuales
La Dirección deberá obtener un asesoría independiente sobre el cumplimiento de la función de servicios de tecnología de información con respecto a requisitos regulatorios y compromisos contractuales en forma cíclica rutinaria.

3.3.6 Evaluación independiente del cumplimiento de leyes y requisitos regulatorios y compromisos contractuales de proveedores externos de servicios
La Dirección deberá obtener una evaluación independiente sobre el cumplimiento de proveedores externos de servicios de tecnología de información con respecto a requisitos regulatorios y compromisos contractuales en forma cíclica rutinaria.

3.3.7 Competencia de la función de evaluación independiente
El responsable para la coordinación y gestión de los servicios de TI deberá asegurarse de que la función de evaluación independiente posee competencia técnica, habilidades y conocimiento necesario para desempeñar dicha función en una forma efectiva, eficiente y económica.

3.3.8 Participación proactiva de auditoría
El responsable para la coordinación y gestión de los servicios de TI deberá buscar la participación de auditoría en una forma proactiva, antes de finalizar soluciones de servicio de tecnología de información.

3.4 PROVEER AUDITORÍA INDEPENDIENTE

3.4.1 Estatutos de auditoría
La alta Dirección de la organización deberá establecer los estatutos para la función de auditoría. Este documento deberá establecer la responsabilidad, autoridad y obligaciones de la función de auditoría. Asimismo este documento deberá ser revisado periódicamente para asegurar que se mantengan la independencia, autoridad y responsabilidad de la función de auditoría.

3.4.2 Independencia
El auditor deberá ser independiente del auditado tanto en actitud como en apariencia (real y percibida). Los auditores no deberán estar relacionados con la sección o departamento que esté siendo auditado, y en la medida de lo posible, deberá también ser independiente de la propia empresa. De esta manera, la función de auditoría deberá ser suficientemente independiente del área auditada para concluir una auditoría en forma objetiva.

3.4.3 Ética y normas técnicas
La función de auditoría deberá asegurar el cumplimiento de los códigos aplicables de ética profesional (ej. Código de Ética) y estándares de auditoría (ej. normas ISO) en todo lo que lleve a cabo. El debido cuidado profesional deberá observarse en todos los aspectos del trabajo de auditoría, incluyendo el respeto de estándares aplicables sobre auditoría y tecnología de información.

3.4.4 Competencia
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que los auditores responsables de las revisiones de las actividades de los servicios de TI de la organización, sean técnicamente competentes y cuentan en forma general con las habilidades y conocimientos necesarios para desempeñar dichas revisiones en forma efectiva, eficiente y económica. El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que el personal asignado a tareas de auditoría de sistemas de información, mantiene su nivel de competencia técnica mediante un programa adecuado de educación profesional continua.

3.4.5 Planeación
La alta Dirección deberá establecer un plan de auditoría para garantizar que se obtenga un aseguramiento regular e independiente con respecto a la efectividad, eficiencia y economía de la seguridad y de los procedimientos de control interno, así como de la habilidad de la Dirección para controlar las actividades de los servicios de TI. Dentro de este plan la Dirección deberá determinar las prioridades relacionadas con la obtención de aseguramiento independiente. Los auditores deberán planear el trabajo de auditoría para alcanzar los objetivos de auditoría y cumplir con los estándares profesionales correspondientes.

3.4.6 Ejecución del trabajo de auditoría

Las auditorías deberán ser supervisadas apropiadamente para proporcionar certeza de que los objetivos de auditoría están siendo alcanzados y que los estándares profesionales de auditoría que sean aplicables están siendo observados. Los auditores deberán asegurarse de obtener evidencia suficiente, confiable, relevante y útil para alcanzar los objetivos de auditoría de forma efectiva. Los hallazgos y conclusiones de auditoría deben estar soportados por un análisis apropiado y una correcta interpretación de esta evidencia.

4 EXPLOTACION (ACTUAR)

4.1 DEFINICIÓN DE NIVELES DE SERVICIO

4.1.1 Marco de referencia para el convenio de nivel de servicio

La alta dirección deberá establecer un marco de referencia en donde presente la definición de los convenios sobre niveles formales de servicio y determine el contenido mínimo: funcionalidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, plan de contingencia/recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambio. Los usuarios y la función de servicios de información deberán contar con un convenio escrito que describa el nivel de servicio en términos cualitativos y cuantitativos. El convenio definirá las responsabilidades de ambas partes. La función de servicios de información deberá prestar la calidad y la cantidad de servicios ofrecida y los usuarios deberán ajustar los servicios solicitados a los límites acordados.

4.1.2 Aspectos sobre los convenios de nivel de servicio

Deberá lograrse un acuerdo explícito sobre los aspectos que el convenio de nivel de servicios deberá tener. El convenio de nivel de servicio deberá cubrir por lo menos los siguientes aspectos: disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados a los usuarios, plan de contingencia/ Recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambios.

4.1.3 Procedimientos de desempeño

Deberán definirse procedimientos que aseguren que la manera y responsabilidades sobre las relaciones que rigen el desempeño (por ejemplo, convenios de confidencialidad) entre todas las partes involucradas sean establecidas, coordinadas, mantenidas y comunicadas a todos los departamentos afectados.

4.1.4 Monitoreo y reporte

El responsable para la coordinación y gestión de todos los servicios de TI deberá designar a un directivo que sea responsable de monitorear y reportar los alcances de los criterios de desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento. Las estadísticas de monitoreo deberán ser analizadas oportunamente. Deberán tomarse acciones correctivas apropiadas e investigarse las fallas.

