ACUERDO #

00002126

La Defensoría de los Habitantes

LA DEFENSORA DE LOS HABITANTES

Con fundamento en los artículos 1 y 2 de la Ley de la Defensoría de los Habitantes de la República, Ley Nº 7319 publicada en La Gaceta Nº 237 del 10 de diciembre de 1992; los artículos 1, 3, 8, 9, incisos a), d) y e), 20, 63 y 66 del Reglamento a dicha Ley, Decreto Ejecutivo Nº 22266-J del 16 de julio de 1993; los artículos 4, 6, 10, 11, 13, 16 párrafo primero, 103 párrafos primero y tercero, 112 párrafo primero y 113 de la Ley General de la Administración Pública, Ley Nº 6227, y los artículos 23 y 27 del Estatuto Autónomo de Organización de la Defensoría de los Habitantes de la República, Acuerdo N° 528-DH del 9 de mayo de 2001, y

CONSIDERANDO

I.- Que el ordenamiento jurídico costarricense otorga a las y los jerarcas de los entes y órganos públicos amplios poderes de dirección y control respecto a la gestión institucional, y los faculta para adoptar las medidas que consideren necesarias con el propósito de garantizar que la prestación del servicio público encomendado se brinde bajo los más altos parámetros de eficiencia y eficacia.

II.- Que la Defensora de los Habitantes de la República es la máxima autoridad en la organización, dirección y coordinación en el funcionamiento de la institución.

III.- Que la Administración Pública, dado el estado actual de avance de la humanidad en el marco de la sociedad de la información, se ha tenido que adaptar dentro de lo que se ha denominado como gobierno electrónico, concretamente Administraciones Públicas Electrónicas, que son aquellas que: "*usan de manera extensiva e intensiva las tecnologías de la información y la comunicación en su organización, funciones, competencias y relaciones internas y externas, con los fines de racionalizar el gasto público, mejorar la calidad de los servicios públicos, obtener mayores grados de eficiencia y eficacia, y participación ciudadana y facilitar la rendición de cuentas y la evaluación del desempeño.*"[1]

IV.- Que con la introducción de las TIC´s en la Administración Pública se busca un Estado con mayores niveles democráticos en un sentido amplio del concepto que no se limita únicamente a la participación, por cuanto además del lógico mejoramiento de ese estándar concreto, necesariamente acarrea un mejoramiento general en la realización de cada una de las funciones que competen al poder público, que no tienen otro objeto más que la satisfacción de los intereses de todas las personas de una manera cada vez más ágil y oportuna.

V.- Que dentro de este panorama se torna necesario que la Defensoría regule una serie de procedimientos y estándares mínimos vinculados con el manejo de la tecnología, en aras de clarificar los procesos internos y tener una base normativa a partir de la cual la institución pueda mejorar la prestación del servicio que se brinda a los y las habitantes. **Por tanto**;

[1] Jinesta Lobo (Ernesto): Tratado de Derecho Administrativo. Tomo I. Parte General. --3ª. 2ed.—San José, C.R.:Editorial Jurídica Continental, 2009. pp 185 y 186.

SE ACUERDA

ÚNICO.- Emitir el siguiente compendio de lineamientos, políticas y estándares en materia tecnológica que entrará a regir en la Defensoría de los Habitantes, el cual estará compuesto por los siguientes instrumentos:

Políticas y lineamientos generales para la Seguridad de la Información

1. Objetivo

Establecer los lineamientos globales para gestionar eficientemente la seguridad de la información dentro de la institución.

2. Responsables

Es responsabilidad del Jefe de Informática y de los colaboradores del departamento de Tecnología de Información velar por la comunicación, el cumplimiento y la mejora de estas políticas.

Es responsabilidad del Comité de TI (creado mediante Acuerdo N°2074 referido a la Comisión Institucional de Tecnologías de la Información (CITI)) apoyar al departamento de Tecnología de Información en la aplicación de las políticas, establecer los mecanismos requeridos para comunicar efectivamente dichas políticas, y establecer controles o sanciones que logren prevenir o resolver el desacato de estas políticas por parte de los involucrados.

3. Definiciones

Amenaza: Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización.

Confidencialidad: se refiere a la necesidad de generar confianza y seguridad, para bloquear el acceso a los activos de TI, por personas, entidades o procesos no autorizados para su uso.

Disponibilidad: se refiere a la capacidad de acceso y uso de los activos de TI, por parte de entidades autorizadas.

Incidente: Cualquier evento que no sea parte de la operación estándar de un servicio que ocasione, o pueda ocasionar, una interrupción o una reducción de la calidad de ese servicio (alineado a ITIL).

Integridad: se refiere a la precisión, completitud y resguardo de un activo de TI.

Riesgo: Es la posibilidad de pérdidas económicas debido a eventos adversos. Entre otros riesgos, pero no limitados a estos, las entidades financieras pueden enfrentar riesgo de crédito, riesgo de precio, riesgo de tasas de interés, riesgo de tipo de cambio, riesgo de liquidez, riesgo operativo, riesgo de tecnologías de información, riesgo legal, riesgo de imagen, riesgo de cumplimiento, Riesgo de gobernabilidad y riesgo de conglomerado.

Riesgo de Tecnologías de Información (TI): El riesgo de TI es la posibilidad de pérdidas económicas y no económicas derivadas de un evento relacionado con el acceso o uso de la tecnología, que afecta el desarrollo de los procesos del negocio y la gestión de riesgos de la entidad, al atentar contra la confidencialidad, integridad, disponibilidad, eficiencia, confiabilidad y oportunidad de la información.

Respaldo: toda aquella información que es copia del original y que es obtenida para asegurar la accesibilidad en caso de contingencia.

TI: Tecnología de Información.

Vulnerabilidad: La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

4. Políticas

1. Sobre el marco de trabajo asociado a la Seguridad de la Información

La institución debe ejecutar actividades de forma continua que le permitan un abordaje global e integral de la identificación y gestión de los riesgos asociados a la Seguridad de la Información. Sobre este abordaje integral, el Departamento de Informática mantendrá políticas que mitiguen los riesgos de Seguridad de la Información relacionados con el uso de la tecnología de información. Para asegurar que sea integral, se deberá considerar dentro de la gestión otros elementos complementarios:

a. Administración de riesgos de TI: que permite mantener un proceso estándar para la identificación, evaluación, respuesta, mantenimiento y monitoreo de riesgos de TI.
b. Plan de continuidad de TI: que debe contemplar la construcción y mantenimiento del plan de continuidad de TI acorde a las necesidades de la institución.
c. Almacenamiento y recuperación de información: que mantiene las actividades y responsabilidades al ejecutar y recuperar respaldos de información.
d. Seguridad física y lógica: que permita la administración de la seguridad de la información.
e. Seguridad del centro de datos: que establece los requisitos para una adecuada seguridad física de las instalaciones del centro de procesamiento de datos.

f. Reglas de utilización e intercambio de datos: que permite establecer para cada intercambio de datos, según los principios de transparencia del estado y los de confidencialidad, integridad y disponibilidad de la información, acuerdos de protección y uso de datos.

2. Sobre el universo de riesgos de TI

Los riesgos de TI son considerados parte de los riesgos operativos de la institución y su alcance está delimitado a aquellos activos de tecnología que la institución utiliza para ejecutar sus labores. Para asegurar el alineamiento con el negocio este universo de riesgos de TI deberá considerar:

a. Los procesos de negocio que son críticos para la institución
b. Las directrices, definiciones, esquemas, etc. de gestión del riesgo dictadas para toda la institución
c. El cumplimiento de los acuerdos de niveles de los servicios de TI que se han trasladado a terceros para su ejecución

3. Sobre la comunicación de los riesgos de TI

Es responsabilidad de las áreas involucradas en la gestión de TI comunicar a los jerarcas de la institución la información relevante relacionada con los riesgos de TI, a fin de adoptar las decisiones y emitir la normativa interna correspondiente.

