NORMA CUBANA

NC

ISO/IEC 20000-2: 2011
(Publicada por la ISO en 2005)

TECNOLOGÍAS DE LA INFORMACIÓN — GESTIÓN DEL SERVICIO — PARTE 2: CÓDIGO DE BUENAS PRÁCTICAS (ISO/IEC 20000-2: 2005, IDT)

Information technology — Service management — Part 2: Code of good practice

ICS: 01.040.35

1. Edición Diciembre 2011

Oficina Nacional de Normalización (NC) Calle E No. 261 El Vedado, 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)
  - Oficina de Informatización de la Sociedad
  - Oficina de Seguridad de las Redes Informáticas
  - SEGURMATICA
  - Oficina Nacional de Normalización

- Es una adopción idéntica de la norma ISO/IEC 20000-2:2005 *Information technology. Service management. Part 2: Code of Practice,* e incorpora a la norma adoptada el Anexo A, que contiene conceptos metodológicos ampliamente empleados, en cuanto a la provisión de los servicios a los clientes internos y externos de la informática, a fin de su utilización a modo de información directiva complementaria para la implantación de la norma en las entidades, propiciando el control, inspección y auditoría a las mismas.

Índice

0 Introducción

Esta parte de la Norma ISO/IEC 20000, al tratarse de un código de buenas prácticas, tiene la forma de guía y recomendaciones. No se debería citar como si fuera una especificación y se debería tener especial cuidado para asegurar que las afirmaciones sobre su cumplimiento no son engañosas.

Esta parte de la Norma ISO/IEC 20000 se debería usar junto con la Norma ISO/IEC 20000-1 dado que esta última contiene las especificaciones asociadas a este código de buenas prácticas.

Se asume que la ejecución de las disposiciones de esta parte de la Norma ISO/IEC 20000 se confía a personal compe-tente y adecuadamente cualificado. Una norma internacional no pretende incluir todas las disposiciones de un contrato. Los usuarios de las normas internacionales son los responsables de su correcta aplicación.

La conformidad con una norma internacional no confiere por si misma inmunidad frente a las obligaciones legales.

Esta parte de la Norma ISO/IEC 20000 describe las mejores prácticas para los procesos de gestión del servicio dentro del alcance de la Norma ISO/IEC 20000-1.

La provisión del servicio adquiere mayor importancia a medida que los clientes requieren servicios cada vez más avanza-dos (al mínimo costo) para satisfacer las necesidades de sus negocios. Este hecho reconoce a su vez que los servicios y la gestión de estos servicios son esenciales para ayudar a las organizaciones a generar ingresos y ser rentables.

La Norma ISO/IEC 20000-1 contiene especificaciones para la gestión de los servicios y se debería leer conjuntamente con esta parte de la Norma ISO/IEC 20000.

La serie de Normas ISO/IEC 20000 posibilita a los proveedores del servicio entender cómo mejorar la calidad del servicio que proporcionen a sus clientes ya sean clientes internos o externos.

Los proveedores del servicio pueden tener dificultades para mantener niveles altos de servicio al cliente debido a las crecientes dependencias existentes entre el soporte de los servicios y el amplio rango de tecnologías disponibles. Al trabajar de forma reactiva, los proveedores emplean muy poco tiempo en la planificación, formación, revisión, investigación y el trabajo junto con los clientes. El resultado de todo esto es el fracaso en la adopción de prácticas de trabajo estructuradas y proactivas.

Se está demandando a estos mismos proveedores del servicio mejorar la calidad, reducir los costos, dar mayor flexibili-dad y una respuesta más rápida a los clientes. La gestión efectiva del servicio proporcione a los clientes altos niveles de servicio y de satisfacción.

La serie de Normas ISO/IEC 20000 hace una distinción entre las mejores prácticas de los procesos, que son indepen-dientes del tamaño, forma, estructuras y nombres que adopten las organizaciones. La serie de Normas ISO/IEC 20000 se aplica igualmente a proveedores del servicio grandes y pequeños, y los requisitos asociados a estas mejores prácticas de los procesos de gestión del servicio no cambian en función de la forma de la organización que proporciona el marco de gestión en que dichos procesos son realizados.

TECNOLOGÍAS DE LA INFORMACIÓN — GESTIÓN DEL SERVICIO — PARTE 2: CÓDIGO DE BUENAS PRÁCTICAS

1 Objeto y campo de aplicación

Esta parte de la Norma ISO/IEC 20000 representa un consenso de la industria respecto a las normas de calidad para los procesos de gestión del servicio de TI. Estos procesos de gestión del servicio proporcionan el mejor servicio posible para cubrir las necesidades de negocio del cliente, con los niveles acordados de recursos, esto es, un servicio profesional, rentable y con riesgos asociados que son conocidos y gestionados.

La variedad de términos que se usan para el mismo proceso, y entre procesos y grupos funcionales (y cargos organizativos), puede hacer que el tema de la gestión del servicio sea confuso para un directivo nuevo. No entender la terminología puede ser una barrera para crear procesos eficaces. Entender la terminología es un beneficio tangible y significativo que proporcionan las Normas ISO/IEC 20000. Esta parte de la Norma ISO/IEC 20000 recomienda que los proveedores del servicio adopten una terminología común y un enfoque más consistente de la gestión del servicio; establece unas bases comunes para la mejora de los servicios. También proporciona un marco de referencia para ser usado por proveedores de herramientas de gestión del servicio.

Al tratarse de una norma basada en procesos, este código de prácticas no pretende ser usado para una evaluación de producto. Sin embargo, las organizaciones que desarrollen herramientas, productos y sistemas de gestión de servicios pueden usar las dos partes de la serie ISO/IEC 20000, las especificaciones y el código de buenas prácticas para ayudar al desarrollo de herramientas, productos y sistemas que soporten las mejores prácticas de la gestión del servicio.

Esta parte de la Norma ISO/IEC 20000 proporciona una guía para los auditores y ofrece asesoría a los proveedores del servicio para la planificación de las mejoras del servicio o para ser auditados conforme a la Norma ISO/IEC 20000-1.

La Norma ISO/IEC 20000-1 especifica una serie de procesos de gestión del servicio relacionados como se muestra en la figura 1.

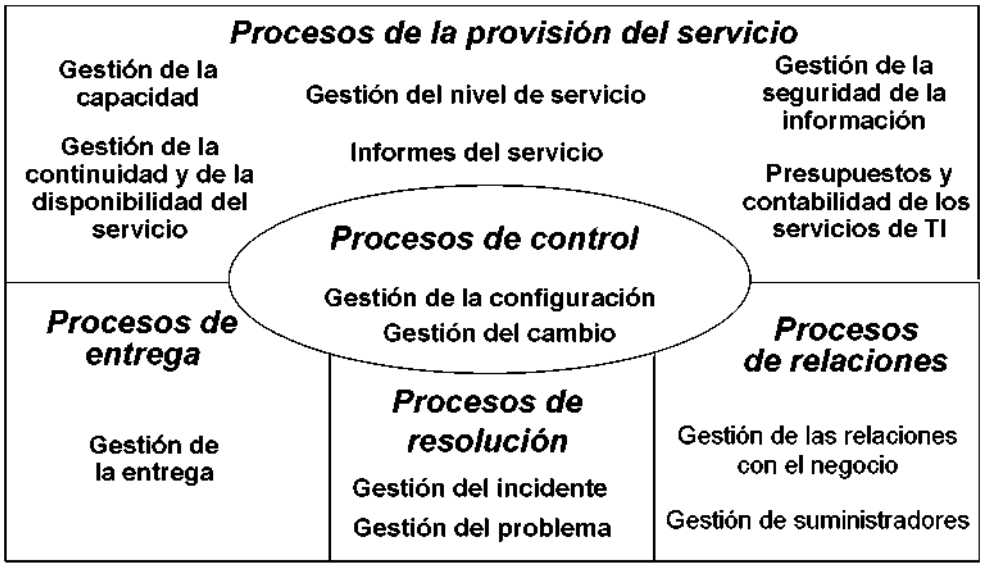

Figura 1 — Procesos de la gestión del servicio

2Términos y definiciones

Para los fines de este documento son aplicables los términos y definiciones dados en la norma iso/iec 20000-1.

3 El sistema de gestión

Objetivo: Proveer un sistema de gestión, incluyendo las políticas y un marco de trabajo para posibilitar la efectiva gestión e implementación de todos los servicios TI.

3.1 Responsabilidad de la dirección

El papel de la dirección para asegurar que las mejores prácticas son adoptadas y mantenidas en los procesos es fundamental para cualquier proveedor del servicio que quiera cumplir con los requisitos de la Norma ISO/IEC 20000-1.

Para asegurar el compromiso de la dirección se debería identificar un responsable a nivel de alta dirección como responsable de los planes de gestión del servicio. Este responsable senior debería responsabilizarse de la entrega a todos los niveles del plan de gestión del servicio.

El rol de responsable senior debería ser estar al frente de los recursos designados para las actividades de mejora del servicio, bien sean actividades continuas o con un enfoque de proyecto.

El responsable senior debería estar apoyado por un grupo encargado de la toma de decisiones que tenga la suficiente autoridad para definir la política y para hacer cumplir sus decisiones.

3.2 Requisitos de la documentación

El responsable debería asegurar que las evidencias necesarias están disponibles para una auditoria de las políticas, planificaciones y procedimientos de la gestión del servicio y de cualquier actividad relacionada con ellos.

Gran parte de las evidencias de los planes y operaciones de la gestión del servicio se deberían encontrar en forma de documentos, los cuales pueden ser de cualquier tipo y estar en cualquier formato o soporte que sea adecuado para su fin.

Los siguientes documentos son considerados normalmente como válidos para servir de evidencias de la planificación de la gestión del servicio:

a) políticas y planes;

b) documentación del servicio;

c) procedimientos;

d) procesos;

e) registros de control de procesos.

Debería existir un proceso para la creación y gestión de los documentos para ayudar a asegurar que se satisfacen las características descritas.

La documentación se debería proteger de daños, debidos, por ejemplo, a escasas condiciones del entorno donde se encuentran y a desastres en los sistemas informáticos.

3.3 Competencia, concienciación y formación

3.3.1 Generalidades

El personal que realiza el trabajo relativo a la gestión del servicio debería ser competente para esta función gracias a la educación recibida, a la formación, las habilidades y la experiencia adecuadas.

El proveedor del servicio debería:

a) determinar las aptitudes necesarias para cada rol en la gestión del servicio;

b) asegurar que el personal es consciente de la relevancia e importancia de sus actividades dentro del más amplio contexto de negocio y de cómo contribuyen a la consecución de los objetivos de calidad;

c) mantener registros apropiados de la educación, formación, habilidades y experiencia;

d) proveer formación o llevar a cabo otras acciones para satisfacer estas necesidades;

e) evaluar la efectividad de las acciones realizadas.

3.3.2 Desarrollo profesional

El proveedor del servicio debería desarrollar y mejorar las competencias profesionales de su fuerza de trabajo. Entre las medidas tomadas para conseguir esto, el proveedor del servicio debería incluir lo siguiente:

a) **contratación:** con el objetivo de comprobar la validez de los detalles de los candidatos al puesto de trabajo (inclu-yendo su cualificación profesional) y de identificar la fortalezas, debilidades y habilidades potenciales de los candidatos frente a una descripción/perfil del puesto de trabajo, frente a los objetivos de la gestión del servicio y frente al conjunto de objetivos de la calidad del servicio;

b) **planificación:** con el objetivo de dotar de personal a los servicios nuevos o a aquellos que se hayan ampliado (también contratando servicios), usando tecnología nueva, asignando personal de gestión del servicio a los equipos de desarrollo de proyecto, planificando la sucesión y rellenando los vacíos que se generen debido a rotación anticipada del personal;

c) **formación y desarrollo:** con el objetivo de identificar los requisitos de formación y desarrollo dentro de un plan de formación y desarrollo y proveer su impartición en el momento oportuno y de forma efectiva.

Se debería formar al personal en los aspectos relevantes de la gestión del servicio (por ejemplo, a través de cursos de formación, auto estudio, tutorías y formación en el trabajo) y se debería desarrollar el trabajo en equipo y las habilida-des de liderazgo. Se debería mantener un registro cronológico de la formación para cada persona, junto con las descripciones de la formación proporcionada.

3.3.3 Enfoques a considerar

Para que los equipos de personal alcancen unos niveles apropiados de competencia, el proveedor del servicio debería decidir cual es la proporción óptima entre las contrataciones a corto plazo y de forma indefinida. El proveedor del servi-cio debería decidir también la proporción a alcanzar entre la contratación de nuevo personal con las habilidades requeridas y el reciclaje de personal ya existente.

NOTA El equilibrio óptimo entre las contrataciones a corto plazo y de forma indefinida es particularmente importante cuando el proveedor del servicio está planificando como proveer un servicio durante y después de cambios a gran escala en el número y habilidades del personal de apoyo.

Los factores que se deberían considerar para establecer la combinación más adecuada de estos enfoques

incluyen:

a) el carácter de las competencias nuevas o modificadas: si son a corto o a largo plazo;

b) la tasa de cambio en las habilidades y competencias;

c) los picos y los descensos esperados en la carga de trabajo y la combinación de habilidades requeridas, datos basados en la gestión del servicio y en la planificación de las mejoras del servicio;

d) disponibilidad de personal competente;

e) tasas de rotación de personal;

f) planes de formación.

Para todo el personal, el proveedor del servicio debería revisar el desempeño a nivel individual al menos anualmente y tomar las acciones oportunas.