4.1.5 Revisión de convenios y contratos de nivel de servicio
El responsable para la coordinación y gestión de los servicios de TI deberá implementar un proceso de revisión regular de los convenios de nivel de servicio y de los contratos de proveedores de servicios como terceras partes.

4.1.6 Elementos sujetos a cargo
Deberán incluirse provisiones para elementos sujetos a cargo en los acuerdos de niveles de servicio para hacer posibles comparaciones y decisiones de niveles de servicio contra su costo.

4.1.7 Programa de mejoramiento del servicio
El responsable para la coordinación y gestión de los servicios de TI deberá implementar un proceso para asegurar que los usuarios y los gerentes de nivel de servicio concuerden regularmente en un programa de mejoramiento del servicio con el fin de dar seguimiento a mejoras al nivel de servicio cuyo costo esté justificado.

4.2 GESTIÓN DE SERVICIOS PRESTADOS POR TERCEROS

4.2.1 Interfases con Proveedores
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que todos los servicios prestados por terceros sean propiamente identificados y que las interfases técnicas y organizacionales con los proveedores sean documentadas.

4.2.2 Relaciones con terceros
El responsable para la coordinación y gestión de los servicios de TI deberá designar un responsable de asegurar la calidad de las relaciones con terceros.

4.2.3 Contratos con terceros
El responsable para la coordinación y gestión de los servicios de TI debe definir procedimientos específicos para asegurar que un contrato formal sea definido y acordado para cada relación de servicio con un proveedor.

4.2.4 Calificación de terceros
El responsable para la coordinación y gestión de los servicios de TI debe asegurar en forma previa a su selección, que los terceros potenciales cuentan con las calificaciones adecuadas a través de una evaluación de su capacidad para proporcionar los servicios requeridos

4.2.5 Contratos con fuentes externas
Deberán definirse procedimientos organizacionales específicos para asegurar que el contrato entre la organización y el proveedor de la administración de instalaciones esté basado en niveles de procesamiento requeridos, seguridad, monitoreo y requisitos de contingencia, así como en otras estipulaciones según sea apropiado.

4.2.6 Continuidad de servicios
Con respecto al aseguramiento de la continuidad de los servicios, el responsable para la coordinación y gestión de los servicios de TI deberá considerar el riesgo de negocios relacionado con la participación de terceros en términos de incertidumbre legal y con el concepto de interés sobre la continuidad y negociar contratos en depósito.

4.2.7 Relaciones de seguridad
Con respecto a las relaciones con los proveedores de servicios como terceras partes, el responsable para la coordinación y gestión de los servicios de TI deberá asegurar que los acuerdos de seguridad (por ejemplo, los acuerdos de no - revelación) sean identificados, declarados explícitamente y acordados, que éstos concuerden con los estándares de negocios universales y estén en línea con los requisitos legales y regulatorios, incluyendo obligaciones.

4.2.8 Monitoreo
El responsable para la coordinación y gestión de los servicios de TI deberá establecer un proceso continuo de monitoreo sobre la prestación de servicio de terceros, con el fin de asegurar el cumplimiento de los acuerdos del contrato.

4.3 ADMINISTRACIÓN DE DESEMPEÑO Y CAPACIDAD

4.3.1 Requisitos de disponibilidad y desempeño
El proceso de administración deberá asegurar que las necesidades de negocio con respecto a disponibilidad y el desempeño de los servicios de información, sean identificadas y convertidas en requisitos y características de disponibilidad.

4.3.2 Plan de disponibilidad
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar el establecimiento de un plan de disponibilidad para alcanzar, monitorear y controlar la disponibilidad de los servicios de información.

4.3.3 Monitoreo y reporte
El responsable para la coordinación y gestión de los servicios de TI deberá implementar un proceso que asegure que el desempeño de los recursos de tecnología de información sea continuamente monitoreado y que las excepciones sean reportadas de manera oportuna y completa.

4.3.4 Herramientas de modelado
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que se utilicen las herramientas de modelado apropiadas para producir un modelo del sistema actual, calibrado y ajustado según la carga de trabajo real y que sea preciso dentro de los niveles de carga recomendados. Las herramientas de modelado deberán utilizarse para apoyar el pronóstico de los requisitos de capacidad, confiabilidad de la configuración, desempeño y disponibilidad. Deberán llevarse a cabo investigaciones técnicas profundas sobre el hardware de los sistemas y deberán incluirse pronósticos acerca de futuras tecnologías.

4.3.5 Manejo proactivo del desempeño
El proceso de administración del desempeño deberá incluir la capacidad de pronóstico para permitir que los problemas sean solucionados antes de que éstos afecten el desempeño del sistema. Deberán llevarse a cabo análisis de las fallas e irregularidades del sistema en cuanto a frecuencia, v grado del impacto y magnitud del daño.

4.3.6 Pronóstico de carga de trabajo
Deberán establecerse controles para asegurar que se preparen pronósticos de carga de trabajo con el fin de identificar tendencias y proporcionar la información necesaria para el plan de capacidad.

4.3.7 Administración de capacidad de recursos
El responsable para la coordinación y gestión de los servicios de TI deberá establecer un proceso de planeación para la revisión del desempeño y capacidad del hardware con el fin de asegurar que siempre exista una capacidad justificable económicamente para procesar las cargas de trabajo acordadas y para proporcionar la cantidad y calidad de desempeño requeridas, prescritas en los acuerdos de nivel de servicio. El plan de capacidad deberá cubrir escenarios múltiples.