4. Sobre los acatamientos generales de seguridad que deben seguir los colaboradores de Informática.

Las principales funciones y responsabilidades de los colaboradores de Informática se encuentran delimitadas en sus perfiles de puestos, pero es importante destacar las siguientes:

a. El Departamento de Informática es el responsable de ejecutar el mantenimiento preventivo y correctivo sobre los activos de TI de la institución.
b. Para todo activo de TI que cambie su ubicación y vaya a ser utilizado por otro usuario, se deberá validar que no contenga datos ni instalaciones del usuario o función anterior.
c. El inventario físico deberá actualizarse cada vez que se realice un cambio de ubicación de un equipo, que se cambien sus características, que se realice una donación, que se clasifique un equipo como "obsoleto", que se deseche físicamente.
d. El Departamento de Informática es responsable de disponer de herramientas de control que detecten cambios en el software o hardware instalado y autorizado.
e. El Departamento de Informática es el responsable de asegurar que todos los esquemas, sistemas y modelos que soporten la seguridad de la información sean revisados y validados para ajustar su aplicación a las necesidades crecientes de la institución
f. El Departamento de Informática es el responsable del funcionamiento de la red por ello deberá asegurar que:
    - El cableado de red sea estructurado y que cumpla con los estándares del mercado.

- La definición de las redes debe considerar la seguridad necesaria para proteger la información y la continuidad de los procesos de la institución; por lo que deberá contemplar los medios necesarios para restringir el tráfico hacia dentro y fuera de la red.
- La red debe estar protegida por medio de un anillo de seguridad perimetral que analice el tráfico de datos que ingresa a la red institucional y contenga las políticas necesarias para impedir el acceso de tráfico no deseado.
- Los usuarios de acceso remoto deben ser autenticados según las directivas de seguridad de red basados en VPNs seguras suministradas por el Departamento de Informática.

g. Los usuarios solo deben tener acceso a los espacios lógicos, servicios y aplicaciones para los cuales han sido autorizados a través de su perfil (sistemas de información, sistemas operativos y bases de datos).
h. El Departamento de Informática es el responsable de establecer las políticas generales de programas de antivirus, antispam y otras amenazas de naturaleza cibernética.
i. El Departamento de Informática es el responsable de implementar un adecuado monitoreo para establecer un esquema preventivo de fallas, este monitoreo debe ayudar a la resolución de problemas.
j. Se debe mantener una bitácora que contenga pistas de auditoría que faciliten la búsqueda de un patrón o de un problema, así como para dar seguimiento a las transacciones que se ejecutan en los sistemas de información, bases de datos y sistemas operativos.
k. Aunque el Departamento de Informática puede utilizar los mecanismos antes descritos en procesos de autoevaluaciones o revisiones. Éstas no sustituirán los procesos de auditoría. Adicionalmente los procesos de auditoría no podrán ser efectuados por los mismos responsables del Departamento de Informática .
l. El acceso a sistemas operativos o sistemas con funcionalidades de uso especializado en servidores, equipo de telecomunicaciones, etc. debe ser limitado a personal con conocimiento técnico calificado para su uso.
m. El Departamento de Informática es el responsable de establecer el plan de contingencia que garantiza la recuperación de información relevante y la continuidad en la prestación de los servicios.
n. Es responsabilidad de los colaboradores del Departamento de Informática seguir y utilizar durante la ejecución de sus labores reglamentos, políticas, procedimientos, instructivos, formularios, estándares, etc. que han sido establecidas para el funcionamiento del departamento.
o. Es responsabilidad de los colaboradores del Departamento de Informática hacer uso adecuado de los recursos y las herramientas que son proporcionadas por la institución, con el propósito de mejorar constantemente el desempeño de sus labores.
p. Es responsabilidad de los colaboradores del Departamento de Informática mantener estricta confidencialidad sobre la información que pueden acceder por la naturaleza de

sus labores, esta información no puede ser revelada ni formal o informalmente, ni puede ser utilizada en beneficio.

q. Es responsabilidad de los colaboradores del Departamento de Informática velar por el cumplimiento de los acuerdos de confidencialidad de la información que se establezcan en las integraciones de sistemas con terceros o uso de los sistemas de terceros. Esta acción se deberá considerar desde las etapas de adquisición y/o desarrollo de software.

5. Sobre el respaldo de la información

a) El Departamento de Informática debe mantener las copias necesarias de la información que se encuentra en los discos duros de los servidores, en medios magnéticos, de manera que permita su rápida recuperación y la restauración del servicio en el menor tiempo posible.

b) El Jefe del Departamento de Informática deberá establecer, de acuerdo con la disponibilidad de recursos del Departamento de Informática, un proceso periódico que considere los respaldos diarios, semanales, mensuales y anuales, que incluya toda la información crítica de la empresa.

c) Este ciclo deberá cumplirse estrictamente con el cronograma de respaldos establecido y con los horarios configurados.

d) La información de cada sistema debe ser respaldada regularmente sobre un medio de almacenamiento como cinta, dispositivo de almacenamiento masivo externo, CD, DVD, etc.

e) Los administradores de los servidores, los sistemas de información o los equipos de comunicaciones, son los responsables de definir la frecuencia de respaldo y los requerimientos de seguridad de la información (codificación) y el administrador del sistema de respaldo, es el responsable de realizar los respaldos periódicos.

f) Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso.

g) Las copias de respaldo se guardarán únicamente con el objetivo de restaurar el sistema luego de un virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, materialización de amenazas, catástrofes y por requerimiento legal.

h) Ningún tipo de información institucional puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo; por lo tanto, es obligación de los usuarios finales realizar las copias en los repositorios destinados para este fin.

i) Debe existir al menos una copia de la información de los discos de red, la cual deberá permanecer fuera de las instalaciones de la Defensoría de los Habitantes.

j) La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información.

k) Semanalmente los administradores de infraestructura de la Defensoría de los Habitantes, verificarán la correcta ejecución de los procesos de backup y controlarán la vida útil de cada dispositivo (cinta, dispositivo de almacenamiento masivo externo, CD, DVD, etc.) o medio empleado.

6. Sobre la administración de la identidad

El departamento de informática debe asegurar que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, entorno de TI, operación de sistemas, desarrollo y mantenimiento) deben ser identificables de manera única. Los nombres de los usuarios genéricos deben ser asociados a una única identidad física de manera que se puedan establecer la responsabilidad de uso entre el usuario y la persona que utiliza dicho usuario, eso significa que un mismo usuario no puede ser asignado a varias personas.

7. Sobre la seguridad física

Se deberán acatar las siguientes políticas para resguardar la seguridad física:

a. El acceso físico a las instalaciones está regulado por el esquema de seguridad física de la institución.
b. El acceso físico a las áreas que contienen los activos de TI requeridos para entregar servicios esenciales de TI, se encuentra restringido y está regulado por los esquemas de seguridad física de TI.
c. Solo el personal autorizado de Informática tiene acceso a las áreas restringidas como cuartos de servidores, cuartos de telecomunicaciones, paneles de control, área de trabajo de los técnicos, etc.
d. La limpieza de los espacios restringidos antes mencionados, debe mantener una serie de reglas establecidas con Departamento de Informática para ser ejecutada de forma adecuada y velar por la protección de la información.
e. Solo los terceros autorizados pueden ingresar en los espacios restringidos y su ingreso se debe dar con la presencia de algún colaborador del Departamento de Informática autorizado para esta labor.
f. En los espacios restringidos no se puede ingresar con alimentos, bebidas, materiales inflamables, u otros elementos que pongan en riesgo el activo.
g. Si por razones protocolarias se traslada temporalmente o parcialmente la custodia de dichos activos se deberá tener una autorización del Jefe del Departamento de Informática, y acatando el procedimiento establecido para la administración de los Activos Fijos de la institución.
h. El ingreso a los centros de procesamiento de datos y áreas de acceso general del Departamento de Informática debe estar justificado por la actividad que lleva a cabo la institución.
i. El acceso directo al cuarto de servidores queda totalmente restringido a únicamente personal del Departamento de Informática que por sus funciones específicas requieran ingresar.