4 Planificación e implementación de la gestión del servicio

4.1 Planificación de la gestión del servicio (Planificar)

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

4.1.1 Alcance de la gestión del servicio

El alcance de la gestión del servicio se debería definir como parte del plan de gestión del servicio. Por ejemplo, puede definirse según:

a) la organización;

b) la ubicación;

c) el servicio.

La dirección debería definir el alcance como parte de sus responsabilidades de gestión (y como parte del plan de gestión del servicio). Luego se debería comprobar si el alcance resulta adecuado para la Norma ISO/IEC 20000-1.

NOTA La planificación de los cambios operativos se describe en el apartado 9.2.

4.1.2 Enfoques de la planificación

Se pueden utilizar varios planes de gestión del servicio en lugar de un plan o programa de gran magnitud. En este caso, los procesos subyacentes a la gestión del servicio deberían ser coherentes entre ellos. También se debería poder demos-trar cómo se gestiona cada requisito de planificación vinculándolo a sus correspondientes funciones, responsabilidades y procedimientos.

La planificación de la gestión del servicio debería formar parte del proceso para convertir las necesidades de los clientes y las intenciones de los directivos en servicios y para proporcionar una guía para dirigir el progreso.

Un plan de gestión del servicio debería incluir:

a) la implementación de la gestión del servicio (o de parte de la gestión del servicio);

b) la entrega de los procesos de la gestión del servicio;

c) los cambios de los procesos de la gestión del servicio;

d) las mejoras de los procesos de la gestión del servicio;

e) los nuevos servicios (hasta el punto que afecten a los procesos incluidos en el alcance acordado de la gestión del servicio).

4.1.3 Eventos a considerar

El plan de gestión del servicio debería estar enfocado a los procesos de gestión del servicio y a los cambios en los servicios desencadenados por eventos como los siguientes:

a) la mejora del servicio;

b) los cambios en el servicio;

c) la normalización de infraestructuras;

d) los cambios de la legislación;

e) las modificaciones de normativas como, por ejemplo, modificaciones de las tasas impositivas locales;

f) la liberalización o la regulación de los sectores industriales;

g) las fusiones y las adquisiciones.

4.1.4 Alcance y contenidos del Plan

Un plan de gestión del servicio debería definir:

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

b) los objetivos y requisitos que se pretenden conseguir con la gestión del servicio;

c) los recursos, instalaciones y presupuestos necesarios para conseguir los objetivos definidos;

d) la estructura de las funciones y las responsabilidades de gestión, incluyendo al responsable senior, a los gerentes de los procesos y a la gestión de suministradores;

d) las interfaces entre los procesos de la gestión del servicio y el modo en que se deberían coordinar los procesos y/o las actividades;

e) el enfoque que se debería aplicar para la identificación, la evaluación y la gestión de riesgos para la consecución de los objetivos definidos;

f) una planificación de los recursos expresada en términos de las fechas en las que deberían estar disponibles las fuen-tes de financiación, las habilidades y los recursos;

h) el enfoque para la modificación del plan y de los servicios definidos por el plan;

i) el modo en que el proveedor del servicio demostrará la continuidad del control de calidad continuo (por ejemplo, auditorías internas);

j) los procesos que se van a ejecutar;

k) las herramientas apropiadas para soportar los procesos

4.2 Implementación de la gestión del servicio y la provisión del servicio (Hacer)

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

La consecución de los procesos de mejores prácticas de gestión de servicios capaces de satisfacer los requisitos de la Norma ISO/IEC 20000 no se alcanzará si los servicios originales no cumplen los requisitos descritos para la implementación en la Norma ISO/IEC 20000-1.

Una vez implementados tanto el servicio como los procesos de gestión de servicios se deberían mantener.

Se deberían realizar revisiones de acuerdo con el apartado 4.3.

NOTA Es posible que la persona que sea adecuada para realizar la planificación y la implementación inicial no sea la apropiada para la operación continua.

4.3 Monitorización, medición y revisión (Verificar)

Objetivo: Monitorizar, medir y revisar que se alcanzan los objetivos de la gestión del servicio y del plan.

El proveedor del servicio debería planificar e implementar la monitorización, la medición, el análisis y la revisión de los servicios, los procesos de gestión del servicio y los sistemas asociados. Entre los elementos que se deberían monitorizar, medir y revisar están los siguientes:

a) los logros respecto a los objetivos de servicio definidos;

b) la satisfacción del cliente;

c) la utilización de los recursos;

d) las tendencias;

e) las no conformidades de mayor consideración;

Los resultados del análisis deberían proporcionar una entrada a un plan para la mejora del servicio.

Además de las actividades de gestión del servicio relativas a la medición y el análisis, es posible que la alta dirección necesite recurrir a auditorías internas y a otros tipos de verificaciones. Al decidir la frecuencia de dichas auditorías internas y verificaciones, se deberían tener en cuenta, entre otros, factores como el nivel de riesgo implicado en un proceso, su frecuencia de realización y su historial de problemas pasados. Las auditorías internas y las verificaciones se deberían planificar, registrar y llevarse a cabo de una manera competente.

4.4 Mejora continua (Actuar)

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

4.4.1 Política

Los proveedores del servicio deberían reconocer que siempre existe la posibilidad de conseguir que la provisión del servicio sea más eficaz y más eficiente. Debería hacerse pública una política de la calidad y de mejora del servicio. Todas las personas implicadas en la gestión del servicio y la mejora del servicio deberían ser conscientes de la política de calidad del servicio y de cuál debería ser su contribución personal a la consecución de los objetivos establecidos en esta política.

En particular, todo el personal del proveedor del servicio implicado en la gestión del servicio debería tener un conocimiento detallado de las repercusiones de estos factores sobre los procesos de gestión del servicio.

Debería existir una coordinación eficaz entre la estructura de gestión propia del proveedor del servicio, los clientes y los suministradores del proveedor del servicio a la hora de tratar cuestiones que afecten a la calidad del servicio y a los requisitos del cliente.

4.4.2 Planificación de mejoras del servicio

Los proveedores del servicio deberían adoptar un enfoque metódico y coordinado para cumplir con los requisitos de la política desde su propia perspectiva y desde la perspectiva del cliente.

Antes de implementar un plan de mejora del servicio, se deberían registrar los niveles de servicio y la calidad del servicio como línea de referencia sobre la que se puedan comparar las mejoras reales. Para evaluar la eficacia del cambio se debería comparar la mejora real con la mejora prevista.

NOTA 1 Los requisitos para la mejora del servicio pueden venir de todos los procesos.

Los proveedores del servicio deberían animar a su personal y a sus clientes a proponer alternativas para mejorar los servicios.

NOTA 2 Esto se puede conseguir utilizando esquemas de sugerencias, círculos de calidad, grupos de usuarios y reuniones de coordinación.

Los objetivos de la mejora del servicio deberían ser medibles, estar vinculados con los objetivos de negocio y estar documentados en un plan.

La mejora del servicio se debería gestionar de una manera activa y se debería supervisar el progreso tomando como referencia los objetivos formalmente acordados.

5 Planificación e implementación de nuevos servicios, o de servicios modificados

Objetivo: Asegurar que, tanto los servicios nuevos, como las modificaciones a los servicios existentes, serán gestiona-dos y entregados con los costos y la calidad acordados.

5.1 Temas a considerar

La planificación de los nuevos servicios o de los servicios modificados debería incluir la revisión de los siguientes aspectos:

a) los presupuestos;

b) llos recursos de personal;

c)los niveles de servicio existentes;

d) los SLAs y otros objetivos o compromisos del servicio;

e) los procesos de gestión del servicio, procedimientos y documentación existentes;

f) el enfoque de la gestión del servicio, incluyendo la implementación de los procesos de gestión del servicio que hubieran sido previamente excluidos del enfoque.

5.2 Registros de los cambios

Todas las modificaciones al servicio se deberían reflejar en los registros de gestión del cambio:

Esto incluye a los planes para:

a) la contratación y formación del personal;

b) la reubicación;

c) la formación al usuario;

d) las comunicaciones sobre los cambios;

e) los cambios en la naturaleza de la tecnología a la que se da soporte;

f) el cierre formal de los servicios.

6 Procesos de la provisión del servicio

6.1 Gestión de nivel de servicio

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

6.1.1 Catálogo de servicios

Todos los servicios deberían estar definidos en un catálogo de servicios. Este catálogo puede ser referenciado desde el SLA y debería utilizarse para recoger aquellos aspectos considerados como demasiado cambiantes para ser introducidos en el SLA.

El catálogo de servicios debería ser mantenido y estar actualizado en todo momento.

NOTA El catálogo de servicios puede incluir información genérica como:

a) el nombre del servicio,

b) los objetivos (por ejemplo tiempo de respuesta o de instalación de una impresora, tiempo para reiniciar un servicio tras un fallo importante),

c) datos de contacto,

d) horario del servicio y excepciones,

e) disposiciones de seguridad.

El catálogo de servicios en un documento clave para establecer las expectativas del cliente y debería ser fácilmente accesible y estar ampliamente disponible tanto para los clientes como para el personal de apoyo.

6.1.2 Acuerdos de nivel de servicio (SLAs)

Todo servicio debería estar formalmente documentado en un acuerdo de nivel de servicio (SLA). El SLA debería ser autorizado formalmente por la dirección del cliente y los representantes del proveedor del servicio. El SLA debería estar sujeto a la gestión del cambio, así como el servicio que describe.

El presupuesto y las necesidades del cliente deberían ser los elementos en que se base el contenido, la estructura y los objetivos del SLA. Los objetivos, respecto de los cuales debería medirse el servicio prestado, se deberían definir desde la perspectiva del cliente.

Los SLAs deberían incluir únicamente un conjunto adecuado de objetivos para centrar la atención en los aspectos más importantes del servicio.

NOTA 1 Demasiados objetivos pueden generar confusión y conllevar un exceso de gastos.

El contenido mínimo que debería tener un SLA, o que se debería referenciar desde él, es el siguiente:

a) descripción breve del servicio;

b) periodo de validez y/o mecanismo de control de cambios del SLA;

c) detalles sobre la autorización;

d) descripción breve de las comunicaciones, incluida la generación de informes;

e) datos de contacto de las personas autorizadas a actuar ante emergencias, participar en la resolución de incidentes y problemas, así como en la recuperación del servicio o en la aplicación de soluciones temporales;

f) horario de servicio, por ejemplo de 9:00 h a 17:00 h, y excepciones al mismo (por ejemplo fines de semana o periodos vacacionales), periodos críticos para el negocio y cobertura fuera del horario;

g) interrupciones planificadas y acordadas, incluido el aviso que se debe dar y el número por periodo;

h) responsabilidades del cliente, por ejemplo seguridad;

i) responsabilidades y obligaciones del proveedor del servicio, por ejemplo seguridad;

j) directrices sobre impactos y prioridades;

k) procesos de escalado y de notificación;

l) procedimientos de reclamación;

m) objetivos del servicio;

n) límites de la carga de trabajo (superior e inferior), por ejemplo la capacidad del servicio de soportar un número acordado de clientes o un volumen de trabajo o la capacidad de procesamiento del sistema;

o) detalles de alto nivel de la gestión financiera, por ejemplo códigos de imputación, etc.;

p) acciones a llevar a cabo en caso de interrupción del servicio;

q) procedimientos de mantenimiento interno;

r) glosario de términos;

s) servicios de soporte y otros relacionados con el propio servicio;

t) las excepciones a las cláusulas incluidas en el SLA.

NOTA 2 La información volátil o común a varios SLAs (como datos de contacto) se pueden referenciar desde el SLA sin que esto suponga un impacto en la calidad de los procesos de SLM siempre que los documentos de referencia estén también bajo el control del proceso de gestión del cambio.

NOTA 3 En el SLA se suele hacer referencia al plan de continuidad y a los detalles de la contabilidad y del presupuesto.

NOTA 4 El glosario de términos normalmente suele ser único y común a todos los documentos, incluyendo el catálogo de servicios.

6.1.3 El proceso de gestión de nivel de servicio

Los cambios importantes en el negocio, debidos, por ejemplo, al crecimiento, fusiones y reorganizaciones del negocio, y los cambios en los requisitos del cliente, pueden implicar el ajuste de los niveles de servicio, su redefinición o incluso su suspensión temporal. El proceso de SLM debería ser flexible para adecuarse a estos cambios. El proceso de SLM debería asegurar que el proveedor del servicio continua focalizado en el cliente durante la planificación, implantación y la gestión continua del servicio prestado.

Se le debería dar al proveedor del servicio la información adecuada para permitirle que comprenda las motivaciones y requisitos del negocio del cliente.

El proceso de SLM debería gestionar y coordinar a quienes contribuyen al nivel de servicio, para incluir:

a) acuerdo en los requisitos del servicio y en las características de la carga de trabajo esperada del servicio;

b) acuerdo en los objetivos de servicio;

c) medición e informe de los niveles de servicio conseguidos, cargas de trabajo y explicaciones cuando no se alcanzan los objetivos acordados;

d) inicio de la acción correctiva;

e) entrada al programa de mejora del servicio.

El proceso debería animar tanto al proveedor del servicio como al cliente a desarrollar una actitud proactiva con objeto de garantizar que ambos tienen una responsabilidad compartida sobre el servicio.

La satisfacción del cliente es una parte importante de la gestión de nivel de servicio pero debería reconocerse que es una medida subjetiva, mientras que los objetivos de servicio incluidos en el SLA deberían ser medidas objetivas. El proceso de SLM debería trabajar conjuntamente con los procesos de gestión de relaciones con el negocio y gestión de suministradores.