4.3.8 Disponibilidad de recursos
El responsable para la coordinación y gestión de los servicios de TI deberá prevenir que se pierda la disponibilidad de los recursos, mediante la implementación de mecanismos de tolerancia de fallas, mecanismos de asignación equitativa de recursos y la definición de prioridades de tareas.

4.3.9 Calendarización de recursos
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar la adquisición oportuna de la capacidad requerida, tomando en cuenta aspectos como resistencia, contingencia, cargas de trabajo y planes de almacenamiento.

4.4 ASEGURAR LA CONTINUIDAD DEL SERVICIO

4.4.1 Marco de referencia de contingencia de tecnología de información
El responsable para la coordinación y gestión de los servicios de TI deberá crear un marco de referencia de contingencia que defina los roles, responsabilidades, el enfoque basado en riesgo /la metodología a seguir y las reglas y la estructura para documentar el plan, así como los procedimientos de aprobación.

4.4.2 Estrategia y filosofía de contingencia de tecnología de información
El responsable para la coordinación y gestión de los servicios de TI deberá garantizar que el Plan de contingencia de tecnología de información se encuentra en línea con el plan general de contingencia de la empresa para asegurar consistencia. Aún más, el plan de contingencia de TI debe tomar en consideración el plan a mediano y largo plazo de tecnología de información, con el fin de asegurar consistencia.

4.4.3 Contenido del plan de contingencia de tecnología de información
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que se desarrolle un plan escrito conteniendo lo siguiente: Guías sobre la utilización del Plan de Contingencia; Procedimientos de emergencia para asegurar la integridad de todo el personal afectado; Procedimientos de respuesta definidos para regresar al negocio al estado en que se encontraba antes del incidente o desastre; Procedimientos para salvaguardar y reconstruir las instalaciones; Procedimientos de coordinación con las autoridades públicas; Procedimientos de comunicación con los interesados: empleados, clientes clave, proveedores críticos, accionistas y la dirección; e Información crítica sobre grupos de contingencia, personal afectado, clientes, proveedores, autoridades públicas y medios de comunicación.

4.4.4 Minimización de requisitos de contingencia de tecnología de información.
El responsable para la coordinación y gestión de los servicios de TI deberá establecer procedimientos y guías para minimizar los requisitos de contingencia con respecto a personal, instalaciones, hardware, software, equipo, formatos, consumibles y mobiliario.

4.4.5 Mantenimiento plan de contingencia de tecnología de información
El responsable para la coordinación y gestión de los servicios de TI deberá proveer procedimientos de control de cambios para asegurar que el plan de contingencia se mantiene actualizado y refleja requisitos de negocio actuales. Esto requiere de procedimientos de mantenimiento del plan de contingencia alineados con el cambio, la administración y los procedimientos de recursos humanos.

4.4.6 Pruebas del plan de contingencias de tecnología de información
Para contar con un plan efectivo de contingencias, la alta dirección necesita evaluar su adecuación de manera regular; esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas e implementar un plan de acción de acuerdo con los resultados.

4.4.7 Capacitación sobre el plan de contingencias de tecnología de información
La metodología de contingencias para desastres deberá asegurar que todas las partes interesadas reciban sesiones de entrenamiento regulares con respecto a los procedimientos a ser seguidos en caso de un incidente o un desastre.

4.4.8 Distribución del plan de contingencia de tecnología de información
Debido a la naturaleza sensitiva de la información del plan de contingencia, dicha información deberá ser distribuida solo a personal autorizado y mantenerse bajo adecuadas medidas de seguridad para evitar su divulgación. Consecuentemente, algunas secciones del plan deberán ser distribuidas solo a las personas cuyas actividades hagan necesario conocer dicha información.

4.4.9 Procedimientos de respaldo de procesamiento para departamentos usuarios
La metodología de contingencia deberá asegurar que los departamentos usuarios establezcan procedimientos alternativos de procesamiento, que puedan ser utilizados hasta que la función de servicios de información sea capaz de restaurar completamente sus servicios después de un evento o un desastre.

4.4.10 Recursos críticos de tecnología de información
El plan de contingencia deberá identificar los programas de aplicación, servicios de terceros, sistemas operativos, personal, insumos, archivos de datos que resultan críticos así como los tiempos necesarios para la recuperación después de que se presenta un desastre.

4.4.11 Centro de datos y hardware de respaldo
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que la metodología de contingencia incorpora la identificación de alternativas relativas al centro de datos y al hardware de respaldo, así como una selección alternativa final. En caso de aplicar, deberá establecerse un contrato formal para este tipo de servicios.

4.4.12 Procedimiento de refinamiento del plan de contingencia
Dada una exitosa reanudación de los servicios de TI después de un desastre, el responsable para la coordinación y gestión de los servicios de TI deberá establecer procedimientos para evaluar lo adecuado del plan y actualizarlo de acuerdo con los resultados de dicha evaluación.

4.5 GARANTIZAR LA SEGURIDAD DE SISTEMAS

4.5.1 Administrar medidas de seguridad
La seguridad en Tecnología de Información deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requisitos de negocio. Esto incluye: traducir

información sobre evaluación de riesgos a los planes de seguridad de tecnología; implementar el plan de seguridad de tecnología de información; actualizar el plan de seguridad de tecnología de información para reflejar cambios en la configuración de tecnología; evaluar el impacto de solicitudes de cambio en la seguridad de tecnología de información; monitorear la implementación del plan de seguridad de tecnología de información; y alinear los procedimientos de seguridad de tecnología de información a otras políticas y procedimientos

4.5.2 Identificación, autenticación y acceso
El acceso lógico y el uso de los recursos de TI deberán restringirse a través de la instrumentación de un mecanismo adecuado de autenticación de usuarios identificados y recursos asociados con las reglas de acceso. Dicho mecanismo deberá evitar que personal no autorizado, conexiones telefónicas de marcado y otros puertos de entrada del sistema (redes) tengan acceso a los recursos de cómputo, de igual forma deberá minimizar la necesidad de firmas de entrada múltiples a ser utilizadas por usuarios autorizados. Asimismo deberán establecerse procedimientos para conservar la efectividad de los mecanismos de autenticación y acceso (por ejemplo, cambios periódicos de contraseñas).