8. Sobre el uso de los activos de TI

Todo colaborador que haga uso de un activo de TI debe acatar las siguientes políticas:

a. El uso de los activos de TI es exclusivo para ejecutar actividades relacionadas con la institución, y no podrá ser utilizado para otros fines.
b. El Departamento de Informática tendrá administradores autorizados para la instalación de software, ningún usuario final podrá instalar o desinstalar software de sus activos de TI.
c. El Departamento de Informática contará con herramientas y directivas de control que impidan o detecten cambios en el software o hardware instalado y autorizado.
d. El Departamento de Informática establecerá el software autorizado que será el único a ser utilizado en los activos de TI
e. Toda la información, licencias y uso de software debe ser legal y aprobado por los responsables de los activos de TI.
f. Cualquier incorporación de nuevo software o hardware dentro de la plataforma de TI de la institución, debe ser instalado y configurado por personal del Departamento de Informática para disminuir cualquier riesgo.
g. La información personal como música, fotografías personales, videos, etc. que no sea de interés para la institución no deberá mantenerse en los activos de TI de la institución.
h. Aquella información que sea de interés para la institución que consuma una alta tasa de espacio de almacenamiento, o que se clasifica como música, videos, fotografías, etc., deberá ser reportada a los responsables de TI para buscar una fuente alterna de almacenamiento y respaldo, y así no afecte el desempeño del recurso compartido.
i. Cada vez que un usuario necesite dejar su puesto de trabajo deberá asegurarse de no dejar expuesta información sensible o de acceso restringido.
j. Cada vez que un usuario necesite dejar su puesto de trabajo debe bloquear su usuario en su PC o dispositivo móvil para evitar que otras personas hagan robo de su identidad.
k. Es responsabilidad de los usuarios proteger y resguardar el acceso de otras personas, a programas o servicios que estén relacionados con la identidad del usuario (correo, firmas electrónicas, opciones de sistemas de información, etc.)
l. Cada colaborador que reciba un activo de TI para ejecutar sus labores o para custodiarlo debe velar por el uso adecuado de dicho activo.
m. Los colaboradores o terceros que cesen las labores para la institución deberán devolver los activos de TI que, están en su custodia o le han sido asignados para su uso, estos activos deben estar en perfecto estado.
n. El Departamento de Informática debe proporcionar mecanismos lógicos o físicos que protejan la información confidencial o sensible para la institución.
o. Cualquier daño accidental o intencional a un activo de TI será objeto de una investigación y si se determina negligencia por parte del usuario, éste se someterá a los procedimientos administrativos correspondientes.
p. Para aquellos activos de TI que están expuestos a ser dañados por desastres naturales, se deberán tomar medidas para considerar evitar o minimizar dichos riesgos.

9. Sobre responsabilidades de los usuarios

a. La Defensoría de los Habitantes suministra una cuota de almacenamiento para la información en un servidor de archivos con los permisos necesarios para que cada usuario guarde la información que catalogue como importante y sobre ella se garantizará la disponibilidad en caso de un daño en el equipo asignado.
b. El Departamento de Informática instalará copia de los programas que han sido adquiridos legalmente en los equipos asignados en las cantidades requeridas para suplir las necesidades. En el caso que no se cuente con el respectivo licenciamiento se instalarán los aplicativos necesarios equivalentes en tecnologías de Software Libre o Código Abierto. El uso de programas sin su respectiva licencia y autorización del Departamento de Informática (imágenes, vídeos, software o música), obtenidos a partir de otras fuentes (internet, dispositivos de almacenamiento externo), puede implicar amenazas legales y de seguridad de la información para la entidad, por lo que esta práctica no está autorizada.
c. Todo el software usado en la plataforma tecnológica de la Defensoría de los Habitantes debe tener su respectiva licencia, acorde con los derechos de autor. En caso contrario utilizar herramientas de Software Libre para satisfacer las necesidades y requerimientos.
d. Los programas instalados en los equipos, son de propiedad de la Defensoría de los Habitantes, la copia no autorizada de programas o de su documentación, implica una violación a la ley por lo tanto aquellos funcionarios, contratistas o demás colaboradores que utilicen copias no autorizadas de programas o su respectiva documentación, quedarán sujetos a las sanciones que especifique la ley.
e. La Defensoría de los Habitantes se reserva el derecho de proteger su buen nombre y sus inversiones en hardware y software, fomentando controles internos para prevenir el uso o la realización de copias no autorizadas de los programas de propiedad de la entidad. Estos controles pueden incluir valoraciones periódicas del uso de los programas, auditorías anunciadas y no anunciadas.
f. Los recursos tecnológicos y de software asignados a las y los funcionarios de la Defensoría de los Habitantes son responsabilidad de cada funcionario.
g. Los usuarios son los responsables de la información que administran en sus equipos personales y deben abstenerse de almacenar en ellos información no institucional.
h. Los dispositivos electrónicos (computadores, impresoras, fotocopiadoras, escáner, etc.) solo deben utilizarse para los fines autorizados por la entidad.

10. Sobre responsabilidades del personal de Tecnologías de Información

a. La Administración institucional de la Defensoría de los Habitantes, en conjunto con el Departamento de Informática deberán propiciar actividades para concientizar al personal sobre las precauciones necesarias que deben realizar los usuarios finales, para evitar revelar información confidencial por medio de conversaciones telefónicas, envío de correos, sms, capturas de pantalla, entre otros.

b. Los datos de los sistemas de información y aplicaciones no deben intercambiarse utilizando archivos compartidos en los computadores, discos virtuales, CD, DVD, medios removibles; deben usarse los mismos servicios del sistema de información, los cuales están controlados y auditados.
c. El personal del Departamento de Informática no debe dar a conocer su clave de usuario a terceros bajo ninguna circunstancia.
d. Los usuarios y claves de los administradores de sistemas y del personal del Departamento de Informática son de uso personal e intransferible.
e. El personal del Departamento de Informática debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la entidad de acuerdo con el rol asignado.
f. Los documentos y en general la información de procedimientos, seriales, software etc. deben mantenerse custodiados en todo momento para evitar el acceso a personas no autorizadas.
g. Para el cambio o retiro de equipos de funcionarios, se deben seguir políticas de saneamiento, es decir llevar a cabo mejores prácticas para la eliminación de la información de acuerdo con el software disponible en la entidad. Por ejemplo: Formateo seguro, destrucción total de documentos o borrado seguro de equipos electrónicos.
h. Los funcionarios encargados de realizar la instalación o distribución de software, sólo instalarán productos con licencia y software autorizado o en su defecto Software Libre.
i. Los funcionarios del Departamento de Informática tienen el deber ético y profesional de no revelar a terceras personas, la información a la que tengan acceso en el ejercicio de sus funciones. En consecuencia, se obligan a mantenerla de manera confidencial, privada y a protegerla para evitar su divulgación.
j. Los funcionarios del Departamento de Informática no utilizarán la información para fines comerciales o diferentes al ejercicio de sus funciones.
k. Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro.
l. Las copias licenciadas y registradas del software adquirido, deben ser únicamente instaladas en los equipos y servidores de la entidad. Se deben hacer copias de seguridad en concordancia con las políticas del proveedor y de la entidad.
m. La copia de programas o documentación, requiere tener la aprobación escrita del Departamento de Informática de la Defensoría de los Habitantes y del proveedor si éste lo exige.
n. El personal del Departamento de Informática debe velar por que se cumpla con el registro en la bitácora de acceso al Centro de Datos, de las personas que hayan sido autorizadas para que ingresen; las cuales en todo momento deben de ser supervisadas.
o. El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado.
p. Todos los servidores deben ser configurados con el mínimo de servicios necesarios y obligatorios para desarrollar las funciones designadas.

q. Estarán bajo custodia del Departamento de Informática los medios magnéticos/electrónicos (CDs, DVDs, u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso, adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y los passwords de administración de los equipos informáticos, sistemas de información o aplicativos.
r. El Departamento de Informática no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean de la Defensoría de los Habitantes.