6.1.4 Acuerdos de servicio de soporte

Los servicios de soporte de los cuales depende el servicio prestado se deberían documentar y acordar con cada suminis-trador de servicios. Esto incluye los grupos internos que proveen parte del servicio ofrecido por el proveedor del servicio.

6.2 Generación de informes del servicio

Objetivo: generar informes fiables y realistas en el tiempo acordado para posibilitar una toma de decisiones basada en la información así como una comunicación efectiva.

NOTA El éxito de todos los procesos de gestión del servicio depende del uso de la información proporcionada en los informes de servicio.

6.2.1 Política

Los requisitos para la generación de informes para clientes y para gestión interna se deberían acordar y ser registrados.

La supervisión del servicio y la generación de informes abarca todos los aspectos medibles del servicio, proporcionando datos actuales e históricos.

Cuando existan múltiples proveedores, suministradores principales y suministradores subcontratados por éstos, los informes deberían reflejar las relaciones entre ellos. Por ejemplo, un suministrador principal debería informar sobre la totalidad del servicio que presta, incluyendo cualquier servicio realizado por un tercero y que forme parte del que el suministrador principal gestiona como parte del servicio al cliente.

6.2.2 Propósito de los informes del servicio y verificación de su calidad

Los informes de servicio se deberían generar a tiempo, y ser claros, fiables y concisos.

Se deberían adecuar a las necesidades de quien lo recibe y ser suficientemente precisos para poder ser utilizados como herramienta de apoyo en la toma de decisiones.

La presentación debería ayudar a comprender los informes de forma que sean fácilmente asimilables, por ejemplo usan-do gráficos.

Se deberían generar distintos tipos de informes:

a) informes reactivos, que muestran lo que ha ocurrido;

b) informes proactivos, que avisen por adelantado de eventos significativos con objeto de permitir que se puedan realizar acciones preventivas (por ejemplo, informes sobre inminentes rupturas de los SLAs);

c) distribución previa de informes que muestren las actividades planificadas.

6.2.3 Informes de servicio

El proveedor del servicio debería generar informes para los clientes y para la dirección, que cubran los

siguientes aspectos:

a) comportamiento frente a objetivos de nivel de servicio, por ejemplo informes de caídas del servicio, logros;

b) no conformidades frente a normas;

c) características de la carga de trabajo y volumen de la información, por ejemplo incidentes, problemas, cambios y tareas, clasificación, ubicación, clientes, tendencias estacionales, combinación de prioridades, número de solicitudes de ayuda;

d) informes de resultados después de eventos de alto nivel, por ejemplo cambios y entregas;

e) información de tendencias por periodos (por ejemplo diaria, semanal, mensual);

f) informes que incluyan información de cada proceso, por ejemplo número de incidentes y de preguntas más frecuentes, componentes de la infraestructura poco fiables, tareas que consumen gran número de recursos económicos, técnicos o humanos;

g) informes para destacar cargas de trabajo futuras o planificadas.

6.3 Gestión de la continuidad y disponibilidad del servicio

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

NOTA Los desastres o fallos del servicio pueden ocurrir por muchas razones, incluyendo la denegación del servicio, ataques, virus, acceso no permitido a las instalaciones o un desastre natural.

6.3.1 Generalidades

Los requisitos de continuidad y disponibilidad se deberían identificar sobre la base de las prioridades del negocio del cliente, los acuerdos de nivel de servicio y los riesgos evaluados. El proveedor del servicio debería mantener una capacidad suficiente para el servicio junto con planes fácilmente realizables, diseñados para asegurar que los requisitos acordados pueden ser alcanzados en todas las circunstancias, desde el funcionamiento habitual hasta los casos de caídas graves del servicio. El proveedor del servicio debería planificarse para satisfacer los datos conocidos de incrementos o decrementos de volumen de usuarios, picos o caídas previstos de la demanda y cualquier otro cambio futuro conocido. Los requisitos deberían incluir los derechos de acceso y los tiempos de respuesta así como la disponibilidad de los componentes del sistema.

La gestión de la disponibilidad y continuidad del servicio debería trabajar conjuntamente con el objetivo de asegurar que se mantengan los niveles de servicio acordados. Estos requisitos deberían tener una influencia capital en las acciones, esfuerzos y recursos destinados para satisfacer la disponibilidad de los servicios que los soportan.

Los procesos que aseguran que se mantiene la disponibilidad requerida, deberían incluir aquellos elementos de la provisión del servicio que estén bajo el control bien del propio cliente o de otros proveedores del servicio.

6.3.2 Actividades y supervisión de la disponibilidad

La gestión de la disponibilidad debería:

a) supervisar y registrar la disponibilidad del servicio;

b) mantener datos históricos precisos;

c) realizar comparaciones con los requisitos definidos en los SLAs para identificar no conformidades con los objetivos de disponibilidad acordados;

d) documentar y revisar las no conformidades;

e) predecir la disponibilidad a futuro;

f) cuando sea posible, se deberían predecir los posibles problemas y llevar a cabo las acciones preventivas.

Se debería asegurar la disponibilidad de todos los componentes del servicio, registrando y llevando a cabo las acciones correctivas.

6.3.3 Estrategia de continuidad del servicio

El proveedor del servicio debería desarrollar y mantener una estrategia que defina el enfoque general a seguir para satisfacer las obligaciones de continuidad del servicio. Esta estrategia debería incluir la evaluación de riesgos y tener en cuenta los horarios de servicio acordados y los periodos críticos del negocio. El proveedor del servicio debería acordar lo siguiente con cada grupo de clientes y servicios:

a) los periodos máximos aceptables de pérdida continuada del servicio;

b) los periodos máximos aceptables de degradación del servicio;

c) los niveles aceptables de degradación del servicio durante un periodo de recuperación del servicio.

La estrategia de continuidad debería ser revisada con una periodicidad acordada, al menos

anualmente. Cualquier cambio a la estrategia debería ser acordado formalmente

6.3.4 Planificación y prueba de la continuidad del servicio

El proveedor del servicio debería asegurar que:

a) los planes de continuidad tienen en cuenta las dependencias entre el servicio y los componentes de los sistemas;

b) se registran y mantienen los planes de continuidad del servicio y el resto de documentos requeridos para dar soporte a la continuidad del servicio;

c) la responsabilidad para activar los planes de continuidad está claramente asignada y los planes establecen claramente la responsabilidad para la toma de las acciones necesarias frente a cada objetivo;

d) las copias de seguridad de los datos, los documentos, el software y cualquier equipo y personal necesario para la restauración del servicio están disponibles de forma rápida ante un desastre o un fallo importante del servicio;

e) al menos una copia de todos los documentos relativos a la continuidad del servicio debería estar almacenada y ser mantenida en una localización remota y segura, junto al equipamiento que sea necesario para permitir su uso;

f) el personal conoce y asume su rol para activar y/o ejecutar los planes y tiene acceso a la documentación relativa a la continuidad del servicio.

Los planes de continuidad del servicio y la documentación relacionada (por ejemplo los contratos) deberían estar liga-dos a los procesos de gestión del cambio y de gestión de los contratos.

Los planes de continuidad del servicio y la documentación relacionada (por ejemplo los contratos) deberían evaluarse respecto al impacto previamente a que se aprueben los cambios en el sistema y en el servicio, y previamente a acordar los nuevos requisitos del cliente o bien cambios en éstos siempre que sean siginificativos.

Se deberían llevar a cabo pruebas con una frecuencia suficiente para asegurar que los planes de continuidad son efectivos y permanecen así aún cuando se producen cambios en los sistemas, procesos, personal y necesidades del negocio. El cliente y el proveedor del servicio deberían estar implicados conjuntamente en las pruebas, basadas en un conjunto acordado de objetivos. Los fallos en las pruebas se deberían documentar y revisar para proveer de información a un plan de mejora del servicio.

6.4 Elaboración del presupuesto y contabilidad de los servicios de TI

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

6.4.1 Generalidades

Esta sección cubre la realización de los presupuestos y de la contabilidad para los servicios de TI. En la práctica, muchos proveedores están implicados en la facturación del servicio. Sin embargo, dado que la facturación es una actividad opcional, no está cubierta por esta norma. Se recomienda a los proveedores del servicio que cuando lleven a cabo la facturación, el mecanismo empleado para ello esté definido en detalle y sea entendido por todas las partes implicadas.

La responsabilidad sobre muchas de las decisiones financieras va a estar fuera del ámbito de la gestión del servicio y también podrían dictarse externamente los requisitos acerca de qué información financiera se debe facilitar, de qué manera y con qué frecuencia. Las disposiciones de esta sección están enfocadas en las prácticas que se deberían seguir para satisfacer los requisitos de la norma. Sin embargo, se pueden tener en cuenta requisitos más amplios en el caso de que impacten en alguna de las políticas y procedimientos definidos.

6.4.2 Política

Debería existir una política para la gestión financiera de los servicios. La política debería definir los objetivos a ser cumplidos por la realización de los presupuestos y la contabilidad.

La política debería definir también el nivel de detalle al que se lleva a cabo la elaboración de los presupuestos y la contabilidad, teniendo en cuenta:

a) los tipos de costos a ser contabilizados;

b) el reparto de los gastos generales, por ejemplo reparto en partes iguales, reparto porcentual o reparto basado en el tamaño de los elementos variables empleados;

c) la granularidad del negocio del cliente, por ejemplo unidades de negocio tomadas como una sola, dividas en departa-mentos o según las diferentes ubicaciones;

d) las reglas para manejar las variaciones frente al presupuesto, por ejemplo el nivel de variación necesario para que se escale a la alta dirección;

e) los enlaces o vinculación con la gestión de nivel de servicio.

El nivel de inversión en los procesos de elaboración del presupuesto y contabilidad debería estar basado en las necesidades de detalles financieros que tengan los clientes, el proveedor del servicio y los proveedores, según esté definido en la política.

NOTA Los proveedores del servicio que operen en un entorno comercial podrían necesitar invertir mucho más esfuerzo y tiempo en la gestión financiera. Contrariamente, para aquellos proveedores del servicio que sólo necesiten la simple identificación de los costos, esta gestión puede ser mucho más simple.

La realización de los presupuestos y la contabilidad se deberían realizar por todos los proveedores del servicio, cuales-quiera que fueran sus otras políticas en cuanto a gestión financiera.

6.4.3 Elaboración del presupuesto

La elaboración del presupuesto debería tener en cuenta los cambios planificados de los servicios durante el periodo presupuestario y, en el caso de que las necesidades presupuestarias excedan los fondos disponibles, planificar la gestión que se va a hacer del déficit.

La elaboración de los presupuestos puede tener en cuenta factores tales como variaciones estacionales y cambios planificados a corto plazo en los costos y facturación de los servicios.

El seguimiento de los costos frente al presupuesto debería facilitar lo antes posible la información de las variaciones frente al presupuesto.

Se debería establecer un proceso para gestionar las implicaciones de las variaciones frente al presupuesto.

La elaboración de los presupuestos y el seguimiento de los costos deberían dar soporte a la planificación de la operación de cambios en los servicios para que los niveles de dichos servicios puedan mantenerse a lo largo del año.

6.4.4 Contabilidad

Los procesos de contabilidad se deberían usar para realizar el seguimiento de los costos hasta el nivel de detalle acordado durante un periodo de tiempo también acordado.

Las decisiones sobre la provisión del servicio deberían estar basadas en comparaciones sobre la eficacia en costos.

Los modelos de costos deberían ser capaces de mostrar los costos de la provisión del servicio.

Los estados de cuentas deberían mostrar las situaciones de excesos y defectos de gasto así como las recuperaciones de dichas situaciones y deberían permitir al lector entender los costos de niveles bajos de servicio o de pérdidas de servicio.

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.

Los requisitos actuales y esperados del negocio en relación al servicio se deberían conocer en términos de lo que el negocio va a necesitar para dar servicio a sus clientes.

Las previsiones de negocio y las estimaciones de carga de trabajo se deberían traducir a requisitos específicos y quedar documentadas. El resultado de las variaciones en la carga de trabajo o en el entorno debería ser predecibles; se deberían recoger y analizar datos actuales e históricos de utilización de componentes y recursos, al nivel adecuado, con el fin de dar soporte al proceso.

La gestión de la capacidad debería ser el punto focal de todas las cuestiones de rendimiento y capacidad.

El proceso debería ofrecer soporte directo al desarrollo de servicios nuevos y a la modificación de los mismos realizan-do un dimensionamiento y una modelización de servicios.

Se debería generar un plan de capacidad donde se documente el rendimiento real de la infraestructura y los requisitos esperados, con la frecuencia suficiente para tener en cuenta el ritmo de cambios de los servicios y de los volúmenes de servicio, la información de los informes de gestión del cambio y del negocio del cliente.

Dicho informe debería elaborarse al menos anualmente. Se deberían documentar las opciones existentes junto con su costo para cumplir con los requisitos del negocio así como las soluciones recomendadas para conseguir los objetivos de nivel de servicio tal como están definidos en el SLA.

Debería existir una buena comprensión de la infraestructura técnica y sus capacidades presentes y las que estén proyectadas.

6.6 Gestión de la seguridad de la información

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

6.6.1 Generalidades

La seguridad de la información es el resultado de un sistema de políticas y procedimientos diseñados para identificar, controlar y proteger la información y cualquier equipamiento empleado junto con el almacenamiento, transmisión y procesamiento de dicha información.

El personal del proveedor del servicio con roles de especialista en seguridad de la información debería estar familia-rizado con la Norma ISO/IEC 17799, *Tecnologías de la información. Técnicas de seguridad. Código de prácticas para la gestión de la seguridad de la información*.