4.5.3 Seguridad de acceso a datos en línea
En un ambiente de tecnología de información en línea, el responsable para la coordinación y gestión de los servicios de TI deberá implementar procedimientos acordes con la política de seguridad que garantiza el control de la seguridad de acceso, tomando como base las necesidades individuales demostradas de visualizar, agregar, modificar o eliminar datos.

4.5.4 Administración de cuentas de usuario
El responsable para la coordinación y gestión de los servicios de TI deberá establecer procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión y suspensión de cuentas de usuario. Deberá incluirse un procedimiento de aprobación formal que indique el propietario de los datos o del sistema que otorga los privilegios de acceso.

4.5.5 Revisión por la dirección de cuentas de usuario
La alta dirección deberá contar con un proceso de control establecido para revisar y confirmar periódicamente los derechos de acceso.

4.5.6 Control de usuarios sobre cuentas de usuario
Los usuarios deberán controlar en forma sistemática la actividad de su(s) propia(s) cuenta(s). También se deberán establecer mecanismos de información para permitirles supervisar la actividad normal, así como alertarlos oportunamente sobre actividades inusuales.

4.5.7 Vigilancia de seguridad
La administración de seguridad de los servicios de TI debe asegurar que la actividad de seguridad sea registrada y que cualquier indicación sobre una inminente violación de seguridad sea notificada inmediatamente al administrador y que las acciones consecuentes sean tomadas en forma automática.

4.5.8 Clasificación de datos
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que todos los datos son clasificados en términos de sensitividad, mediante una decisión explícita y formal del dueño de los datos de acuerdo con el esquema de clasificación. Aún los datos que requieran “no protección” deberán contar con una decisión formal que les asigne dicha clasificación.

4.5.9 Clasificación de datos
Deben existir controles para asegurar que la identificación y los derechos de acceso de los usuarios, así como la identidad del sistema y la propiedad de los datos, son establecidos y administrados de forma única y centralizada, para obtener consistencia y eficiencia de un control global de acceso.

4.5.10 Reportes de violación y de actividades de seguridad
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que las violaciones y la actividad de seguridad sean registradas, reportadas, revisadas y escaladas apropiadamente en forma regular para identificar y resolver incidentes que involucren actividades no autorizadas. El acceso lógico a la información sobre el registro de recursos de cómputo (seguridad y otros registros) deberá otorgarse tomando como base el principio de menor privilegio (necesidad de saber).

4.5.11 Manejo de incidentes
El responsable para la coordinación y gestión de los servicios de TI deberá implementar la capacidad de manejar incidentes de seguridad computacional, dar atención a dichos incidentes mediante el establecimiento de una plataforma centralizada con suficiente experiencia y equipada con instalaciones de comunicación rápidas y seguras. Deberán establecerse las responsabilidades y los procedimientos de manejo de incidentes para asegurar una respuesta apropiada, efectiva y oportuna a los incidentes de seguridad.

4.5.12 Re-acreditación
La alta dirección deberá asegurar que se lleve a cabo periódicamente una re-acreditación de seguridad por ejemplo, a través de equipos de personal técnico especializado con el fin de conservar al día el nivel de seguridad aprobado formalmente y la aceptación del riesgo residual.

4.5.13 Confianza en contrapartes
Las políticas organizacionales deberán asegurar que se instrumenten prácticas de control para verificar la autenticidad de las contrapartes que proporcionan instrucciones o transacciones electrónicas. Esto puede lograrse mediante el intercambio confiable de contraseñas, dispositivos de seguridad o llaves criptográficas.

4.5.14 Autorización de transacciones
Las políticas organizacionales deberán asegurar que, en donde sea apropiado, sean instrumentados controles para proporcionar autenticidad de transacciones. Esto requiere el empleo de técnicas criptográficas para “firmar” y verificar transacciones.

4.5.15 No negación
Las políticas organizacionales deberán asegurar que, en donde sea apropiado, las transacciones no puedan ser negadas por ninguna de las partes y que se instrumenten controles para proporcionar no negación (*non repudiation*) de origen o destino, prueba de envío (*proof of submission*), y recibo de transacciones. Esto puede ser implementado a través de firmas digitales, registro de tiempos y terceros confiables.

4.5.16 Sendero seguro
Las políticas organizacionales deberán asegurar que la información de transacciones sensitivas es enviada y recibida exclusivamente a través de canales o senderos seguros (*trusted paths*). La información sensitiva incluye: información sobre administración de seguridad, datos de transacciones sensitivas, contraseñas y llaves criptográficas. Para lograr esto, se pueden

establecer canales confiables mediante el encriptamiento entre usuarios, entre usuarios y sistemas y entre sistemas.

4.5.17 Protección de funciones de seguridad
Todo el hardware y software relacionado con seguridad debe encontrarse permanentemente protegido contra intromisiones para proteger su integridad y contra divulgación de sus claves secretas. Adicionalmente, la organización deberá mantener discreción sobre el diseño de su seguridad, pero no basar la seguridad en mantener el diseño como secreto.