11. Sobre la administración de la identidad

Todos los usuarios (internos, externos y temporales) deben asegurarse que tiene asignada una clave de acceso que les garantice para poder acceder a los diferentes sistemas de aplicación, herramientas de oficinas, portal, acceso a Internet y uso de aplicaciones de terceros. Todo usuario debe ser identificado de manera única dentro del entorno de tecnologías de información.

Está completamente prohibido prestar o revelar nombres de usuario o claves de acceso.

12. Sobre virus y spam

El Departamento de Informática mantiene una serie de controles automáticos para la detección y eliminación de virus y correos "spam" (no deseado), pero es responsabilidad del usuario hacer un uso adecuado de los mismos y no deshabilitarlos.

13. Sobre el uso de redes inalámbricas

El Departamento de Informática definirá, cuando menos, una red pública y una red privada para el acceso a las redes inalámbricas de la institución por parte de visitantes y de personal interno.

Políticas para la gestión de la operación y administración de la capacidad

5. Objetivo

Establecer los lineamientos globales para gestionar eficientemente los servicios de tecnología de información, así como los recursos asignados apoyar dichos servicios.

6. Alcance

Estas políticas aplican a todos los servicios de tecnología de información en la institución, así como a los activos de TI que la institución utiliza o requiere utilizar para entregar dichos servicios. Deben ser acatadas por los colaboradores directos de la institución, así como por los proveedores que entreguen servicios de tecnología de información para la institución (Tercerización).

7. Responsables

Es responsabilidad del Jefe de Informática y de los colaboradores del Departamento de Informática velar por la comunicación, el cumplimiento y la mejora de estas políticas.

Es responsabilidad del Comité de TI apoyar al Departamento de Informática en la aplicación de las políticas.

Es responsabilidad del Comité de TI establecer los mecanismos requeridos para comunicar efectivamente dichas políticas, así como establecer controles que logren prevenir o resolver el desacato de estas políticas por parte de los involucrados.

Es responsabilidad de todos los colaboradores de la institución conocer y acatar las políticas de Seguridad de la Información, así mismo deben conocer las sanciones en caso de su desobediencia.

8. Definiciones

Acuerdo de nivel de operación (OLA): Un acuerdo interno que cubre la prestación de servicios que da soporte a la organización de TI en su prestación de servicios.

Acuerdo de nivel de servicio (SLA): Acuerdo por escrito entre un proveedor de servicios y los usuarios del cliente, el cual documenta los niveles de servicio acordados para un servicio prestado.

Cambio: Adición, modificación o eliminación de un elemento (sea éste una aplicación, parámetro, plataforma, procedimiento, proceso o servicio).

Cambio en el Servicio: Adición, modificación o eliminación de un servicio (o de un componente de un servicio) autorizado, planificado o soportado y su correspondiente documentación.

Capacidad: Contar con los atributos o recursos necesarios para realizar o lograr metas establecidas o SLAs establecidos.

Catálogo de Servicios: Parte del Portafolio de Servicios, el cual consiste de los servicios que actualmente están en operación y están a disposición de los clientes.

Centro de Servicio: Punto central de contacto al que acuden todos los usuarios.

Cliente: Una persona o una entidad externa o interna que recibe los servicios empresariales de TI. También conocido como Usuario.

CMDB: Repositorio centralizado que contiene toda la información referente a los elementos de configuración a través de su ciclo de vida. La información que contiene usualmente corresponde a los atributos del elemento de configuración y sus relaciones con otros elementos.

Disponibilidad: Habilidad de un elemento de configuración o de un Servicio de desempeñar apropiadamente su función cuando ésta es requerida. La disponibilidad está determinada por la confiabilidad, el estado del mantenimiento, la entrega, el desempeño y la seguridad.

Desempeño: La implantación real o el logro de un proceso

Elementos de configuración: componentes de los servicios TI, así como los servicios que éstos nos ofrecen, por ejemplo:

- Dispositivos de hardware como PCs, impresoras, routers, monitores
- Software: sistemas operativos, aplicaciones
- Documentación: manuales, acuerdos de niveles de servicio

Evento: Cualquier suceso detectado o identificado que tiene importancia para la administración de la plataforma o la entrega de servicios de TI porque permite evaluar el impacto que una desviación ocasione o pueda ocasionar sobre los servicios (alineado a ITIL).

Incidente: Cualquier evento que no sea parte de la operación estándar de un servicio que ocasione, o pueda ocasionar, una interrupción o una reducción de la calidad de ese servicio (alineado a ITIL).

ITIL: Librería de Infraestructura de TI de la Oficina de Gobierno Gubernamental del Reino Unido (OGC).Un conjunto de lineamientos sobre la administración y procuración de servicios operativos de TI.

Nivel de Servicio: Acuerdo de las cualidades o requisitos que se cumplirán entre todas las partes que intervienen en la prestación de un servicio.

OLA: Ver Acuerdo de nivel de operación.

Portafolio de Servicios: Conjunto de compromisos e inversiones que asume el proveedor del servicio para con sus clientes.

Problema: Causa subyacente desconocida de uno o más incidentes.

Proveedor de TI: Persona física o jurídica que provee o presta un servicio relacionado con la tecnología de información, sea independiente o que pertenezca al mismo grupo o conglomerado financiero, incluyendo las casas matrices.

Servicio: Medio de entregar valor a los clientes facilitándoles los resultados que quieren recibir sin que asuman los costos y riesgos específicos de generarlos.

SLA: Ver Acuerdo de nivel de servicio.

Tecnología de información (TI): Conjunto de técnicas que permiten la captura, almacenamiento, transformación, transmisión y presentación de la información generada o recibida a partir de procesos, de manera que pueda ser organizada y utilizada en forma consistente y comprensible por los usuarios que estén relacionados con ella. Incluye elementos de hardware, software, telecomunicaciones y conectividad.

Usuario: Ver Cliente.

9. Políticas

14. Sobre los servicios de tecnología de información de la institución

Un servicio es un medio de entregar valor a los clientes facilitándoles los resultados que quieren recibir sin que asuman los costos y riesgos específicos de generarlos. Los servicios de tecnología de información se identifican pues quienes los entregan son del departamento de informática o proveedores de TI. Los servicios de tecnología oficiales de la institución se encuentran definidos en el portafolio de servicios.

15. Sobre el apoyo a los servicios de tecnología de información

La institución debe apoyar y velar por la obtención de los recursos humanos, materiales y económicos requeridos para procurar una entrega exitosa de los servicios de tecnología de información del portafolio de servicios. Adicionalmente el Comité de TI debe apoyar y velar por la obtención de los recursos humanos, materiales y económicos requeridos para procurar una entrega exitosa de los servicios de TI.

16. Sobre el marco de trabajo asociado a la entrega de los servicios de tecnología de información

TI debe establecer un marco de trabajo o un esquema para entregar los Servicios de tecnología de información, el cual esté alineado a las necesidades y capacidades de la institución.

Dicho marco debe considerar:

a. Marco de trabajo de administración de niveles de servicio entre el cliente y el proveedor de servicio: que debe asegurar que los servicios estén alineados a los requerimientos y prioridades del negocio, que se facilita la comprensión entre el cliente y el proveedor de

servicio mediante la definición de los servicios dentro del catálogo, que se acuerdan los niveles de servicio y operación, que establece los roles en la entrega de los servicios, así como las responsabilidades de los proveedores y los usuarios.

b. El sistema de Escritorio de Servicios: que se utiliza para el registro, monitoreo y reporte de las llamadas, incidentes, solicitudes de servicio y necesidades de información
c. El Repositorio centralizado conteniendo toda la información referente a los elementos de configuración a través de su ciclo de vida.
d. El esquema para escalar la atención de los servicios de tecnología de información, así como de los incidentes y problemas.
e. El esquema para reportar el desempeño de los servicios: el cual se utiliza para comprobar que los servicios de tecnología de información se ejecutan contra acuerdos de niveles de servicio equitativos y exigibles.