6.6.2 Identificación y clasificación de los activos de información

El proveedor del servicio debería:

a) mantener un inventario de los activos de información (por ejemplo, ordenadores, sistemas de comunicación, equipos del entorno, documentos y otra información) que son necesarios para la provisión del servicio;

b) clasificar cada activo de acuerdo con su criticidad para el servicio y el nivel de protección que éste requiera, así como nombrar a un propietario que sea el responsable de proporcionar dicha protección;

c) la responsabilidad para la protección de los activos debería recaer en el propietario de dichos activos, aunque estos pueden delegar las responsabilidades de la gestión diaria de la seguridad.

6.6.3 Prácticas para la evaluación de los riesgos de seguridad

La evaluación de los riesgos de seguridad debería:

a) ser realizada con una periodicidad acordada;

b) ser registrada;

c) ser mantenida durante los cambios (cambios de las necesidades del negocio, de procesos o de configuraciones);

d) ayudar a entender en qué podría impactar uno de los servicios gestionados;

e) proveer de información para las decisiones referentes a los tipos de controles a establecer.

6.6.4 Riesgos para los activos de información

Los riesgos para los activos de información se deberían evaluar en función de:

a) su naturaleza (por ejemplo: funcionamiento defectuoso del software, errores de operación, fallos de comunicación);

b) probabilidad;

c) impacto potencial para el negocio;

d) experiencias pasadas.

6.6.5 Seguridad y disponibilidad de la información

Al evaluar los riesgos, se debería prestar atención a los siguientes puntos:

a) revelación de información sensible a partes no autorizadas;

b) información inexacta, incompleta o inválida (por ejemplo: información fraudulenta);

c) información que quede inservible para su uso (por ejemplo: debido a un corte de energía eléctrica);

d) daño físico o destrucción de los equipos necesarios para proveer los servicios.

También se deberían tener en cuenta los objetivos de la política de seguridad de la información, las necesidades para satisfacer los requisitos específicos de los clientes respecto a la seguridad (por ejemplo: niveles de disponibilidad) y los requisitos legales o regulatorios que apliquen.

6.6.6 Controles

Además de otros controles que puedan ser justificables y aconsejados en esta parte de la Norma ISO/IEC 20000 (por ejemplo: en la continuidad del servicio), los proveedores del servicio deberían aplicar los siguientes controles como una buena práctica en gestión de la seguridad de la información:

a) la alta dirección debería definir la política de seguridad de la información, comunicarla a su personal y a sus clientes y asegurarse de que se implanta eficazmente;

b) los roles y las responsabilidades para la gestión de la seguridad de la información se deberían definir y asignar a un puesto de trabajo;

c) un representante del equipo de dirección (el rol puede ser desempeñado por un propietario que sea un responsable senior) debería supervisar y mantener la eficacia de la Política de Seguridad de la Información;

d) el personal que ejerza un rol significativo en seguridad debería recibir formación en seguridad de la información;

e) todo el personal debe ser concienciado acerca de la política de seguridad de la información;

f) debería haber apoyo de expertos en la evaluación de riesgos y en la implementación de los controles;

g) los cambios no deberían comprometer la operación efectiva de los controles;

h) se debería hacer un informe de los incidentes de seguridad de la información siguiendo los procedimientos de gestión del incidente y, también, se debería iniciar una respuesta a dichos incidentes.

6.6.7 Documentos y registros

Los registros se deberían analizar periódicamente para proporcionar información a la dirección en cuanto a:

a) la eficacia de la política de seguridad de la información;

b) las tendencias que aparezcan en los incidentes en seguridad de la información;

c) dar entrada de información a un plan de mejora del servicio;

d) tener bajo control el acceso a la información, los activos y los sistemas. La gestión de la seguridad de la información debería estar documentada de una manera fiable.

7 Procesos de relaciones

7.1 Generalidades

Los procesos de relación describen los dos aspectos relacionados de la gestión de suministradores y la gestión de relaciones con el negocio. Esta norma se dirige hacia el rol de un proveedor del servicio, el cual cumple un papel entre los suministradores, que proporcionan bienes o servicios a dicho proveedor del servicio, y los clientes, que reciben los servicios.

Tanto los suministradores, como los clientes pueden ser internos y externos a la organización del proveedor del servicio. Las relaciones externas se formalizarán mediante contratos. Las relaciones internas se formalizarán mediante acuerdos de servicio o de soporte interno que son a menudo designados como acuerdos de nivel operacional.

La figura 2 muestra una representación simplificada de las relaciones.

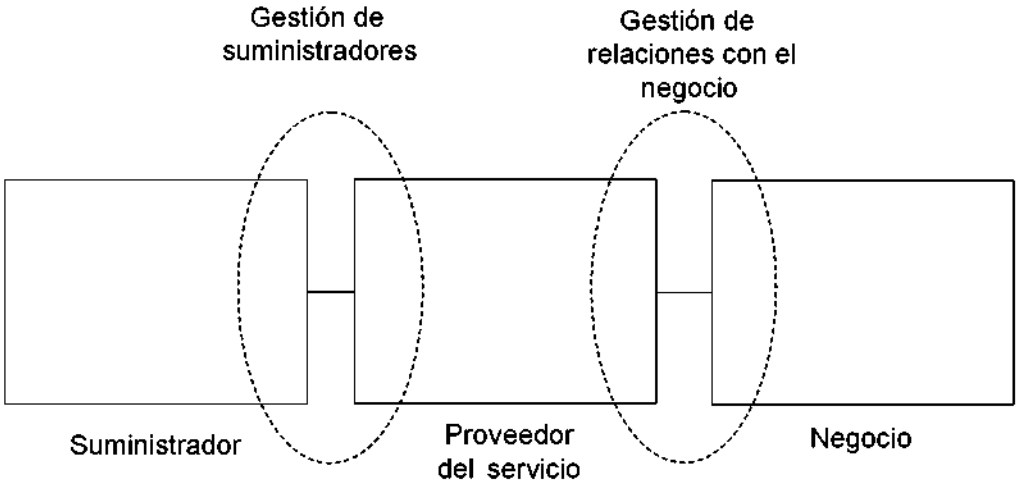

Figura 2 — Procesos de relaciones

Como muestra la figura 2, el proveedor del servicio juega un papel dentro de la cadena de suministro, en la cual cada eslabón debería añadir valor, de forma que el proveedor del servicio que recibe bienes o servicios procedentes del suministrador y entrega un servicio mejorado al cliente.

A modo de aclaración, dentro de esta sección el término proveedor del servicio se utiliza siempre para describir la organización a la que se dirige este documento, independientemente del papel, o sentido en la cadena, que tiene en el proceso que se describe.

En la práctica, las relaciones raramente son así de simples, sino que implican múltiples participantes, asumiendo papeles, tanto como suministradores, como clientes y con conexiones de negocio entre muchos de ellos de forma directa o bien mediante el proveedor del servicio.

Los procesos de relación deberían asegurar que todas las partes:

a) entienden y satisfacen las necesidades del negocio;

b) entienden las capacidades y limitaciones;

c) entienden las responsabilidades y las obligaciones.

Estos procesos también deberían asegurar que los niveles de satisfacción del cliente son apropiados y que se comunican y entienden las necesidades futuras del negocio.

El alcance, los roles y las responsabilidades de las relaciones con el negocio y las relaciones con los suministradores deberían definirse y acordarse. Esto debería incluir la identificación de todos los grupos de interés, los contactos y los medios y frecuencia de la comunicación.

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 en los fundamentos de su negocio.

7.2.1 Revisiones del servicio

El proveedor del servicio y los clientes deberían realizar revisiones del servicio, al menos anualmente y antes y después de cambios importantes. La revisión debería considerar el comportamiento previo, tratar las necesidades de negocios actuales y previstas y proponer cualquier cambio necesario en el alcance del servicio y los SLAs. Otros grupos de interés

implicados como por ejemplo subcontratistas, clientes, grupos de usuarios u otros grupos representativos, pueden ser invitados a participar en las reuniones de revisión.

El proveedor del servicio y los clientes deberían también acordar los procedimientos de revisión parcial para tratar el progreso, los logros y los problemas detectados. Estas reuniones deberían planificarse y ser notificadas a los grupos de interés para los que sea relevante.

El proveedor del servicio debería planificar y registrar todas las reuniones formales, registrar los problemas tratados y realizar el seguimiento de las acciones acordadas.

El proveedor del servicio debería establecer una relación con sus clientes de manera que éstos puedan estar al tanto de las necesidades del negocio y de los cambios principales para poder prepararse para dar una respuesta a los mismos.

7.2.2 Reclamaciones del servicio

El proveedor del servicio y los clientes deberían acordar un procedimiento formal de reclamaciones que elimine cualquier ambigüedad sobre qué constituye una reclamación y cómo se debería gestionar. El proveedor del servicio debería poner en marcha un proceso para tomar las acciones adecuadas en la resolución de los problemas.

El proceso debería identificar a la persona de contacto en el proveedor del servicio al que dirigir las reclamaciones formales El proveedor del servicio debería registrar, investigar, tomar acciones, elaborar informes y cerrar formalmente todas las reclamaciones de servicio. Las reclamaciones más relevantes se deberían revisar periódicamente y ser escaladas a la alta dirección si no se resuelven dentro de los plazos acordados con los clientes. Los proveedores del servicio deberían analizar periódicamente las reclamaciones registradas para identificar tendencias y elaborar informes con este análisis para los clientes. Los resultados de tal análisis se deberían usar cuando sea apropiado para el establecimiento de un plan de mejora del servicio.

7.2.3 Medición de la satisfacción del cliente

Se debería medir la satisfacción del cliente para permitir al proveedor del servicio comparar el desempeño con los objetivos de satisfacción de clientes y con encuestas previas. El alcance y la complejidad de la encuesta se deberían concebir de forma que los clientes puedan responder fácilmente y sin que se requiera un excesivo tiempo para cumplimentar de una manera adecuada dicha encuesta.

Se deberían investigar las variaciones significativas en los niveles de satisfacción para llegar a entender las razones de las mismas. Los análisis de tendencias u otras comparaciones solo deberían realizarse sobre preguntas comparables y entre métodos de muestreo comparables.

Los resultados y conclusiones de las encuestas de satisfacción del cliente se deberían tratar con el cliente. Se debería acordar un plan de acción, utilizándolo como entrada para un plan de mejora del servicio sobre cuyo progreso se informe al cliente.

Las felicitaciones sobre el servicio se deberían documentar y dar a conocer al equipo que esté prestando el servicio.

7.3 Gestión de suministradores

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

7.3.1Introducción

Los procedimientos de gestión de suministradores deberían garantizar que:

a) el suministrador entiende sus obligaciones frente al proveedor del servicio;
b) los requisitos acordados y legítimos son cumplidos dentro del alcance y los niveles de servicio acordados;
c) los cambios son gestionados;

d) se registran las transacciones de negocio entre todas las partes;
e) se puede controlar la información sobre el desempeño de todos los suministradores y actuar en consecuencia.

7.3.2 Gestión de contratos

El proveedor del servicio debería designar un responsable para hacerse cargo de los contratos y acuerdos con los suministradores. En el caso de que haya todo un grupo de personal involucrado en esta tarea, debería existir un proceso común para asegurar que la información sobre el desempeño de los suministradores está controlada y se actúa consecuentemente.

Debería existir una persona de contacto definida dentro de la organización del proveedor del servicio que sea el responsable de la relación con cada suministrador.

Todos los contratos con suministradores deberían contener una planificación de las revisiones para evaluar si los objetivos de negocio para el suministro de un servicio siguen siendo válidos.

Debería existir un proceso claramente definido para la gestión de cada contrato. El proceso para la modificación de contratos debería estar también claramente definido. Cualquier cambio a este procedimiento se debería notificar formalmente a todos los suministradores afectados.

Se debería mantener una lista de puntos de contacto dentro de las respectivas organizaciones (la del suministrador y la del proveedor del servicio). Si un contrato incluye penalizaciones o bonificaciones, se deberían establecer claramente sus fundamentos y elaborar un informe del cumplimiento de los requisitos.

7.3.3 Definición del servicio

Para cada servicio y suministrador el proveedor del servicio debería mantener:

a) una definición de servicios, roles y responsabilidades;

b) el alcance del servicio;

c) un proceso de gestión de contratos, los niveles de autorización y un plan de extinción del

contrato;

d) las condiciones de pago, si son relevantes;

e) los parámetros de informe y el registro acordados sobre el desempeño alcanzado.

7.3.4 Gestión de múltiples suministradores

Debería quedar claro si el proveedor del servicio trata con todos los suministradores de forma directa o mediante un suministrador principal que toma la responsabilidad de los suministradores subcontratados.

El suministrador principal debería registrar los nombres, responsabilidades y relaciones entre todos los suministradores subcontratados y ponerla a disposición del proveedor del servicio si así lo requiere.

El proveedor del servicio debería obtener evidencias de que los suministradores principales gestionan formalmente a los suministradores subcontratados; guiándose, cuando sea apropiado, por los requisitos incluidos en la Norma ISO/IEC 20000-1.

7.3.5 Gestión de los conflictos contractuales

Tanto el proveedor del servicio como el suministrador deberían funcionar conforme a un proceso para gestionar los conflictos, el cual se debería definir o referenciar dentro del contrato.

Debería existir un procedimiento o itinerario para poder escalar los conflictos que no puedan ser resueltos mediante el procedimiento ordinario.

El proceso debería asegurar que los conflictos son registrados, investigados, que se toman las acciones necesarias sobre ellos y que se cierran formalmente.