4.5.18 Administración de llaves criptográficas
El responsable para la coordinación y gestión de los servicios de TI deberá definir e implementar procedimientos y protocolos a ser utilizados en la generación, distribución, certificación, almacenamiento, entrada, utilización y archivo de llaves criptográficas con el fin de asegurar la protección de las mismas contra modificaciones y divulgación no autorizada. Si una llave se encuentra comprometida (en riesgo), el responsable para la coordinación y gestión de los servicios de TI deberá asegurarse de que esta información se hace llegar a todas las partes interesadas a través de un listado de revocación de certificados o mecanismos similares.

4.5.19 Prevención, detección y corrección de software "malicioso"
Con respecto al software malicioso, tal como los virus computacionales o Caballos de Troya, el responsable para la coordinación y gestión de los servicios de TI deberá establecer un marco de referencia de adecuadas medidas de control preventivas, de detección y correctivas.

4.5.20 Arquitectura de *Fire Walls* y conexión a redes públicas
Si existe conexión con Internet u otras redes públicas en la organización, se deberá contar con sistemas *Fire Wall* adecuados para proteger en contra de negación de servicios y cualquier acceso no autorizado a los recursos internos; deberá controlar en ambos sentidos cualquier flujo de administración de infraestructura y de aplicaciones y deberá proteger en contra de negación o ataques de servicio.

4.5.21 Protección de valores electrónicos
El responsable para la coordinación y gestión de los servicios de TI debe proteger consistentemente la integridad de todas las tarjetas o dispositivos físicos similares, que son utilizados para autenticación o almacenamiento de información financiera u otra información sensitiva, tomando en consideración las instalaciones relacionadas, dispositivos, empleados y métodos de validación utilizados.

4.6 IDENTIFICACIÓN Y ASIGNACIÓN DE COSTOS

4.6.1 Elementos sujetos a cargo
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que los elementos sujetos a cargo sean identificables, medibles y predecibles para los usuarios. Los usuarios deberán ser capaces de controlar el uso de los servicios de información y de los niveles de facturación asociados.

4.6.2 Procedimientos de costo
El responsable para la coordinación y gestión de los servicios de TI deberá definir e implementar procedimientos de costo para proporcionar información a la Dirección acerca del costo de prestar servicios de información, asegurando al mismo tiempo la economía. Las variaciones entre los costos pronosticados y los reales deberán ser analizadas adecuadamente y reportados, con el fin

de facilitar el monitoreo de los mismos. Además, la alta Dirección deberá evaluar periódicamente los resultados de los procedimientos de contabilidad de costos de los servicios de TI, a la luz de los otros sistemas de medición financiera de la organización.

4.6.3 Procedimientos de cargo y facturación a usuarios
El responsable para la coordinación y gestión de los servicios de TI deberá definir y utilizar procedimientos de cargo y facturación. Esta deberá mantener procedimientos de cargo y facturación que fomenten el uso apropiado de los recursos de cómputo y aseguren el trato justo de los departamentos usuarios y sus necesidades. El monto cargado deberá reflejar los costos asociados con la prestación de servicios.

4.7 EDUCACIÓN Y ENTRENAMIENTO DE USUARIOS

4.7.1 Identificación de necesidades de entrenamiento
En línea con el plan a largo plazo, el responsable para la coordinación y gestión de los servicios de TI deberá establecer y mantener procedimientos para identificar y documentar las necesidades de entrenamiento de todo el personal que haga uso de los servicios de información. Deberá establecerse un curriculum de entrenamiento para cada grupo de empleados.

4.7.2 Organización del entrenamiento
Tomando como base las necesidades identificadas, el responsable para la coordinación y gestión de los servicios de TI deberá definir los grupos objetivo, identificar y asignar entrenadores y organizar oportunamente las sesiones de entrenamiento. Asimismo, deberán investigarse las alternativas de entrenamiento (localidad interna o externa, entrenadores internos o externos).

4.7.3 Entrenamiento sobre principios y conciencia de seguridad
Todo el personal deberá estar capacitado y entrenado en los principios de seguridad de sistemas. La alta Dirección deberá proporcionar un programa de educación y entrenamiento que incluya: conducta ética de los servicios de TI, prácticas de seguridad para proteger de una manera segura contra daños que afecten la disponibilidad, la confidencialidad la integridad y el desempeño de las tareas.

4.8 APOYO Y ASISTENCIA A LOS CLIENTES DE TECNOLOGÍA DE INFORMACIÓN

4.8.1 Buró de ayuda
Deberá establecerse un soporte para usuarios dentro de una función de buró de ayuda. Las personas responsables de llevar a cabo esta función deberán interactuar estrechamente con el personal de manejo de problemas.

4.8.2 Registro de preguntas del usuario
Deberán establecerse procedimientos para asegurar que todas las preguntas de los clientes sean registradas adecuadamente por el buró de ayuda.

4.8.3 Escalamiento de preguntas del cliente
Los procedimientos del buró de ayuda deberán asegurar que las preguntas de los clientes que no puedan ser resueltas inmediatamente sean reasignadas apropiadamente dentro de los servicios de TI hasta el nivel adecuado para atenderlas.

4.8.4 Monitoreo de atención a clientes
El responsable para la coordinación y gestión de los servicios de TI deberá establecer procedimientos para monitorear oportunamente la atención a las preguntas de los clientes. Las preguntas que permanezcan pendientes por largo tiempo deberán ser investigadas y atendidas.