17. Sobre la vigencia del portafolio de servicios de TI

Es responsabilidad de cada encargado o administrador de servicio asignado, velar por mantener vigente y actualizada la información del portafolio de los servicios que le corresponden, así como los pasos o documentos que el usuario final debe completar para solicitar el servicio.

18. Sobre los acatamientos generales de gestión de servicios de tecnología de información que deben seguir los colaboradores de TI

Las principales funciones y responsabilidades de los colaboradores de informática se encuentran delimitadas en sus perfiles de puestos, pero es importante destacar las siguientes:

a. El Departamento de Informática es el responsable de mantenerse atento a las necesidades y prioridades del negocio, así como los cambios en las mismas, y reflejarlo en la mejora del catálogo de servicios
b. El Departamento de Informática es el responsable de negociar y acordar los niveles de servicio a entregar a los usuarios y documentar formalmente dichos acuerdos
c. El Departamento de Informática es el responsable de seguir el esquema de escalaciones para la atención de los servicios de tecnología de información
d. Es responsabilidad de cada encargado o administrador de servicio asignado de asegurarse de que el monitoreo y reporte de desempeño de los servicios se generen, se investiguen las desviaciones en el logro de los acuerdos de servicio, se tomen las acciones pertinentes para prevenir su recurrencia, se conozca por parte de los usuarios el desempeño de los servicios y se logre la satisfacción de los usuarios
e. El Departamento de Informática es el responsable de seguir el esquema de clasificación de problemas establecido para los servicios de tecnología de información.
f. El Departamento de Informática es el responsable de ejecutar el mantenimiento preventivo y correctivo sobre los activos de TI de la institución.
g. El Departamento de Informática es el responsable de seguir el esquema de autorización de cambios establecido para los servicios de tecnología de información.
h. El Departamento de Informática es responsable de disponer de prácticas o herramientas para la prevención de la inclusión de software no-autorizado.

i. El Departamento de Informática es el responsable de implementar un adecuado monitoreo para establecer un esquema preventivo de fallas, este monitoreo debe ayudar a la resolución de problemas.
j. Es responsabilidad de cada encargado o administrador de servicio asignado, mantener la documentación necesaria para establecer una base de datos de conocimiento, que permita al Departamento de Informática entregar de forma rápida y eficiente los servicios, así como solucionar los incidentes o problemas, aún y cuando el responsable no esté disponible.
k. El Departamento de Informática es el responsable del estado del licenciamiento y las acciones a tomar para cumplir la regulación existente.
l. El Departamento de Informática es el responsable de contar con un plan de capacidad en el cual se asegure que los recursos necesarios para la prestación de los servicios acordes a la demanda o utilización por parte de los usuarios, así como el desempeño de los activos de TI esté al nivel requerido para procurar una entrega exitosa de los servicios de TI.
m. Es responsabilidad de los colaboradores de Informática seguir y utilizar durante la ejecución de sus labores reglamentos, políticas, procedimientos, instructivos, formularios, estándares, etc. que han sido establecidas para el funcionamiento del departamento.
n. Es responsabilidad de los colaboradores de Informática hacer uso adecuado de los recursos y las herramientas que son proporcionadas por la institución, con el propósito de mejorar constantemente el desempeño de sus labores.

19. Sobre la responsabilidad de los usuarios finales en la gestión de servicios de tecnología de información

Los usuarios que utilizan los servicios de TI deben conocer el portafolio de servicios de TI y los acuerdos de niveles de servicio que cada uno posee.

El usuario tiene el deber de cumplir con los procesos establecidos para la prestación de los servicios, esto incluye la solicitud formal del servicio y el cumplimiento de los acuerdos de niveles de servicio que le corresponden a él, así como el reporte de si la solución satisface sus necesidades en el tiempo previsto.

El usuario tiene el derecho de exigir el cumplimiento de los niveles de servicio que le corresponden a TI.

20. Sobre la administración de la configuración

El inventario físico deberá actualizarse cada vez que se realice un cambio de ubicación de un equipo, que se cambien su características, que se realice una donación, que se clasifique un equipo como "obsoleto", que se deseche físicamente. Además, el Departamento de Informática debe actualizar el inventario físico. Se deben mantener gráficos o diseños que establezcan la relación de los elementos de configuración.

21. Sobre la administración de eventos e incidentes

Es responsabilidad de cada encargado o administrador de los servicios relacionados con la atención de incidentes, procurar un esquema preventivo basado en monitoreo y atención de eventos, así mismo es su responsabilidad evaluar el comportamiento de los incidentes para establecer la causa raíz de éstos y evaluar su erradicación.

22. Sobre la administración de problemas

Es responsabilidad de cada encargado o administrador de servicio asignado, procurar un esquema para la prevención de la ocurrencia de problemas, así mismo es su responsabilidad evaluar la resolución de los problemas para identificar si han surgido incidentes como resultado de la resolución, si logró su propósito y si el usuario impactado está satisfecho.

Se debe mantener una bitácora que contenga pistas de auditoría que faciliten la búsqueda de un patrón o de un problema.

Es responsabilidad de cada encargado o administrador de servicio asignado, mantener la documentación necesaria para establecer una base de datos de conocimiento con el registro de los errores conocidos y sus resoluciones conocidas.

23. Sobre la administración de cambios

Es responsabilidad de cada colaborador de Informática que aplique un cambio de planificar y coordinar su aplicación, probar el cambio previo a su aplicación, así mismo es su responsabilidad evaluar la aplicación del cambio para identificar si han surgido incidentes como resultado de la aplicación del cambio, si el cambio logró su propósito, si el Solicitante del cambio está satisfecho.

Es responsabilidad de cada colaborador de Informática que aplique un cambio el completar la documentación del cambio verificando que se actualizaron el sistema asociado o la CMDB, la documentación de usuario y los procedimientos o documentos que sufrieron algún impacto por el cambio.

24. Sobre la administración de capacidad y disponibilidad

Es responsabilidad de cada encargado o administrador de servicio asignado, evaluar el desempeño y la capacidad de entrega de los servicios asignados. En caso de mantener un bajo desempeño y/o baja capacidad de atención se deben establecer acciones para su mejora.

Es responsabilidad de cada encargado o administrador de servicio asignado, establecer los manuales, procedimientos, estándares, instructivos, entre otros que permitan entregar al usuario final el rendimiento requerido sobre los activos de TI, esto en especial para todos aquellos procesos críticos de la institución. En caso de mantener un bajo rendimiento de los activos de TI se deben establecer acciones para su mejora. Adicionalmente se debe evitar la desactualización de la

plataforma tecnológica que directamente afecte el rendimiento de los activos de TI y que degrade la entrega de los niveles de acuerdos de servicio pactado.

25. Sobre el desempeño de los servicios de tecnología de información

El desempeño de los servicios de TI es medido mensualmente mediante el cumplimiento de los niveles de acuerdo de servicio. Si dichos acuerdos no se están cumpliendo se deben establecer acciones para su mejora.

26. Sobre la dependencia de recursos humanos para entregar servicios de tecnología de información

Es responsabilidad de la Jefatura de Informática junto con cada encargado o administrador de servicio asignado, proveer un esquema de trabajo o documentación en donde no se establezca una dependencia de un único recurso, en especial hacia funcionarios con conocimiento específico. En caso de mantener dicha dependencia se deben establecer acciones para su mejora.