7.3.6 Finalización del contrato

El proceso de gestión de contratos debería contemplar la extinción del contrato (tanto planificada, como prematura). También debería proporcionar un mecanismo de transferencia del servicio a otra organización.

8 Procesos de resolución

8.1 Antecedentes

La gestión del incidente y del problema son procesos distintos, aunque están estrechamente relacionados. El proceso de gestión del incidente se encarga de la restauración del servicio a los usuarios, mientras la gestión del problema tiene como misión la identificación y la eliminación de las causas de los incidentes.

8.1.1 Establecimiento de prioridades

Los objetivos para la resolución deberían estar basados en la prioridad. La prioridad se debería basar en el impacto y la urgencia. El impacto se debería basar en el nivel de daño real o potencial al negocio del cliente. La urgencia se debería basar en el tiempo entre la detección del problema o del incidente y el momento en que se produce el impacto sobre el negocio del cliente.

La planificación de la resolución de incidentes o problemas debería tener en cuenta, como mínimo, lo siguiente:

a) la prioridad;

b) las habilidades disponibles;

c) los requisitos de competencia para los recursos;

d) el esfuerzo/costo necesario para proporcionar el método de resolución;

e) el tiempo transcurrido para proporcionar un método de resolución.

NOTA La prioridad se utiliza durante toda la gestión del servicio pero es fundamental para la gestión del incidente y del problema.

8.1.2 Soluciones provisionales

Siempre que sea necesario, la gestión del problema debería desarrollar y mantener soluciones provisionales para permitir a la gestión del incidente ayudar a los usuarios o al personal a restaurar el servicio.

Un error conocido sólo se debería cerrar cuando se haya aplicado satisfactoriamente un cambio correctivo o el error deje de existir (por ejemplo, porque el servicio ya no se utilice).

La gestión del problema debería tener acceso a la información sobre las áreas de negocio afectadas por los problemas.

Se debería almacenar y mantener en la base de datos de conocimiento, la información sobre las soluciones provisionales, su aplicabilidad y su efectividad.

8.2 Gestión del incidente

Objetivo: Restaurar el servicio en los niveles acordados tan pronto como sea posible o responder a las peticiones de servicio.

8.2.1 Generalidades

NOTA 1 El proceso de gestión del incidente puede ser proporcionado por un servicio de atención al cliente, que actúe como punto de contacto diario con los usuarios.

NOTA 2 La gestión de incidentes debería ser:

a) un proceso tanto proactivo como reactivo, que responda a los incidentes que afecten, o que pudieran potencialmente, afectar al servicio;

b) un proceso centrado en la restauración del servicio a los clientes y no en la determinación de la causa de los incidentes.

El proceso de gestión del incidente debería incluir lo siguiente:

a) la recepción, el registro, la asignación de prioridad y la clasificación de las llamadas;

b) la resolución de primera línea o la derivación;

c) la consideración de cuestiones de seguridad;

d) el seguimiento y la gestión del ciclo de vida de los incidentes;

e) la verificación y el cierre de los incidentes;

f) el contacto de primera línea con los clientes;

g) el escalado.

Se puede informar sobre incidentes mediante llamadas telefónicas, buzón de voz, visitas, cartas, faxes o mensajes de correo electrónico, o bien pueden ser registrados los avisos directamente por los clientes que tengan acceso al sistema de registro de incidentes, o se pueden registrar automáticamente mediante un software de supervisión automática.

Todos los incidentes se deberían registrar de modo que la información relevante se pueda recuperar y analizar.

El progreso (o su ausencia) de la resolución del incidente se debería comunicar a las partes real o potencialmente afectadas. Todas las acciones se deberían registrar en el registro del incidente.

El personal de gestión del incidente debería tener acceso a una base de conocimientos actualizada que contenga información sobre técnicos especialistas, incidentes anteriores, problemas relacionados y errores conocidos, soluciones provisionales y listas de comprobación que ayuden a restaurar el servicio para la empresa.

Siempre que sea posible, se debería proporcionar al cliente los medios necesarios para continuar con sus actividades empresariales, aunque sea con un servicio degradado (por ejemplo inhabilitando una función defectuosa). El motivo es minimizar la repercusión sobre las actividades empresariales del cliente. Cuando la causa del problema siga sin determinarse pero se haya establecido una solución provisional, se deberían registrar los detalles para utilizarlos durante la diagnosis continua del problema y cuando se produzcan incidentes similares.

Un incidente sólo debería cerrarse definitivamente cuando el usuario que haya notificado dicho incidente haya podido confirmar que el incidente se ha resuelto y el servicio ha sido restaurado.

8.2.2 Incidentes graves

Se debería definir claramente qué constituye un incidente grave y quién está capacitado para llevar a cabo cambios en el funcionamiento habitual del proceso de incidentes/problemas.

Todos los incidentes graves deberían tener en todo momento un gestor responsable claramente definido.

La designación como responsable de un incidente grave debería proporcionar los niveles de autoridad individual adecuados para la función de coordinar y controlar todos los aspectos de la resolución. Esto debería incluir una responsabilidad del escalado y una comunicación eficaces entre todas las áreas implicadas en la resolución y hacia los clientes que se vean afectados por dicho incidente grave.

NOTA Este nivel de autoridad puede ser temporal y aplicarse sólo mientras dure el incidente grave.

El proceso para un incidente grave debería incluir una revisión que proporcionará información al plan de mejora del servicio.

8.3 Gestión del problema

Objetivo: minimizar las interrupciones de servicio de cara al negocio mediante la identificación y el análisis proactivos de las causas de los incidentes y mediante la gestión del problema hasta su cierre.

8.3.1 Alcance de la gestión del problema

El proceso de gestión del problema debería investigar las causas subyacentes de los incidentes.

La gestión del problema debería prevenir de una manera proactiva la repetición o la duplicación de los incidentes o de los errores conocidos de acuerdo con los requisitos del negocio.

8.3.2 Inicio de la gestión del problema

Se deberían clasificar los incidentes para ayudar a determinar las causas de los problemas. La clasificación puede hacer referencia a los problemas y cambios existentes.

NOTA Cuando se registren incidentes por primera vez, su categorización se verá influenciada por otros factores que incluyen el servicio, el área de negocio afectada y los síntomas que se presenten.

8.3.3 Errores conocidos

Cuando la investigación de la gestión del problema haya identificado la causa del origen de un incidente y un método para resolver los incidentes, el problema se debería clasificar como un error conocido.

Se deberían registrar todos los errores conocidos tomando como referencia los servicios real o potencialmente afectados además del elemento de configuración que se sospeche que causa el error en cuestión.

La información sobre los errores conocidos en los servicios que se estén introduciendo en el entorno productivo se debería pasar a la gestión del servicio y se debería registrar en la base de datos de conocimiento, junto con las soluciones provisionales existentes.

Un error conocido no se debería cerrar hasta que se haya resuelto satisfactoriamente.

NOTA El cliente o el proveedor del servicio pueden decidir que la resolución resulta demasiado cara o que no aporta beneficio al negocio. En este caso, esto debería quedar claramente documentado. No obstante, el error conocido debería permanecer abierto, puesto que aún existe la posibilidad de que se produzcan incidentes a consecuencia de este error y es posible que se necesiten soluciones provisionales y/o una reconsideración de la decisión para resolver el error.

8.3.4 Resolución del problema

Cuando la causa raíz se haya identificado y se haya tomado una decisión para resolver el error, la resolución se debería conducir a través del proceso de gestión del cambio.

8.3.5 Comunicación

La información sobre soluciones provisionales, arreglos permanentes o el progreso de los problemas se debería comunicar a las partes afectadas o puede requerirse para dar soporte a los servicios afectados.

8.3.6 Seguimiento y escalado

Se debería realizar un seguimiento del progreso de todos los problemas.

Todos los problemas se deberían escalar a las partes apropiadas. El proceso debería cubrir:

a) el registro de los cambios de las identidades de los responsables de la resolución de problemas durante el ciclo de vida de cada problema;

b) la identificación de incidentes que rompan los objetivos del nivel de servicio;

c) la distribución de información en cascada a los clientes y colegas para que puedan llevar a cabo las acciones adecua-das para minimizar la repercusión del problema no resuelto;

d) la definición de los puntos de escalado;

e) el registro de los recursos empleados y de las acciones realizadas.

8.3.7 Cierre de registros de incidentes y problemas

El procedimiento de cierre del registro debería incluir comprobaciones para garantizar que:

a) los detalles de la resolución se hayan registrado con precisión;

b) la causa esté categorizada para facilitar el análisis;

c) si es necesario, tanto el personal del cliente como el personal de soporte estén al corriente de la resolución;

d) el cliente acepte que la resolución se ha conseguido;

e) el cliente sea informado si no se va a llegar a una resolución o ésta no resulta posible.

8.3.8 Revisiones de problemas

Se deberían realizar revisiones de los problemas siempre que, la investigación para esclarecer los problemas no resueltos, no habituales o de gran repercusión, las justifique. La finalidad de estas revisiones es encontrar mejoras para el proceso y evitar la repetición de incidentes o errores.

Las revisiones de problemas son normalmente:

a) revisiones de los niveles de incidentes individuales y del estado de problemas respecto a los niveles de servicio;

b) revisiones de la dirección para resaltar los problemas que requieren una acción inmediata;

c) revisiones de la dirección para determinar y analizar tendencias y para proporcionar información a otros procesos como, por ejemplo, el de educación y formación del cliente.

8.3.9 Temas a tratar en las revisiones

Las revisiones deberían incluir información de:

a) tendencias, por ejemplo, problemas e incidentes recurrentes, errores conocidos, etc.;

b) problemas recurrentes de una determinada clasificación de componente o de ubicación;

c) deficiencias causadas por la subcontratación, la formación o la documentación;

d) no-conformidades, por ejemplo, conforme a normas, políticas y leyes;

e) errores conocidos en las entregas planificadas;

f) el compromiso del personal para resolver los incidentes y los problemas;

g) repetición de incidentes o problemas ya resueltos.

Las mejoras del servicio o del proceso de gestión de problemas se deberían registrar e incluir en un plan de mejora del servicio.

La información se debería añadir a la base de conocimientos de gestión de problemas.

Toda la documentación relevante se debería actualizar, por ejemplo, las guías del usuario y la documentación del sistema.

8.3.10 Prevención de problemas

La gestión proactiva de problemas debería conducir a una reducción de los incidentes y de los problemas. Debería incluir referencias a la información que resulte de ayuda para el análisis como, por ejemplo:

a) activos y configuración;

b) gestión del cambio;

c) un error conocido y divulgado, información sobre las soluciones provisionales de los proveedores;

d) información histórica sobre problemas similares.

La prevención de problemas debería abarcar desde la prevención de incidentes individuales, tales como las dificultades reiteradas para utilizar una determinada función de un sistema, hasta las decisiones estratégicas. Es probable que estas últimas requieran un gasto de implementación considerable, por ejemplo, la inversión en una red mejor; a este nivel, la gestión del problema proactiva se funde con la gestión de la disponibilidad.

La prevención de problemas también incluye el suministro de información a los clientes para evitar que tengan que pedir ayuda en el futuro, por ejemplo, para prevenir incidentes causados por la falta de conocimiento o la falta de for-mación del usuario.

9 Procesos de control

9.1 Gestión de la configuración

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

9.1.1 Planificación e implementación de la gestión de la configuración

La gestión de la configuración se debería planificar e implementar junto con la gestión del cambio y la gestión de entregas para asegurar que el proveedor del servicio pueda gestionar sus activos y configuraciones de TI de forma efectiva.

Debería estar disponible una información precisa sobre la configuración para dar soporte a la planificación y al control de los cambios a medida que los sistemas y los servicios nuevos y modificados son liberados y distribuidos. El resultado debería ser un sistema eficiente que integre los procesos de gestión de la información de configuración del proveedor del servicio con los de los clientes y suministradores, cuando proceda.

Todos los activos y configuraciones principales se deberían tener en cuenta y tener un gestor responsable que asegure que se mantienen la protección y el control apropiados, por ejemplo: los cambios son autorizados antes de la implementación.

Se podría delegar la tarea de implementar los controles, pero la responsabilidad sigue estando en el gestor responsable. Este gestor responsable debería disponer de la información necesaria para delegar esta responsabilidad, por ejemplo, la persona que autoriza un cambio podría requerirle información del costo, riesgos, impacto del cambio y recursos para la implementación.

La infraestructura y/o los servicios deberían tener un plan(es) actualizado(s) de gestión de la configuración, que puede ser independiente o formar parte de otros documentos de la planificación. Éstos deberían incluir o describir:

a) ámbito, objetivos, políticas, roles y responsabilidades normalizados;

b) los procesos de gestión de la configuración para definir los elementos de configuración de los servicios e infraestructuras, controlar los cambios en las configuraciones, registrar e informar del estado de los ítems de configuración y verificar la integridad y la exactitud de los elementos de configuración;

c) los requisitos para la contabilidad, el seguimiento y la auditoria, por ejemplo, para propósitos de seguridad, legales, regulatorios o de negocio;

d) el control de la configuración (acceso, protección, versionado, construcción, control de entrega);

e) el proceso de control de los elementos de contacto que identifiquen, registren y gestionen los elementos y la infor-mación de la configuración en los límites comunes a dos o más organizaciones, por ejemplo: interfaces de sistemas, versiones;

f) la planificación y el establecimiento de los recursos para mantener los activos y las configuraciones bajo control y mantener el sistema de gestión de la configuración, por ejemplo, formación;

g) la gestión de los suministradores y subcontratistas que estén llevando a cabo labores de gestión de la configuración.