4.8.5 Análisis y reporte de tendencias
Deberán establecerse procedimientos que aseguren el reporte adecuado de las preguntas de los clientes y su solución, de los tiempos de respuesta y la identificación de tendencias. Los reportes deberán ser analizados y sus resultados deberán ser atendidos adecuadamente.

4.9 GESTIÓN DE LA CONFIGURACIÓN

4.9.1 Registro de la configuración
Deberán establecerse procedimientos para asegurar que sean registrados únicamente elementos de configuración autorizados e identificables en el inventario, al momento de la adquisición. Por otra parte, deberán establecerse procedimientos para dar seguimiento a los cambios en la configuración (nuevo elemento, cambio de estatus de desarrollo a prototipo). El registro en bitácoras y el control deberán ser una parte integrada del sistema de registro de configuración, incluyendo revisiones de registros modificados.

4.9.2 Configuración base
El responsable para la coordinación y gestión de los servicios de TI deberá asegurarse de que existan elementos de configuración en la línea de referencia o base como punto de verificación al cual regresar después de las modificaciones.

4.9.3 Registro de estatus
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que los registros de configuración reflejen el estatus real de todos los elementos de la configuración incluyendo la historia de los cambios.

4.9.4 Control de la configuración
Los procedimientos deberán asegurar que la existencia y consistencia del registro de la configuración de los servicios de TI sean revisadas periódicamente.

4.9.5 Software no autorizado
El responsable para la coordinación y gestión de los servicios de TI deberá revisar periódicamente la existencia de software no autorizado en las computadoras personales de la organización.

4.9.6 Almacenamiento de software
Deberá definirse un área de almacenamiento de archivos (biblioteca) para todos los elementos de software válidos en las fases apropiadas del ciclo de vida de desarrollo de sistemas. Estas áreas deberán estar separadas unas de otras y de las áreas de almacenamiento de archivos de desarrollo, pruebas y producción.

4.10 ADMINISTRACIÓN DE PROBLEMAS E INCIDENTES

4.10.1 Sistema de administración de problemas
El responsable para la coordinación y gestión de los servicios de TI deberá definir e implementar un sistema de administración de problemas para asegurar que todos los eventos operacionales que no formen parte de la operación estándar (incidentes, problemas y errores) sean registrados,

analizados y resueltos oportunamente. Deberán emitirse reportes de incidentes en el caso de problemas significativos.

4.10.2 Escalamiento de problemas
La alta dirección deberá definir e implementar procedimientos de escalamiento de problemas para asegurar que los problemas identificados sean resueltos oportunamente de la manera más eficiente. Estos procedimientos deberán asegurar que las prioridades sean establecidas apropiadamente. Los procedimientos también deberán documentar el procedimiento de escalamiento para la activación del plan de contingencia de tecnología de información.

4.10.3 Seguimiento de problemas y trazas de auditoría
El sistema de administración de problemas deberá proporcionar elementos adecuados para trazas de auditoría que permitan el seguimiento de las causas a partir de un incidente (por ejemplo, liberación de paquetes o implementación de cambios urgentes) y viceversa. Deberá trabajar estrechamente con la administración de cambios, la administración de disponibilidad y la administración de configuración.

4.11 ADMINISTRACIÓN DE DATOS

4.11.1 Procedimientos de preparación de datos
El responsable para la coordinación y gestión de los servicios de TI deberá establecer procedimientos de preparación de datos a ser seguidos por las unidades organizativas de los usuarios. En este contexto, el diseño de formas de entrada de datos deberá ayudar a minimizar los errores y las omisiones. Durante la creación de los datos, los procedimientos de manejo de errores deberán asegurar razonablemente que los errores y las irregularidades sean detectados, reportados y corregidos.

4.11.2 Procedimientos de autorización de documentos fuente
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que los documentos fuente sean preparados apropiadamente por personal autorizado que actúa dentro de su autoridad, y que se establezca una separación de funciones adecuada con respecto al origen y aprobación de documentos fuente.

4.11.3 Recopilación de datos de documentos fuente
Los procedimientos de la organización deberán asegurar que todos los documentos fuente autorizados estén completos, sean precisos, registrados apropiadamente y transmitidos oportunamente para la entrada de datos.

4.11.4 Manejo de errores de documentos fuente
Los procedimientos de manejo de errores durante la creación de datos deberán asegurar razonablemente que los errores y las irregularidades sean detectados, reportados y corregidos.

4.11.5 Retención de documentos fuente
Deberán establecerse procedimientos para asegurar que la organización pueda retener o reproducir los documentos fuentes originales durante un período de tiempo razonable para facilitar la recuperación o reconstrucción de datos, así como para satisfacer requisitos legales.

4.11.6 Procedimientos de autorización de entrada de datos
La organización deberá establecer procedimientos apropiados para asegurar que la entrada de datos sea llevada a cabo únicamente por personal autorizado.

4.11.7 Chequeos de exactitud, suficiencia y autorización
Los datos sobre transacciones, capturados para su procesamiento (generados por personas, por sistemas o entradas de interfaz) deberán estar sujetos a una variedad de controles para verificar su exactitud, suficiencia y validez. Asimismo, deberán establecerse procedimientos para asegurar que los datos de entrada sean validados y editados tan cerca del punto de origen como sea posible.

4.11.8 Manejo de errores en la entrada de datos
La organización deberá establecer procedimientos para la corrección y reenvío de datos que hayan sido capturados erróneamente.

4.11.9 Integridad de procesamiento de datos
La organización deberá establecer procedimientos para el procesamiento de datos que aseguren que la segregación de funciones sea mantenida y que el trabajo realizado sea verificado rutinariamente. Los procedimientos deberán asegurar que se establezcan controles de actualización adecuados como totales de control "corrida a corrida" y controles de actualización de archivos maestros.