27. Sobre la contratación de Terceros para entrega de servicios de tecnología de información

La contratación de servicios de TI en su mayoría es adquirida bajo tres modalidades:

a. Contratación de servicios o compra de productos: para la cual se debe delimitar un alcance a través de entregables y atributos en las especificaciones, si fuese necesario se establecen los acuerdos de niveles de servicio.
b. Contratación de horas o profesionales (outtasking), para la cual se contratan horas de profesionales los cuales son administrados por el personal de TI, estos profesionales ejecutan las labores bajo la normativa de TI. El desempeño o la calidad de los productos entregados son responsabilidad de la institución y no del proveedor.
c. Tercerización de servicios (outsourcing), para la cual se desplaza por completo la ejecución del servicio a un Tercero y se establecen los acuerdos de niveles de servicio que el proveedor debe cumplir, dichos acuerdos deben considerar el cumplimiento de la normativa vigente para la institución, y si ésta llega a cambiar se deben de revalorar los contratos establecidos con los proveedores. El desempeño o la calidad de los productos entregados son responsabilidad del proveedor y no de la institución.

Para cualquiera de los tres casos la institución debe velar por el cumplimiento de la relación contractual, y en dicha relación deben quedar especificadas cláusulas relacionadas con riesgos o continuidad.

Todas aquellas terceras partes involucradas en la prestación de servicios deben acatar la reglamentación, políticas, procedimientos de la institución. En especial aquellas relacionadas con la continuidad de la prestación de servicios y con seguridad de TI.

28. Sobre la adquisición y el mantenimiento de la infraestructura tecnológica

Es responsabilidad de la institución la inversión en adquirir y dar mantenimiento apropiado en la infraestructura tecnológica requerida para brindar los servicios de TI acordados con el negocio.

a. El Departamento de Informática es el responsable de debe evaluar individualmente en cada incorporación de nuevas capacidades tecnológicas los costos de complejidad que implica dicha inclusión, por ejemplo necesidades de contratos de soporte anual, capacitación, consultorías para configuración adicional, recursos adicionales de desarrollo o soporte, herramientas para monitoreo de la capacidad, software o hardware de seguridad para la nueva capacidad, entre otras.
b. El Departamento de Informática es el responsable de debe evaluar individualmente en cada incorporación de nuevas capacidades tecnológicas la viabilidad comercial del proveedor, por ejemplo las referencias, la experiencia, entre otras.
c. El Departamento de Informática es el responsable de debe evaluar individualmente en cada incorporación de nuevas capacidades tecnológicas el producto que se va a adquirir, por ejemplo otras empresas que están utilizando el producto, ejecución de laboratorios de prueba o de pruebas piloto, entre otras.

29. Sobre el uso de ambientes de desarrollo y pruebas

a. El Departamento de Informática es el responsable de establecer un ambiente de desarrollo y pruebas separado del de producción.
b. Los ambientes de desarrollo y pruebas de factibilidad e integración de las aplicaciones e infraestructura que TI establecerá deberán ser similares al de producción. En caso de no poder replicar completamente al de producción, al menos considerarán similar
    - Funcionalidad
    - Configuración de hardware
    - Configuración de software
    - Seguridad
c. Es responsabilidad de los colaboradores de Informática involucrados en la preparación y el uso de los ambientes de desarrollo y pruebas que los datos de prueba que utilicen sean si no son confidenciales o datos reducibles a clientes o que comprometan los negocios de la institución o terceros, de lo contrario, deben utilizar datos enmascarados para evitar posibles fugas de información.
d. Es responsabilidad de los colaboradores de Informática involucrados en la preparación y el uso de los ambientes de desarrollo y pruebas que la eliminación de datos de prueba la realicen de forma segura.
e. Es responsabilidad de los colaboradores de Informática involucrados en la preparación y el uso de los ambientes de desarrollo y pruebas asegurarse de que los accesos a los ambientes de desarrollo y pruebas sean únicamente para el administrador del ambiente, los colaboradores de Informática miembros del equipo de desarrollo, los usuarios expertos y los usuarios requeridos para las pruebas.
f. Es responsabilidad de los colaboradores de Informática involucrados en la preparación y el uso de los ambientes de desarrollo y pruebas asegurarse que los accesos a los ambientes de desarrollo y pruebas tengan las mismas restricciones del ambiente de producción.

g. Es responsabilidad de los colaboradores de Informática involucrados en la preparación y el uso de los ambientes de desarrollo y pruebas que consideren cómo ejecutar la migración entre ambientes y el control de versiones.

30. Sobre la ejecución de pruebas

h. Es responsabilidad de la Jefatura de Informática junto con cada encargado o administrador de servicio asignado utilizar pruebas para verificar la factibilidad e integración de las aplicaciones e infraestructura.

i. Es responsabilidad de cada encargado o administrador de servicio asignado realizar pruebas de funcionalidad entre la aplicación o la infraestructura y la plataforma existente con el fin de validar los procesos, reglas de negocio establecidas y los requerimientos funcionales.

j. Es responsabilidad de cada encargado o administrador de servicio asignado realizar pruebas de integración entre la aplicación o la infraestructura y la plataforma existente con el fin de garantizar que su operación integrada es correcta.

k. Es responsabilidad de cada encargado o administrador de servicio asignado realizar pruebas de desempeño entre la aplicación o la infraestructura y la plataforma existente con el fin de asegurar que se cumplen con los parámetros de rendimiento que se espera de ellas.

l. Cada encargado o administrador de servicio asignado podrá considerar criterios como
    - impacto de la aplicación o la infraestructura sobre: los procesos críticos de negocio, los usuarios críticos o una cantidad masiva de usuarios
    - si la aplicación o la infraestructura es una nueva capacidad tecnológica
    - si el desarrollo de software requiere un esfuerzo mayor a dos semanas para determinar en cuáles casos ejecutar las pruebas.

Políticas para la adquisición de TI

10. Objetivo

El proceso y los requisitos de las adquisiciones que lleva a cabo del Departamento de Informática están definidas en la Ley de Contratación Administrativa, sin embargo existen una serie de elementos que deben ser considerados dentro de los aspectos técnicos durante la definición del objeto de la contratación y la definición del alcance de los elementos técnicos. Por lo tanto estas políticas tiene el objetivo de establecer una serie de consideraciones que debe mantener Informática al momento de entregar los términos de referencia técnicos al proceso de adquisiciones que ejecuta la Proveeduría.

11. Alcance

Este instructivo aplica para todos los términos técnicos de contratación que el departamento de Informática debe construir y enviar a la Proveeduría institucional para ejecutar una adquisición.

12. Responsables

La aplicación de este instructivo es responsabilidad del Jefe de Informática.

13. Definiciones

Accesibilidad: Que tan abierto es el proveedor para comunicarme y obtener sus servicios o producto, desde el punto de vista de localización, negociación con el cliente, establecimiento de relaciones de largo plazo, etc.

Agilidad en los trámites: Que tan ágil es el proveedor para atender solicitudes de los clientes de la organización.

Asesoría técnica y servicio postventa: Determina si el proveedor atiende sus compromisos post venta, tales como asesorar técnicamente al cliente o bien atención de garantías.

Capacidad: Contar con los atributos necesarios para realizar o lograr.

Costos de complejidad: corresponden a costos de transición y/o migración, costos por administración de riesgos técnicos, la flexibilidad de incorporar adicionales o agregados en el futuro, los costos de integración con el resto de la plataforma existente y la vida útil de la inversión en cuanto a necesidad de actualizaciones en la tecnología.

Cotización: Oferta que el proveedor presenta a solicitud de la organización contratante.

Desempeño: La implantación real o el logro de un proceso.

Información y comunicación: Mide en qué grado el proveedor se preocupa por mantener informados a los clientes de la organización sobre nuevas opciones, mejoras, o capacidades que le pueden ayudar a mejorar su negocio.

Oferta: Cotización que el proveedor presenta a solicitud de la organización contratante.