NOTA Se debería implantar un nivel apropiado de automatización para asegurar que los procesos no se conviertan en ineficaces, o en proclives al error o que no pudieran ejecutarse.

9.1.2 Identificación de configuración

Todos los elementos de configuración deberían estar identificados de manera unívoca y estar definidos por atributos que describan sus características funcionales y físicas. La información debería ser relevante y auditable.

En la base de datos de la configuración se deberían utilizar y registrar los marcados apropiados u otros métodos de identificación.

Los elementos a ser gestionados se deberían identificar usando los criterios de selección establecidos y deberían incluir:

a) todas las distribuciones y entregas de los sistemas de información y del software (incluyendo software de terceras partes) y la documentación relativa de los sistemas, por ejemplo, las especificaciones de requisitos, diseños, infor-mes de prueba, documentación de la entrega;

b) las líneas de referencia de la configuración o las premisas de construcción para cada entorno, módulo hardware normalizado y versión;

c) copia física maestra y bibliotecas electrónicas, por ejemplo: la biblioteca definitiva de software;

d) las herramientas o paquetes usados para la gestión de la configuración;

e) licencias;

f) componentes de seguridad, por ejemplo: cortafuegos;

g) activos físicos que sean necesarios para la gestión financiera de activos o bien por motivos de negocio, por ejemplo: medios magnéticos seguros, equipamiento;

h) documentación relativa al servicio, por ejemplo: SLAs, procedimientos;

i) instalaciones para el soporte del servicio, por ejemplo: energía eléctrica para la sala de ordenadores;

j) relaciones y dependencias entre los elementos de la configuración.

NOTA Otros elementos que podrían se considerados como elementos de configuración son:

a) otra documentación;
b) otros activos;
c) otras instalaciones, por ejemplo: emplazamientos;
d) unidades de negocio;
e) personas.

Se deberían identificar las relaciones y dependencias adecuadas entre los elementos de configuración para proporcionar el nivel de control necesario.

Cuando sea necesario establecer alguna trazabilidad, el proceso debería asegurar que se puede seguir el registro de los elementos de la configuración en todo su ciclo de vida, desde los documentos de requisitos hasta los registros de entrega, por ejemplo, utilizando una matriz de trazabilidad.

9.1.3 Control de la configuración

El proceso debería garantizar que sólo los elementos de la configuración autorizados e identificables son aceptados y registrados desde su recepción hasta su baja.

Ningún elemento de la configuración se debería añadir, modificar, reemplazar o eliminar/retirar sin la documentación de control apropiada, por ejemplo: aprobación de la solicitud de cambio, información actualizada de la versión.

Para proteger la integrad de los sistemas, servicios e infraestructura, los elementos de la configuración se deberían mantener en un entorno seguro y adecuado que:

a) los proteja de accesos no autorizados, cambios o corrupción, por ejemplo: virus:

b) proporcione algún medio de recuperación ante desastres;

c) permita la recuperación controlada de una copia del maestro controlado, por ejemplo: software.

9.1.4 Seguimiento del estado de configuración y elaboración de informes

Los registros de la configuración se deberían mantener actualizados y con la precisión adecuada para reflejar los cam-bios en el estado, localización y versión de los elementos de la configuración.

El seguimiento del estado debería proporcionar información sobre los datos actuales e históricos de cada elemento de configuración a lo largo de su ciclo de vida. Esto debería permitir el seguimiento de los cambios en los elementos de la configuración a través de sus diferentes estados, por ejemplo: solicitado, recibido, en pruebas de aceptación, activo, bajo cambio, retirado y eliminado.

La información de la configuración se debería mantener actualizada y disponible para: los planes, la toma de decisiones y la realización de cambios a las configuraciones definidas.

Cuando sea requerida, la información de la configuración debería estar accesible a: usuarios, clientes, suministradores y socios para darles apoyo en sus planes y en la toma de decisiones. Por ejemplo, un proveedor externo de servicios podría poner accesible su información de la configuración a los clientes y a otras partes, para dar soporte a los procesos de gestión del servicio del resto de las partes implicadas para un servicio completo extremo a extremo.

Los informes de gestión de la configuración deberían estar disponibles para todas las partes correspondientes. Los informes deberían cubrir: la identificación y el estado de los elementos de la configuración, sus versiones y la documentación asociada.

Los informes deberían cubrir:

a) las últimas versiones de los elementos de la configuración;

b) la localización del elemento de configuración y, para el software, la localización de las versiones maestras:

c) interdependencias;

d) historia de la versión;

e) estado de los elementos de la configuración que conjuntamente constituyan:

   1) la configuración del servicio o del sistema;
   2) un cambio, una línea de referencia, un paquete de instalación o una entrega;
   3) una versión o una variante.

9.1.5 Verificación y auditoria de la configuración

Los procesos de verificación y auditoria, en sus aspectos físicos y funcionales, se deberían planificar y se debería reali-zar una comprobación para asegurar que los procesos y recursos adecuados están establecidos para:

a) proteger las configuraciones físicas y el capital intelectual de la organización;

b) asegurar que el proveedor del servicio tiene el control de sus configuraciones, las copias maestras y las licencias;

c) garantizar que la información de la configuración está actualizada, controlada y es visible;

d) asegurar que un cambio, una entrega, un sistema o un entorno es conforme a los requisitos contratados o especifica-dos y que los registros de la configuración son exactos.

Periódicamente se deberían realizar auditorías de la configuración, antes y después de un cambio importante, después de un desastre y a intervalos aleatorios.

Las deficiencias y las no conformidades se deberían registrar, evaluar e iniciar una acción correctiva, actuar sobre ellas; y se debería realimentar a las partes correspondientes así como establecer un plan de mejora del servicio.

NOTA Normalmente hay dos tipos de auditoria de la configuración:

a) auditoria funcional de la configuración: un examen formal para verificar que un elemento de configuración ha alcanzado el rendimiento y características funcionales especificadas en sus documentos de configuración;
b) auditoria física de la configuración: un examen formal de la configuración "según sale de fábrica" de un elemento de configuración para verificar su conformidad con sus documentos de configuración del producto.

9.2 Gestión del cambio

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

9.2.1 Planificación e implantación

Los procesos y procedimientos de gestión de cambio deberían garantizar que:

a) los cambios tienen claramente definido y documentado su alcance;

b) sólo son aprobados los cambios que proporcionan beneficios al negocio, por ejemplo: comerciales, legales, regulato-rios o estatutarios;

c) los cambios son planificados en base a la prioridad y al riesgo;

d) los cambios a las configuraciones pueden se verificados durante la implementación del cambio;

e) cuando sea requerido, el plazo para la implementación de los cambios es supervisado y mejorado;

f) puede demostrarse cómo un cambio es:

1) generado, registrado y clasificado (con las referencias a los documentos que dieron origen al cambio);
2) evaluado en relación al impacto, la urgencia, el costo, los beneficios y el riesgo del cambio en el servicio, en los clientes y en los planes de despliegue;
3) revertido o remediado, si no tuvo éxito;
4) documentado, por ejemplo, la solicitud de cambio está asociada a los elementos de configuración afectados, a la versión actualizada de la implementación y a los planes de despliegue;
5) aprobado o rechazado por una autoridad de cambios, dependiendo de su tipo, tamaño o riesgo;
6) implementado por el responsable designado dentro de los grupos responsables de los componentes a ser cambiados;
7) probado, verificado y entregado;
8) cerrado y revisado;
9) planificado, supervisado e incluido en un informe;
10) asociado a incidentes, problemas, otro cambio y a los registros de elementos de configuración,

cuando sea apropiado.

El estado de los cambios y las fechas de implementación planificadas se deberían usar como base para la planificación del cambio y del despliegue.

La información de planificación debería estar disponible para las personas afectadas por el cambio.

Cuando se pueda ocasionar una perdida del servicio durante el horario normal del servicio, las personas afectadas deberían acordar el cambio antes de su implementación.

9.2.2 Cierre y revisión de una solicitud de cambio

Todos los cambios se deberían revisar en relación a su éxito o fallo después de la implementación y cualquier mejora debería ser registrada. Se debería realizar una revisión después de la implementación en los cambios principales para comprobar que:

a) el cambio cumple sus objetivos;

b) los clientes están satisfechos con los resultados;

c) no ha habido efectos colaterales inesperados.

Toda no conformidad se debería registrar y tomarse las acciones pertinentes.

Cualquier debilidad o deficiencia identificada en la revisión del proceso de gestión del cambio, debería alimentar los planes de mejora del servicio.

9.2.3 Cambios de emergencia

En ocasiones se requiere la realización de cambios de emergencia, y cuando sea posible, se debería seguir el proceso de cambio, aunque algunos detalles se documenten a posteriori. Cuando el proceso de emergencia se salte algunos requisitos del proceso de gestión del cambio, el cambio debería cumplir estos requisitos tan pronto como sea posible.

Los cambios de emergencia se deberían justificar por quien los implementa y deberían ser revisados después del cambio para verificar que era una verdadera emergencia.

9.2.4 Informes, análisis y acciones de la gestión del cambio

Los registros de los cambios se deberían analizar de forma periódica, para detectar incrementos en el nivel de cambios, frecuencia de los tipos recurrentes, tendencias emergentes y cualquier otra información relevante. Los resultados y las conclusiones derivados del análisis de los cambios se deberían registrar y actuar sobre ellos.

10 Procesos de entrega

10.1 Proceso de gestión de la entrega

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

10.1.1 Generalidades

La gestión de la entrega debería coordinar las actividades del proveedor del servicio, los diferentes proveedores y el ne-gocio para planificar y desplegar una entrega a lo largo de un entorno distribuido.

Son esenciales una buena planificación y gestión para empaquetar y distribuir una entrega con éxito, y para gestionar los impactos y riesgos asociados al negocio y a las TI. Se debería planificar con el negocio la entrega de los sistemas de información, las infraestructuras, los servicios y la documentación afectados.

Todas las actualizaciones asociadas a la documentación se deberían incluir en la entrega, por ejemplo: los procesos de negocio, los documentos de apoyo y los acuerdos de nivel de servicio.

Se debería evaluar el impacto de todos los elementos de configuración, nuevos o cambiados, requeridos para efectuar los cambios autorizados.

El proveedor del servicio se debería asegurar de que los aspectos técnicos y no técnicos de la entrega son considerados de forma conjunta.

Los elementos de la entrega deberían poder ser trazables y no ser modificables. Solo se deberían aceptar en el entorno de producción las entregas adecuadas, probadas y aprobadas.

10.1.2 Política de entrega

Debería existir una política de entrega que incluya:

a) la frecuencia y tipos de entregas;

b) los roles y las responsabilidades para la gestión de la entrega;

c) la autoridad para pasar la entrega a los entornos de pruebas de aceptación y de la producción;

d) una identificación y descripción única para todas las entregas;

e) una aproximación en torno a la agrupación de los cambios en una entrega;

f) una aproximación para la automatización de los procesos de construcción, instalación, y distribución de la entrega para ayudar a su repetibilidad y a su eficiencia;

g) la verificación y la aceptación de una entrega.

10.1.3 Planificación de la entrega y del despliegue

El proveedor del servicio debería trabajar conjuntamente con el negocio para asegurar que los elementos de configuración que se van a desplegar en una entrega son compatibles entre sí y con los elementos de configuración del entorno de destino.

Planificación de la entrega debería asegurar que los cambios de los sistemas de información, infraestructuras, servicios y documentación afectados son acordados, autorizados, planificados, coordinados y que se realiza un seguimiento de los mismos.

La entrega y el despliegue se deberían planificar en etapas ya que los detalles del despliegue podrían no ser conocidos inicialmente.

La planificación de una entrega y del despliegue normalmente debería incluir:

a) las fechas de la entrega y la descripción de los entregables;

b) los cambios y problemas relacionados, errores conocidos cerrados o resueltos por esta entrega y errores conocidos que hayan sido identificados durantes las pruebas de la entrega;

c) los procesos relacionados para la implementación de una entrega a lo largo de todo el negocio y las diferentes unidades geográficas;

d) el modo en el que se dará marcha atrás de la entrega o en que esta se remediará si no se concluye con

éxito;

e) los procesos de verificación y aceptación;

f) la comunicación, preparación, documentación y formación para los clientes y personal de apoyo;

g) la logística y los procesos implicados para realizar la compra, el almacenamiento, la expedición, la conexión, la aceptación y la puesta a disposición de los bienes;

h) los recursos de apoyo necesarios para asegurar el mantenimiento de los niveles de servicio;

i) la identificación de las dependencias, los cambios relacionados y los riesgos asociados que pueden perjudicar el paso sin complicaciones de una entrega a los entornos de pruebas de aceptación y de producción;

j) la autorización de la entrega;

k) el calendario de auditorías del entorno de producción cuando sea necesario asegurar, para actualizaciones de gran tamaño, que el entorno de producción está en el estado esperado en el momento de instalar la entrega.

10.1.4 Desarrollo o compra de software

Se deberían verificar en el momento de la recepción, las entregas de sistemas de información y de software provenientes de equipos de desarrollo propios, desarrolladores de sistemas, integradores u otras organizaciones.

El proceso completo se debería documentar en el plan de gestión de la configuración.