4.11.10 Validación y edición de procesamiento de datos
La organización deberá establecer procedimientos para asegurar que la validación, autenticación y edición del procesamiento sean llevadas a cabo tan cerca del punto de origen como sea posible. Cuando se utilicen sistemas de Inteligencia Artificial, dichos sistemas serán ubicados en una infraestructura de control interactiva con operadores humanos para asegurar que las decisiones vitales son aprobadas.

4.11.11 Manejo de errores en el procesamiento de datos
La organización deberá establecer procedimientos de manejo de errores en el procesamiento de datos que permitan la identificación de transacciones erróneas sin que éstas sean procesadas y sin interrumpir el procesamiento de otras transacciones válidas.

4.11.12 Manejo y retención de datos de salida
La organización deberá establecer procedimientos para el manejo y la retención de datos de salida de sus programas de aplicación de tecnología de información. En caso de que instrumentos negociables (ej. tarjetas de valor) sean los receptores de la salida, se deberá poner cuidado especial en prevenir usos inadecuados.

4.11.13 Distribución de datos de salida
La organización deberá establecer y comunicar procedimientos escritos para la distribución de datos de salida de tecnología de información.

4.11.14 Balanceo y conciliación de datos de salida
La organización deberá establecer procedimientos para asegurar que los datos de salida sean balanceados rutinariamente con los totales de control relevantes. Deberán existir trazas de auditoría para facilitar el seguimiento del procesamiento de transacciones y la conciliación de los datos con problema.

4.11.15 Revisión de datos de salida y manejo de errores
La alta Dirección de la organización deberá establecer procedimientos para asegurar que la precisión de los reportes de los datos de salida sea revisada por el proveedor y por los usuarios

relevantes. Así mismo, deberán establecerse procedimientos para controlar los errores contenidos en los datos de salida.

4.11.16 Provisiones de seguridad para reportes de salida
La organización deberá establecer procedimientos para garantizar que la seguridad de los reportes de datos de salida sea mantenida para todos aquellos reportes que estén por distribuirse, así como para todos aquéllos que ya hayan sido distribuidos a los usuarios.

4.11.17 Protección de información sensible durante transmisión y transporte
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que durante la transmisión y transporte de información sensible, se proporcione una adecuada protección contra acceso o modificación no autorizada, así como contra envíos a direcciones erróneas.

4.11.18 Protección de información crítica a ser desechada
El responsable para la coordinación y gestión de los servicios de TI deberá definir e implementar procedimientos para impedir la divulgación indebida o el desecho de información delicada de la organización. Tales procedimientos deberán garantizar que ninguna información marcada como "borrada" o "desechada", pueda ser accedida por personas internas o externas a la organización.

4.11.19 Administración de almacenamiento
Deberán desarrollarse procedimientos para el almacenamiento de datos que consideren requisitos de recuperación, de economía y las políticas de seguridad.

4.11.20 Períodos de retención y términos de almacenamiento
Deberán definirse los períodos de retención y los términos de almacenamiento para documentos, datos, programas, reportes y mensajes (de entrada y de salida), así como los datos (claves, certificados) utilizados para su encriptamiento y autenticación.

4.11.21 Sistema de administración de la librería de medios
La función de servicios de información deberá establecer procedimientos para asegurar que el contenido de su librería de medios sea inventariado sistemáticamente, que cualquier discrepancia revelada por un inventario físico sea solucionada oportunamente y que se lleven a cabo las medidas necesarias para mantener la integridad de los medios magnéticos almacenados en la librería.

4.11.22 Responsabilidades de la administración de la librería de medios
El responsable para la coordinación y gestión de los servicios de TI deberá establecer procedimientos de administración para proteger el contenido de la librería de medios. Deberán definirse estándares para la identificación externa de medios magnéticos y el control de su movimiento y almacenamiento físico para soportar su seguimiento y registro. Las responsabilidades sobre el manejo de la librerías de medios (cintas magnéticas, cartuchos, discos y diskettes) deberán ser asignadas a miembros específicos del personal de servicios de información.

4.11.23 Respaldo y restauración
El responsable para la coordinación y gestión de los servicios de TI deberá implementar una estrategia apropiada de respaldo y restauración para asegurar que ésta incluya una revisión de los requisitos de la entidad, así como el desarrollo, implementación, prueba y documentación del plan de recuperación. Se deberán establecer procedimientos para asegurar que los respaldos satisfagan los requisitos mencionados anteriormente.

4.11.24 Funciones de respaldo
Deberán establecerse procedimientos para asegurar que los respaldos sean realizados de acuerdo con la estrategia de respaldo definida, y que su utilidad sea verificada regularmente.

4.11.25 Almacenamiento de respaldos
Los procedimientos de respaldo para los medios relacionados con tecnología de información deberán incluir el almacenamiento apropiado de los archivos de datos, del software y de la documentación relacionada, tanto dentro como fuera de las instalaciones. Los respaldos deberán ser almacenados con seguridad y las instalaciones de almacenamiento deberán ser revisadas periódicamente con respecto a la seguridad de acceso físico y la seguridad de los archivos de datos y otros elementos.

4.11.26 Archivo
La alta dirección deberá implementar una política y procedimientos para asegurar que el archivo cumple con requisitos legales y de negocio y que se encuentra debidamente protegido y registrado adecuadamente.

4.11.27 Protección de mensajes sensitivos
Con respecto a la transmisión de datos a través de Internet u otra red pública, El responsable para la coordinación y gestión de los servicios de TI deberá definir e implementar procedimientos y protocolos para ser utilizados para el aseguramiento de la integridad, confidencialidad y “no repudio” de mensajes sensitivos.