Plan estratégico de TI: Un plan a largo plazo, Ej., con un horizonte de tres a cinco años, en el cual la gerencia del negocio y de TI describen de forma cooperativa cómo los recursos de TI contribuirán a los objetivos estratégicos empresariales (metas)

Plan Táctico de TI (Plan Operativo de TI): Un plan a mediano plazo, Ej., con un horizonte de seis a dieciocho meses, que traduzca la dirección del plan estratégico de TI en las iniciativas requeridas, requisitos de recursos y formas en las que los recursos y los beneficios serán supervisados y administrados

Portafolio de Servicios: Una agrupación de servicios, administrados y vigilados para optimizar el retorno sobre la inversión.

Portafolio de Proyectos: Una agrupación de programas y proyectos, administrados y vigilados para optimizar el retorno sobre la inversión.

Programa: Una agrupación estructurada de proyectos independientes que incluye el alcance completo del negocio, del proceso, de las personas, de la tecnología y las actividades organizacionales que se requieren (tanto necesarias como suficientes) para lograr un resultado de negocios claramente especificado.

Proyecto: Un conjunto estructurado de actividades relacionadas con la entrega de una capacidad definida a la organización (la cual es necesaria, aunque no suficiente para lograr un resultado de negocio requerido) con base en un cronograma y presupuesto acordado.

Relación precio/calidad: Mediante este requisito la institución determina si el proveedor suple productos/servicios de calidad y su precio es aceptable conforme a los precios de mercado para el mismo producto/servicio. La evaluación de este ítem puede ser determinada comparativamente con las ofertas de los otros proveedores o bien por la experiencia de quien recibe las cotizaciones.

Responsabilidad en el cumplimiento de contrato: Se entiende por cumplimiento de contrato como la capacidad del proveedor para cumplirle a la institución con lo pactado en la oferta o bien en los casos en que expresamente medie un contrato para adquisición de recursos de TI, la capacidad para cumplir con las cláusulas establecidas en el mismo.

Responsabilidad y ética en los negocios: Es el grado de responsabilidad y ética del proveedor al hacer negocios con sus clientes. Busca evitar establecer relaciones con proveedores que pueden ser problemáticos, que evaden regulación o bien que ofrecen productos y servicios de dudosa procedencia.

Tratamiento de quejas y no conformidades: Efectividad del proveedor para resolver las quejas y no conformidades que le han planteado sus clientes cuando de él depende directamente su atención, o bien la efectividad para establecer un canal de contacto con un Tercero que pueda ayudar al cliente a resolver sus no conformidades.

14. Políticas para la adquisición de TI

1. El departamento de Informática es responsable de planificar las adquisiciones que son necesarias para su mantener la operación de los servicios tecnológicos, considerando que la institución tiene el contenido presupuestario. Las adquisiciones debe estar alineadas con uno o algunos de los siguientes elementos:
    a. Plan Estratégico de TI o su dirección tecnológica establecida en él
    b. Plan Anual Operativo de TI
    c. Actualización de la infraestructura tecnológica
    d. Implementación de la arquitectura de la información
2. Las adquisiciones tecnológicas deben utilizar los "Estándares tecnológicos" para delimitar los requerimientos técnicos y así mantener una infraestructura tecnológica vigente.
3. El departamento de Informática debe considerar la obsolescencia de la infraestructura tecnológica y mantener un adecuado remplazo, de forma tal que no existan deficiencias en la operación y entrega de los servicios de Informática.
4. El departamento de Informática debe considerar los mantenimientos preventivos y correctivos que podrían ser requeridos para mantener la entrega de los servicios de Informática según los acuerdos pactados con el cliente interno.
5. Para desarrollar las especificaciones se deben considerar al menos:
    a. La descripción del alcance del trabajo o los servicios/entregables solicitados con las especificaciones técnicas considerando los "Estándares tecnológicos", y la "Arquitectura de la información", esta descripción debe estar delimitada en términos de productos entregables
    b. Para cada producto entregable se debe establecer los elementos o criterios de aceptación que serán revisados, evaluados o medidos para la aceptación del entregable, es decir, lo que debe cumplir una vez que el producto haya sido finalizado
    c. Los supuestos o suposiciones que el Proveedor potencial debe considerar para el desarrollo o la entrega del trabajo/servicios/entregables. Estos supuestos deben ser finitos y claros en términos metodológicos para evitar no delimitar adecuadamente el alcance y por ende el costo del producto o servicio
    d. El plazo o el cronograma esperado para el trabajo/servicios/entregables o la expectativa del mismo (por ejemplo plazo mínimo, plazo máximo, plazo promedio, etc.); si hay Acuerdos de Niveles de Servicios que debe cumplir se incluyen
    e. Las características que deben tener los ambientes de desarrollo y prueba para soportar efectiva y eficientemente las pruebas de factibilidad e integración de las aplicaciones e infraestructura considerando
        i. la funcionalidad

ii. la configuración de hardware
iii. la configuración de software
iv. las pruebas de integración
v. las pruebas de desempeño
vi. la migración entre ambientes
vii. el control de versiones
viii. los datos
ix. las herramientas de prueba
x. la seguridad

f. El mantenimiento que debe incluirse dentro de la adquisición (en caso de aplicar para el producto/servicio)
g. Las características que debe poseer el Proveedor potencial que sustente su experiencia y referencias de clientes actuales/anteriores, su viabilidad y futuro en el mercado, el nivel de dependencia del mismo
h. La garantía que se espera tener del producto/servicio
i. Las condiciones de pago (si aplican)
j. Verificar si hay otra consideración que aplica la contratación administrativa para el bien o servicio que se está adquiriendo.

6. Establecer los criterios de decisión sobre la adquisición para encontrar la mejor oferta. Para establecer los criterios de decisión sobre la adquisición se deben considerar al menos:
    a. Apego a los requerimientos o especificaciones, considerando la factibilidad e integración de las aplicaciones e infraestructura
    b. Calidad
    c. Precio
    d. Tiempo de entrega
    e. Viabilidad de la continuidad del Proveedor potencial o existencia de Proveedores alternativos; considerando los riesgos del Proveedor sobre la institución
    f. Condiciones de pago
    g. Garantía
    h. Accesibilidad
7. Establecer las condiciones que debe cumplir el proveedor y que son relevantes para el mantenimiento del producto o servicio a adquirir, considerar:
    a. Las especificaciones del producto o servicio son claras, finitas y concisas para los proveedores, y mantienen concordancia con lo que se adquiere en el mercado
    b. La flexibilidad para mejoras de capacidad que posee el producto/servicio que está adquiriendo
    c. La vida útil que posee el producto/servicio que está adquiriendo
    d. Los criterios de decisión que se considerarán para elegir la mejor oferta
    e. La información mínima que debe presentar el Proveedor potencial para analizar su desempeño
    f. Garantías

g. Mantenimiento
h. Escalabilidad
i. Elementos para garantizar la factibilidad e integración de las aplicaciones e infraestructura con el producto/servicio cotizado O propuesta de pruebas a realizar para comprobar la factibilidad e integración de las aplicaciones e infraestructura

8. En caso de la adquisición de software considerar si se tendrán los programas fuentes o no y la capacidad que tendrá el departamento de Informática de variar la funcionalidad del producto. En caso de mantener los programas fuentes se debe considerar el esquema de desarrollo de software, y de requerirse desarrollo del proveedor se debe evaluar el nivel de dependencia hacia éste y la afectación de los costos de operación de TI. En caso de requerir nuevos conocimientos por parte del departamento de Informática se debe asegurar la transferencia de éste. Si se adquiere desarrollo a la medida se debe comprender los derechos de autor y licenciamiento, los procesos de diseño y arquitectura de las aplicaciones y la entrega de elementos de diseños como diccionarios de datos, esquemas de diseños, documentación dentro del código, manual de usuarios, etc. de forma tal que permita la continuidad y el mantenimiento de los productos adquiridos.

9. En caso de necesitar el levantamiento de requerimientos de software para hacer una adquisición, el departamento de Informática debe trabajar de forma conjunta con el departamento de Planificación para mantener la integridad del modelo de arquitectura, considerando los procesos de negocio, y las relaciones que éstos presentan.