10.1.5 Diseñar, construir y configurar una entrega

Los procesos de gestión de la entrega y distribución se deberían diseñar e implementar para:

a) asegurar que existe conformidad con la arquitectura de sistemas, la gestión del servicio y las normas de infraestruc-tura del proveedor del servicio;

b) mantener la integridad durante la construcción, instalación, manipulación, empaquetado y entrega;

c) usar bibliotecas de software y repositorios relacionados para gestionar y controlar los componentes durante los procesos de construcción y de entrega;

d) asegurar que los riesgos estén claramente identificados y que se pueden llevar a cabo acciones de recuperación si se requieren;

e) habilitar verificaciones antes de la instalación para comprobar que la plataforma de destino satisface los requisitos previos;

f) habilitar verificaciones que comprueben que una entrega está completa cuando llega a su destino.

Las salidas de este proceso deberían incluir las notas de la entrega, las instrucciones de instalación y el software y hardware ya instalados, en relación a la línea de referencia de la configuración.

Las salidas de la entrega se deberían entregar al grupo responsable de las pruebas.

Los procesos de construcción, gestión de la entrega y distribución se deberían automatizar para reducir errores, asegurando que el proceso es repetible y que se pueden desplegar rápidamente las nuevas entregas.

10.1.6 Verificación y aceptación de la entrega

El resultado final debería ser una aprobación basada en el grado en el que el paquete completo de la entrega recoge la totalidad de los requisitos.

Los procesos de verificación y aceptación deberían:

a) verificar que el entorno controlado de las pruebas de aceptación se ajusta a los requisitos del entorno de producción de destino;

b) asegurar que la entrega se ha creado a partir de versiones bajo el control de gestión de la configuración y que se han instalado en el entorno de pruebas de aceptación usando el proceso de producción planificado;

c) verificar que se ha completado el nivel adecuado de pruebas, por ejemplo, pruebas funcionales y no funcionales, pruebas de aceptación por el negocio, pruebas en los procedimientos de construcción, despliegue de versiones, distribución e instalación;

d) asegurar que la entrega es probada a la satisfacción de los clientes del negocio y del personal del proveedor del servicio;

e) asegurar que la autoridad apropiada en cuanto a la gestión de la entrega aprueba cada etapa de las pruebas de aceptación;

f) verificar antes de la instalación que la plataforma de destino satisface los requisitos previos de software y hardware;

g) verificar que la entrega está completa cuando llega a su destino.

10.1.7 Documentación

La documentación apropiada debería estar disponible en su totalidad y almacenada según la gestión de la configuración en referencia al elemento de configuración desplegado. Esta documentación debería incluir:

a) la documentación de apoyo, por ejemplo, los acuerdos de nivel de servicio;

b) la documentación de apoyo, por ejemplo, el esquema del sistema, los procedimientos de instalación y de soporte, las ayudas para el diagnóstico y las instrucciones de operación y administración;

c) los procesos de construcción, despliegue de versiones, instalación y distribución;

d) los planes de contingencia y marcha atrás;

e) la planificación de la formación para los responsables del servicio, el personal de apoyo y los clientes;

f) una línea de referencia de la configuración para la entrega, incluyendo elementos de configuración asociados tales como documentación del sistema, entornos de pruebas, documentación de pruebas y versiones de las herramientas de construcción y desarrollo;

g) los cambios, problemas y errores conocidos relacionados;

h) las evidencias de la autorización de la entrega y las evidencias relacionadas de la verificación y la aceptación.

Si un sistema o servicio no cumple completamente con los requisitos especificados para él, antes de pasar a producción se debería identificar y registrar mediante la gestión de la configuración y la gestión del problema.

La información sobre errores conocidos se debería comunicar a la gestión del incidente.

Si la entrega es rechazada, retrasada o cancelada, se debería informar a la gestión del cambio

10.1.8 Despliegue, distribución e instalación

Se debería revisar el plan de despliegue y se deberían añadir detalles, si es necesario, para asegurar que se van a llevar a cabo todas las actividades necesarias.

Es importante que la entrega sea proporcionada de un modo seguro para su destino en el estado esperado. Los procesos de despliegue, distribución e instalación deberían asegurar que:

a) todas las zonas de almacenamiento de hardware y software son seguras;

b) existen procedimientos adecuados para el almacenamiento, expedición, recepción y eliminación de bienes;

c) se planifican y completan las comprobaciones sobre las instalaciones físicas, el entorno, las instalaciones eléctricas y otros servicios;

d) se notifican las nuevas entregas al personal del negocio y del proveedor del servicio;

e) se eliminan los productos, servicios y licencias que quedan sin utilidad tras la nueva entrega.

Después de una distribución de software en una red es esencial comprobar que la entrega está completa y es operativa cuando llega a su destino.

Los registros de activos y de la gestión de la configuración se deberían actualizar con la ubicación y el propietario del software y el hardware tras una instalación llevada a cabo con éxito.

Se debería usar un cuestionario de satisfacción y aceptación por parte del cliente de la instalación para registrar el éxito o el fracaso de dicha instalación. Todos los resultados de las encuestas de satisfacción de los clientes deberían constituir una realimentación para la gestión de las relaciones con el negocio.

10.1.9 Post-implantación y despliegue de la entrega

Se debería medir y analizar el número de incidentes relacionados con una entrega en el periodo inmediatamente posterior a un despliegue para evaluar su impacto en el negocio, en las operaciones y en los recursos de personal de apoyo.

El proceso de gestión del cambio debería incluir una revisión post-implantación.

Las recomendaciones se deberían incluir en un plan de mejora del servicio.

ANEXO A

Directivas generales para la planificación, organización, implantación, operación y supervisión de las tecnologías de la información

1. PLANIFICACIÓN Y ORGANIZACIÓN

1.1 DEFINICIÓN DE UN PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN

1.1.1 Tecnologías de la Información como parte del Plan de la Organización a corto y largo plazo
La máxima 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 Tecnologías de la 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 Tecnologías de la Información
La unidad organizativa que atienda la Informática o las Tecnologías de la Información (en lo adelante dirección de TI) será responsable de desarrollar regularmente planes a largo plazo de Tecnologías de la Información que apoyen el logro de la misión y las metas generales de la organización. De la misma manera, La dirección 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 Tecnologías de la Información - Enfoque y Estructura
La dirección 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 Tecnologías de la Información
La dirección de TI deberá asegurar que se establezca un proceso para modificar oportunamente y con precisión el plan a largo plazo de Tecnologías de la Información con el fin de adaptar los cambios al plan a largo plazo de la organización y los cambios en las condiciones de la Tecnologías de la Información.

1.1.5 Planeación a corto plazo para la Función de Servicios de Información
La dirección de TI deberá asegurar que el plan a largo plazo de Tecnologías de la Información sea traducido regularmente a planes a corto plazo de Tecnologías de la Información. Estos planes a corto plazo deberán asegurar que se asignen los recursos apropiados de la función de servicios de Tecnologías de la Información con una base consistente con el plan a largo plazo de Tecnologías de la 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

Tecnologías de la 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, La dirección de TI 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 Tecnologías de la Información.

1.2.2 Diccionario de Datos y Reglas de Sintaxis de Datos de la Corporación

Deberá asegurarse 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

La dirección 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

La dirección de TI deberá crear y actualizar regularmente un plan de infraestructura tecnológica que concuerde con los planes a largo y corto plazo de Tecnologías de la 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

La dirección 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
La dirección de TI deberá asegurar que los planes de adquisición de hardware y aplicaciones informáticas (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, La dirección 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 vigilar TI y sus actividades. Entre los miembros del comité deberán encontrarse representantes de la alta dirección, 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 a La dirección de TI en la estructura organizacional general, la alta dirección deberá asegurar la existencia de autoridad, actitud crítica e independencia por parte del departamento usuario con un grado tal que sea posible garantizar soluciones de Tecnologías de la Información efectivas y progreso suficiente al implementarlas, así como establecer una relación de sociedad con la alta dirección para incrementar la capacidad de previsión, la comprensión y las habilidades para identificar y resolver problemas de Tecnologías de la 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
La dirección 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 dirección deberá asignar formalmente la responsabilidad de la seguridad lógica y física de los bienes informáticos 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 dirección de 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
La dirección 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
La dirección deberá asegurar que todos los bienes informáticos 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. La dirección 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
- auditoría de seguridad

1.4.11 Asignación de Personal para Tecnologías de la 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 Tecnologías de la 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 Tecnologías de la 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
La dirección 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
La dirección deberá definir e identificar al personal clave de Tecnologías de la Información.

1.4.14 Procedimientos para personal por contrato
La dirección 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 bienes informáticos de información de la organización.

1.4.15 Relaciones
La dirección 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, oficiales de seguridad, gerentes).

1.5 MANEJO DE LA INVERSIÓN EN TECNOLOGÍAS DE LA 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 Tecnologías de la Información. Deberán investigarse alternativas de financiamiento.

1.5.2 Monitoreo de Costo - Beneficios
La dirección 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 Tecnologías de la 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 Tecnologías de la 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
La dirección 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 Tecnologías de la Información.

1.6.2 Responsabilidad de La dirección en cuanto a Políticas
La 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 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 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. La dirección 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

La dirección 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

La dirección 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 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 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
La dirección 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
La dirección 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
La dirección 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
La dirección 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

La dirección 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 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

La dirección 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 Tecnologías de la 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

La dirección deberá asegurar el cumplimiento de los estándares ergonómicos y de seguridad 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

La dirección deberá asegurar el cumplimiento de las regulaciones sobre privacidad o confidencialidad, propiedad intelectual, flujo de datos externos y criptografía aplicables a las prácticas de Tecnologías de la Información de la organización.

1.8.5 Comercio Electrónico

La dirección 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, La dirección 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
La dirección 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
La dirección 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
La dirección deberá establecer un enfoque general para la evaluación de riesgos que defina el alcance 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 bienes informáticos, amenazas, elementos vulnerables y protecciones, tomando en cuenta consecuencias y probabilidad de la 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
La dirección 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
La dirección 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
La dirección 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
La dirección 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 Tecnologías de la 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
La dirección 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) 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
La dirección 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
La dirección 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, La dirección 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
La dirección deberá establecer un proceso para asegurar la coordinación y comunicación estrecha entre los clientes de TI y los implementadores 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 Tecnologías de la Información de calidad que satisfagan las demandas de negocio. La dirección 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
La dirección deberá implementar un proceso para asegurar las buenas relaciones de trabajo con terceras partes como programadores 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
La dirección 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 La dirección de los departamentos usuarios y de 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
La dirección 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
La dirección 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 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
La dirección 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
La dirección 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 abastecimiento
La dirección deberá desarrollar e implementar un enfoque central de abastecimientos que describa un conjunto común de procedimientos y estándares a ser seguidos en la adquisición de hardware, software y servicios relacionados con la Tecnologías de la 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
La dirección deberá asegurar que, para el software con licencia adquirido 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 del órgano de atención a la Informática. 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 del órgano de atención a la Informática 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
La dirección 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
La dirección 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 ADQUISICIÓN 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
La dirección 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 La dirección, por los departamentos usuarios afectados 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 interfaces
La metodología del ciclo de vida de desarrollo de sistemas de la organización debe estipular que se especifiquen, diseñen y documenten apropiadamente todas las interfaces 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 Controlabilidad
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, pruebas de carga y estrés u otras 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
La dirección TI deberá programar 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

La dirección 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 TECNOLOGÍAS DE LA 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 los departamentos usuarios afectados y el grupo de operaciones del órgano de atención a la Informática deberán estar entrenados 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 los Cambios
La dirección deberá asegurar que los cambios sean probados por un grupo de prueba independiente (distinto al de los desarrolladores) 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, 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 La dirección de los departamentos usuarios afectados y del órgano de atención a la Informática. Las pruebas deben cubrir todos los componentes del sistema de información (software de aplicación, instalaciones, tecnología, procedimientos de usuarios).

2.5.7 Pruebas y acreditación de seguridad
La dirección deberá definir e implementar procedimientos para asegurar que La dirección de operaciones y La dirección usuaria aceptan formalmente los resultados de las pruebas y el nivel de seguridad para los sistemas, junto con el riesgo residual existente.

2.5.8 Prueba operacional
La dirección deberá asegurar que, antes de poner el sistema en operación, el usuario o custodio designado (la parte designada para correr 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.

2.5.9 Paso a producción
La dirección deberá definir e implementar procedimientos formales para controlar la entrega del sistema de desarrollo a pruebas 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 CAMBIOS

2.6.1 Inicio y control de solicitudes de cambio
La dirección 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
La dirección 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
La dirección 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
La dirección deberá garantizar que la 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. OPERACIÓN

3.1 DEFINICIÓN DE NIVELES DE SERVICIO

3.1.1 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.

3.1.2 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.

3.1.3 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.

3.1.4 Monitoreo y reporte
La dirección TI deberá designar a un directivo de nivel de servicio 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.

3.1.5 Revisión de convenios y contratos de nivel de servicio
La dirección 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.

3.1.6 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.

3.1.7 Programa de mejoramiento del servicio
La dirección 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.

3.2 GESTIÓN DE SERVICIOS PRESTADOS POR TERCEROS

3.2.1Interfaces con Proveedores
La dirección deberá asegurar que todos los servicios prestados por terceros sean propiamente identificados y que las interfaces técnicas y organizacionales con los proveedores sean documentadas.

3.2.2 Relaciones con terceros
La dirección de la organización del cliente deberá designar un directivo que sea responsable de asegurar la calidad de las relaciones con terceros.

3.2.3 Contratos con terceros
La dirección debe definir procedimientos específicos para asegurar que un contrato formal sea definido y acordado para cada relación de servicio con un proveedor.

3.2.4 Calificación de terceros
La dirección 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

3.2.5 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.