4.11.28 Autenticación e Integridad
Previamente a que alguna acción crítica sea tomada sobre información originada fuera de la Organización que se reciba vía teléfono, correo de voz, documentos (en papel), fax o correo electrónico, se deberá verificar adecuadamente la autenticidad e integridad de dicha información.

4.11.29 Integridad de transacciones electrónicas
Tomando en consideración que las fronteras tradicionales de tiempo y de geografía son menos precisas y confiables, El responsable para la coordinación y gestión de los servicios de TI deberá definir e implementar apropiados procedimientos y prácticas para transacciones electrónicas que sean sensitivas y críticas para la Organización, asegurando la integridad y autenticidad de: atomicidad (unidad de trabajo indivisible, todas sus acciones tienen éxito o todas ellas fallan) consistencia (si la transacción no logra alcanzar un estado final estable, deberá regresar al sistema a su estado inicial); aislamiento (el comportamiento de una transacción no es afectado por otras transacciones que se ejecutan concurrentemente); y durabilidad (los efectos de una transacción son permanentes después que concluye su proceso, los cambios que origina deben sobrevivir fallas de sistema)

4.11.30 Integridad continua de datos almacenados
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que la integridad y lo adecuado de los datos mantenidos en archivos y otros medios (ej. tarjetas electrónicas) se verifique periódicamente. Atención específica deberá darse a dispositivos de valor, archivos de referencia y archivos que contengan información privada.

4.12 ADMINISTRACIÓN DE INSTALACIONES

4.12.1 Seguridad física

Deberán establecerse apropiadas medidas de seguridad física y control de acceso para las instalaciones de tecnología de información de acuerdo con la política de seguridad general, incluyendo el uso de dispositivos de información fuera de las instalaciones. El acceso deberá restringirse a las personas que hayan sido autorizadas a contar con dicho acceso.

4.12.2 Discreción de las instalaciones de tecnología de información
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que se lleve un bajo perfil ó discreción y que la identificación física de las instalaciones relacionadas con sus operaciones de tecnología de información sea limitada.

4.12.3 Escolta de visitantes
Deberán establecerse procedimientos apropiados que aseguren que las personas que no formen parte del grupo de operaciones de los servicios de TI sean escoltadas por algún miembro de ese grupo cuando deban entrar a las instalaciones de cómputo. Deberá mantenerse y revisarse regularmente una bitácora de visitantes.

4.12.4 Salud y seguridad del personal
Deberán establecerse y mantenerse prácticas de salud y seguridad en línea con las leyes y regulaciones internacionales, nacionales, regionales, estatales y locales.

4.12.5 Protección contra factores ambientales
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que se establezcan y mantengan las suficientes medidas para la protección contra los factores ambientales (por ejemplo, fuego, polvo, electricidad, calor o humedad excesivos). Deberán instalarse equipo y dispositivos especializados para monitorear y controlar el ambiente.

4.12.6 Suministro ininterrumpido de energía
El responsable para la coordinación y gestión de los servicios de TI deberá evaluar y proponer a la alta dirección regularmente la necesidad de generadores y baterías de suministro ininterrumpido de energía para las aplicaciones críticas de tecnología de información, con el fin de asegurarse contra fallas y fluctuaciones de energía. Cuando sea justificable, deberá instalarse el equipo más apropiado.

4.13 ADMINISTRACIÓN DE OPERACIONES

4.14.1 Manual de procedimientos de operación e instrucciones
La función de servicios de información deberá establecer y documentar procedimientos estándar para las operaciones de tecnología de información (incluyendo operaciones de red). Todas las soluciones y plataformas de tecnología de información establecidas deberán ser operadas utilizando estos procedimientos, los cuales deberán ser revisados periódicamente para asegurar su efectividad y cumplimiento.

4.13.2 Documentación del proceso de inicio y de otras operaciones
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que el personal de operaciones esté adecuadamente familiarizado y se sienta seguro con las tareas del proceso de inicio y con otras operaciones al tenerlas documentadas y al ser éstas probadas y ajustadas periódicamente según se requiera.

4.13.3 Calendarización de trabajos
El responsable para la coordinación y gestión de los servicios de TI deberá asegurar que la calendarización continua de trabajos, procesos y tareas sea organizada en la secuencia más eficiente, maximizando el proceso y la utilización, con el fin de alcanzar los objetivos establecidos en los convenios de nivel de servicio. Las calendarizaciones iniciales así como los cambios a estas calendarizaciones deberán ser autorizadas apropiadamente.

4.13.4 Salidas de la calendarización de trabajos estándar
Deberán establecerse procedimientos para identificar, investigar y aprobar las salidas de calendarización de trabajos estándar.

4.13.5 Continuidad de procesamiento
Los procedimientos deberán requerir continuidad de procesamiento durante los cambios de turno de operadores mediante la existencia de un paso o entrega formal de actividades, actualizaciones y reportes de estatus sobre las responsabilidades actuales.

4.13.6 Bitácoras de operación
Los controles de la Dirección deberán garantizar que se esté almacenando suficiente información cronológica en bitácoras de operaciones para permitir la reconstrucción, la revisión y el examen oportunos de las secuencias de tiempo de procesamiento y otras actividades que lo rodean y soportan.

4.13.7 Operaciones remotas
Para las operaciones remotas, deberán existir procedimientos específicos que aseguren que la conexión y desconexión de los enlaces con la(s) instalación(es) remota(s) sean identificadas e implementadas.