3.2.6 Continuidad de servicios
Con respecto al aseguramiento de la continuidad de los servicios, La dirección 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.

3.2.7 Relaciones de seguridad
Con respecto a las relaciones con los proveedores de servicios como terceras partes, La dirección 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.

3.2.8 Monitoreo
La dirección 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.

3.3 ADMINISTRACIÓN DE DESEMPEÑO Y CAPACIDAD

3.3.1 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.

3.3.2 Plan de disponibilidad
La dirección deberá asegurar el establecimiento de un plan de disponibilidad para alcanzar, monitorear y controlar la disponibilidad de los servicios de información.

3.3.3 Monitoreo y reporte
La dirección deberá implementar un proceso que asegure que el desempeño de los recursos de Tecnologías de la Información sea continuamente monitoreado y que las excepciones sean reportadas de manera oportuna y completa.

3.3.4 Herramientas de modelado
La dirección 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.

3.3.5 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.

3.3.6 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.

3.3.7 Administración de capacidad de recursos
La dirección 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 requerida, prescrita en los acuerdos de nivel de servicio. El plan de capacidad deberá cubrir escenarios múltiples.

3.3.8 Disponibilidad de recursos
La dirección 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.

3.3.9 Calendarización de recursos
La dirección deberá asegurar la adquisición oportuna de la capacidad requerida, tomando en cuenta aspectos como resistencia, contingencia, cargas de trabajo y planes de almacenamiento.

3.4 ASEGURAR LA CONTINUIDAD DEL SERVICIO

3.4.1 Marco de referencia de contingencia de Tecnologías de la Información
La dirección 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.

3.4.2 Estrategia y filosofía de contingencia de Tecnologías de la Información
La dirección deberá garantizar que el Plan de contingencia de Tecnologías de la 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 Tecnologías de la Información, con el fin de asegurar consistencia.

3.4.3 Contenido del plan de contingencia de Tecnologías de la Información
La dirección 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 dirección e información crítica sobre grupos de contingencia, personal afectado, clientes, proveedores, autoridades públicas y medios de comunicación.

3.4.4 Minimización de requisitos de contingencia de Tecnologías de la Información.
La dirección de servicios de información deberá establecer procedimientos y guías para minimizar los requisitos de contingencia con respecto a personal, instalaciones, hardware, software, equipo, formatos, consumibles y mobiliario.

3.4.5 Mantenimiento plan de contingencia de Tecnologías de la Información
La dirección 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.

3.4.6 Pruebas del plan de contingencias de Tecnologías de la Información
Para contar con un plan efectivo de contingencias, La 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.

3.4.7 Capacitación sobre el plan de contingencias de Tecnologías de la 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.

3.4.8 Distribución del plan de contingencia de Tecnologías de la 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.

3.4.9 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.

3.4.10 Recursos críticos de Tecnologías de la 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.

3.4.11 Centro de datos y hardware de respaldo
La dirección 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.

3.4.12 Procedimiento de refinamiento del plan de contingencia
Dada una exitosa reanudación del órgano de atención a la Informática después de un desastre, La dirección de servicios de información deberá establecer procedimientos para evaluar lo adecuado del plan y actualizarlo de acuerdo con los resultados de dicha evaluación.

3.5 GARANTIZAR LA SEGURIDAD DE SISTEMAS

3.5.1 Administrar medidas de seguridad
La seguridad en Tecnologías de la 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 Tecnologías de la Información; actualizar el plan de seguridad de Tecnologías de la Información para reflejar cambios en la configuración de tecnología; evaluar el impacto de solicitudes de cambio en la seguridad de Tecnologías de la Información; monitorear la implementación del plan de seguridad de Tecnologías de la Información; y alinear los procedimientos de seguridad de Tecnologías de la Información a otras políticas y procedimientos

3.5.2 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).

3.5.3 Seguridad de acceso a datos en línea
En un ambiente de Tecnologías de la Información en línea, la dirección 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.

3.5.4 Administración de cuentas de usuario
La dirección 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.

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

3.5.6 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.

3.5.7 Vigilancia de seguridad
La administración de seguridad del órgano de atención a la Informática 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.

3.5.8 Clasificación de datos
La dirección 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.

3.5.9 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.

3.5.10 Reportes de violación y de actividades de seguridad
La administración del órgano de atención a la Informática 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).

3.5.11 Manejo de incidentes
La dirección 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.

3.5.12 Re-acreditación
La 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.

3.5.13 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.

3.5.14 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.

3.5.15 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.

3.5.16 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.

3.5.17 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.

3.5.18 Administración de llaves criptográficas
La dirección 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), La dirección 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.

3.5.19 Prevención, detección y corrección de software "malicioso"
Con respecto al software malicioso, tal como los virus computacionales o Caballos de Troya, La dirección deberá establecer un marco de referencia de adecuadas medidas de control preventivas, de detección y correctivas.

3.5.20 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.

3.5.21 Protección de valores electrónicos
La dirección 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.

3.6 IDENTIFICACIÓN Y ASIGNACIÓN DE COSTOS

3.6.1 Elementos sujetos a cargo
La dirección 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.

3.6.2 Procedimientos de costo
La dirección 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 del órgano de atención a la Informática, a la luz de los otros sistemas de medición financiera de la organización.

3.6.3 Procedimientos de cargo y facturación a usuarios
La dirección 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.

3.7 EDUCACIÓN Y ENTRENAMIENTO DE USUARIOS

3.7.1 Identificación de necesidades de entrenamiento
En línea con el plan a largo plazo, La dirección 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.

3.7.2 Organización del entrenamiento
Tomando como base las necesidades identificadas, La dirección 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).

3.7.3 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 del órgano de atención a la Informática, 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.

3.8 APOYO Y ASISTENCIA A LOS CLIENTES DE TECNOLOGÍAS DE LA INFORMACIÓN

3.8.1 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.

3.8.2 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.

3.8.3 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 del órgano de atención a la Informática hasta el nivel adecuado para atenderlas.

3.8.4 Monitoreo de atención a clientes
La dirección 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.

3.8.5 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.

3.9 GESTIÓN DE LA CONFIGURACIÓN

3.9.1 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.

3.9.2 Configuración base
La dirección TI deberá asegurarse de que exista una configuración base de elementos como punto de verificación al cual regresar después de las modificaciones.

3.9.3 Registro de estatus
La dirección 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.

3.9.4 Control de la configuración
Los procedimientos deberán asegurar que la existencia y consistencia del registro de la configuración del órgano de atención a la Informática sean revisadas periódicamente.

3.9.5 Software no autorizado
La dirección TI deberá revisar periódicamente la existencia de software no autorizado en las computadoras personales de la organización.

3.9.6 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.

3.10 ADMINISTRACIÓN DE PROBLEMAS E INCIDENTES

3.10.1 Sistema de administración de problemas
La dirección 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.

3.10.2 Escalamiento de problemas
La 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 Tecnologías de la Información.

3.10.3 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.

3.11 ADMINISTRACIÓN DE DATOS

3.11.1 Procedimientos de preparación de datos
La dirección deberá establecer procedimientos de preparación de datos a ser seguidos por los departamentos 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.

3.11.2 Procedimientos de autorización de documentos fuente
La dirección 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.

3.11.3 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.

3.11.4 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.

3.11.5 Retención de documentos fuente

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

3.11.6 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.

3.11.7 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.

3.11.8 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.

3.11.9 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.

3.11.10 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 ubica2dos en una infraestructura de control interactiva con operadores humanos para asegurar que las decisiones vitales son aprobadas.

3.11.11 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.

3.11.12 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 Tecnologías de la 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.

3.11.13 Distribución de datos de salida
La organización deberá establecer y comunicar procedimientos escritos para la distribución de datos de salida de Tecnologías de la Información.

3.11.14 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.

3.11.15 Revisión de datos de salida y manejo de errores
La 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.

3.11.16 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.

3.11.17 Protección de información sensible durante transmisión y transporte
La dirección 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.

3.11.18 Protección de información crítica a ser desechada
La dirección 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.

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

3.11.20 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.

3.11.21 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.

3.11.22 Responsabilidades de la administración de la librería de medios
La dirección 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.

3.11.23 Respaldo y restauración
La dirección 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.

3.11.24 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.

3.11.25 Almacenamiento de respaldos
Los procedimientos de respaldo para los medios relacionados con Tecnologías de la 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.

3.11.26 Archivo
La 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.

3.11.27 Protección de mensajes sensitivos
Con respecto a la transmisión de datos a través de Internet u otra red pública, La dirección deberá definir e implementar procedimientos y protocolos para ser utilizados para el aseguramiento de la integridad, confidencialidad y “no negación” de mensajes sensitivos.

3.11.28 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.

3.11.29 Integridad de transacciones electrónicas
Tomando en consideración que las fronteras tradicionales de tiempo y de geografía son menos precisas y confiables, La dirección 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)

3.11.30 Integridad continua de datos almacenados
La dirección 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.

3.12 ADMINISTRACIÓN DE INSTALACIONES

3.12.1 Seguridad física
Deberán establecerse apropiadas medidas de seguridad física y control de acceso para las instalaciones de Tecnologías de la 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.

3.12.2 Discreción de las instalaciones de Tecnologías de la Información
La dirección TI deberá asegurar que se lleve un bajo perfil ó discreción y que la identificación física de las instalaciones relacionadas con sus operaciones de Tecnologías de la Información sea limitada.

3.12.3 Escolta de Visitantes
Deberán establecerse procedimientos apropiados que aseguren que las personas que no formen parte del grupo de operaciones del órgano de atención a la Informática 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.

3.12.4 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.

3.12.5 Protección contra factores ambientales
La dirección 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.

3.12.6 Suministro ininterrumpido de energía
La dirección deberá evaluar regularmente la necesidad de generadores y baterías de suministro ininterrumpido de energía para las aplicaciones críticas de Tecnologías de la Información, con el fin de asegurarse contra fallas y fluctuaciones de energía. Cuando sea justificable, deberá instalarse el equipo más apropiado.

3.13 ADMINISTRACIÓN DE OPERACIONES

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

3.13.2 Documentación del proceso de inicio y de otras operaciones
La dirección 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.

3.13.3 Calendarización de trabajos
La dirección 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. Los programas iniciales así como los cambios a estas programaciones deberán ser autorizados apropiadamente.

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

3.13.5 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.

3.13.6 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.

3.13.7 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.

4. SUPERVISIÓN (MONITOREO)

4.1 MONITOREO DEL PROCESO

4.1.1 Recolección de datos de monitoreo
Para los procesos de Tecnologías de la 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.

4.1.2 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.

4.1.3 Evaluación de la satisfacción de clientes
A intervalos regulares, La dirección 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.

4.1.4 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, La dirección deberá iniciar y controlar las acciones pertinentes.

4.2 EVALUAR LO ADECUADO DEL CONTROL INTERNO

4.2.1 Monitoreo de control interno
La dirección 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.

4.2.2 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 dirección.

4.2.3 Reporte sobre el nivel de control interno
La dirección 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.

4.2.4 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 "autoauditoría" 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 La dirección deberán revisar la existencia de puntos vulnerables y problemas de seguridad.

4.3 OBTENCIÓN DE EVALUACION INDEPENDIENTE

4.3.1 Certificación / acreditación independiente de control y seguridad de los servicios de TI
La dirección deberá obtener una certificación o acreditación independiente de seguridad y control interno antes de implementar nuevos servicios de Tecnologías de la 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.

4.3.2 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 Tecnologías de la Información y obtener re-certificaciones o re-acreditaciones de estas actividades en forma cíclica rutinaria.

4.3.3 Evaluación Independiente de la efectividad de los servicios de TI
La dirección deberá obtener una evaluación independiente sobre la efectividad de los servicios de Tecnologías de la Información en forma cíclica rutinaria.

4.3.4 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 Tecnologías de la Información en forma cíclica rutinaria.

4.3.5 Evaluación independiente del cumplimiento de leyes y requisitos regulatorios y compromisos contractuales
La dirección deberá obtener un aseguramiento independiente sobre el cumplimiento de la función de servicios de Tecnologías de la Información con respecto a requisitos regulatorios y compromisos contractuales en forma cíclica rutinaria.

4.3.6 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 Tecnologías de la Información con respecto a requisitos regulatorios y compromisos contractuales en forma cíclica rutinaria.

4.3.7 Competencia de la función de evaluación independiente
La dirección 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.

4.3.8 Participación proactiva de auditoría
La dirección de Tecnologías de la Información deberá buscar la participación de auditoría en una forma proactiva, antes de finalizar soluciones de servicio de Tecnologías de la Información.

4.4 PROVEER AUDITORÍA INDEPENDIENTE

4.4.1 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.

4.4.2 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.

4.4.3 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 cubanas, 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 Tecnologías de la Información.

4.4.4 Competencia
La dirección deberá asegurar que los auditores responsables de las revisiones de las actividades del órgano de atención a la Informática 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. La dirección 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.

4.4.5 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 del órgano de atención a la Informática. 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.

4.4.6 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.

Bibliografía

[I] NC-ISO-IEC 20000-1 Tecnología de la información. Gestión del servicio. Parte 1: Especificaciones.

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

[3] NC-ISO 10007 Sistemas de gestión de la calidad. Directrices para la gestión de la configuración.

[4] NC-ISO 9000 Sistemas de gestión de la calidad. Fundamentos y vocabulario.

[5] NC-ISO 9001 Sistemas de gestión de la calidad. Requisitos.

[6] NC-ISO/IEC 90003 Ingeniería del software. Guía de aplicación de la ISO 9001:2000 al software.

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

[8] 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).

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

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

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

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

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

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

[15] 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.

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