10. En caso de necesitar el levantamiento de requisitos mínimos para el desarrollo de software para hacer una adquisición, el departamento de Informática debe trabajar de forma conjunta con el departamento de Planificación para mantener la integridad del modelo de arquitectura, considerando los procesos de negocio, y las relaciones que éstos presentan. Además debe considerar que el proveedor seleccionado finalizará el levantamiento de requerimientos y por ende los alcances del desarrollo podrían cambiar.

11. El departamento de Informática conjuntamente con el departamento de Planificación, podrán mostrar los requisitos o requerimientos resultantes de las adquisiciones, a cualquier instancia de gobierno de TI que considere pertinente involucrar, sin embargo esta no es una actividad obligatoria.

Administración de Servicios de TI

15. Objetivo

Establecer el marco de trabajo de la prestación de servicios para definir y administrar los niveles de servicio con base en los requerimientos de los usuarios de la Defensoría y las capacidades de Informática, con lo cual se obtiene la información necesaria para el seguimiento del desempeño de Informática en función de los servicios que brinda.

16. Alcance

Este procedimiento aplica para todos los servicios de tecnología de información en la institución.

17. Responsables

La CITI (Comisión Institucional de Tecnologías de Información) es la comisión responsable de avalar y comprender el marco de trabajo de los servicios de Informática, el Jefe de Informática y los Administradores de los servicios son los responsables de asegurar que se cumplan los acuerdos establecidos en este procedimiento.

18. Documentos relacionados

Nombre del documento

Catálogo de Servicios de TI

Plan de Continuidad de los Servicios de TI

19. Definiciones

Acuerdo de nivel de operación (OLA): es el acuerdo que se pacta en la prestación de los servicios que dan soporte a la institución de TI.

Acuerdo de nivel de servicio (SLA): Contrato escrito entre un proveedor de servicios y la Defensoría de los Habitantes, el cual documenta los niveles de servicio acordados para un servicio prestado.

Cambio en el Servicio: Adición, modificación o eliminación de un servicio (o de un componente de un servicio) autorizado, planificado o soportado y su correspondiente documentación.

Catálogo de Servicios: Parte del Portafolio de Servicios, el cual consiste de los servicios que actualmente están en operación y están a disposición de los clientes.

Centro de Servicio: Punto central de contacto al que acuden todos los usuarios.

Nivel de Servicio: Acuerdo de las cualidades o requisitos que se cumplirán entre todas las partes que intervienen en la prestación de un servicio.

OLA: Ver Acuerdo de nivel de operación.

Portafolio de Servicios: Conjunto de compromisos e inversiones que asume el proveedor del servicio para con sus clientes.

Proveedor de TI: Persona física o jurídica que provee o presta un servicio relacionado con la tecnología de información, sea independiente o que pertenezca al mismo grupo o conglomerado financiero, incluyendo las casas matrices.

Servicio: Medio de entregar valor a los clientes facilitándoles los resultados que quieren recibir sin que asuman los costos y riesgos específicos de generarlos.

SLA: Ver Acuerdo de nivel de servicio.

Tecnología de información (TI): Conjunto de técnicas que permiten la captura, almacenamiento, transformación, transmisión y presentación de la información generada o recibida a partir de procesos, de manera que pueda ser organizada y utilizada en forma consistente y comprensible por los usuarios que estén relacionados con ella. Incluye elementos de hardware, software, telecomunicaciones y conectividad.

Usuario interno: se refiere al usuario, funcionario de la Defensoría de los Habitantes, que hace uso de los servicios que provee por medio de software o hardware, el Departamento de Informática de la institución.

20. Procedimiento

Diseño de los servicios

Este marco de trabajo de administración de niveles de servicio contiene la estructura organizativa y los pasos a seguir para desarrollar una correcta administración de los niveles de servicios que brinda el Departamento de Informática a la institución, a los usuarios, a los terceros que colaboran con la institución y a los entes supervisores de la institución.

Estructura para administrar niveles de servicios

La estructura organizacional para la administración de los niveles de servicios es la siguiente:

- Coordinador de Niveles de Servicio (corresponde al Jefe de Informática)
- Administrador del servicio (se indica para cada servicio en el catálogo de servicios)
- Administrador del sistema de Escritorio de Servicios (corresponde al Jefe de Informática)
- Usuarios

El Coordinador de Niveles de Servicio tiene las siguientes tareas y responsabilidades:

- Mantenerse atento de las necesidades de la Defensoría de los Habitantes en materia de Tecnologías de Información, así como los cambios en las mismas
- Asegurarse de que las necesidades de servicio sean identificadas y documentadas a través de SLAs y OLAs
- Negociar y acordar los niveles de servicio a entregar a los usuarios y documentar formalmente dichos acuerdos
- Apoyar en el mantenimiento del catálogo de servicios
- Asegurarse de que las metas establecidas hacia los proveedores externos de servicios están alineadas con los SLAs y OLAs
- Asegurarse de que el monitoreo y reporte de resultados de los servicios se generen, se investiguen las desviaciones en el logro de los SLAs y OLAs, y se tomen las acciones pertinentes para prevenir su recurrencia
- Asegurarse de que la revisión del desempeño de los servicios sea conocida por los usuarios y las acciones acordadas a raíz de dicha revisión se ejecuten
- Asegurarse de que se ejecute una mejora continua de los servicios
- Actualizar los SLAs y OLAs regularmente
- Analizar las tendencias de la demanda de los servicios
- Asegurarse de lograr la satisfacción de los usuarios de acuerdo a los SLAs y OLAs acordados

El Administrador del servicio tiene las siguientes tareas y responsabilidades:

- Administrar las tareas de los ejecutores de los servicios
- Tomar decisiones en caso de duda o controversias de los ejecutores de los servicios
- Reportar al Coordinador de Niveles de Servicio cualquier inconveniente que impacte significativamente al negocio
- Participar activamente en la autorización de cambios
- Atender incidentes y el manejo de las solicitudes de servicio en el Escritorio de Servicios, así como el monitoreo de ciertos eventos para ser incluidos en el Escritorio de Servicios

El Administrador del sistema de Escritorio de Servicios tiene las siguientes tareas y responsabilidades:

- Instalar y dar mantenimiento al sistema
- Configurar el sistema con información como mínimo del catálogo de servicios, la asignación y escalación de servicios, los usuarios, los reportes, las interfaces con otros sistemas
- Velar por la continuidad y buen uso del sistema

El usuario tiene las siguientes tareas y responsabilidades:

- Solicitar los servicios según los medios y procesos establecidos
- Reportar si la solución satisface sus necesidades en el tiempo previsto
- Cumplir con los requisitos establecidos para obtener el servicio de acuerdo con los SLAs y OLAs

Creación o modificación de los servicios

ID	Entrada	Actividad	Responsable	Salida
1	Requerimientos de negocio para los servicios de TI que sean expresados	Analizar y documentar los requerimientos de negocio para los servicios de TI. En el caso de servicios existentes la documentación se necesita para aplicar cambios a dichos servicios. En el caso de nuevos servicios se necesita para diseñar el servicio. Frecuencia: cada vez que se vaya a aplicar un cambio a un servicio o se vaya a diseñar un nuevo servicio	Coordinador de Niveles de Servicio con Responsable de proceso de negocio que requiere el servicio	Requerimientos de negocio para los servicios de TI documentados
2	Requerimientos de negocio para los servicios de TI documentados	Definir el servicio, considerando: 1. El(los) proceso(s) de negocio que van a ser soportados por el servicio 2. Entregables que va a brindar el servicio 3. La dependencia del negocio hacia el servicio 4. La prioridad que le da negocio al servicio 5. El impacto al negocio que tiene el servicio 6. Clasificación del servicio 7. Tipo de Servicio 8. Si el servicio es diferenciado indicar las condiciones o usuarios que acceden a esa diferenciación y explicar en qué consiste Frecuencia: cada vez que se vaya a aplicar un cambio a un servicio o se vaya a diseñar un nuevo servicio	Coordinador de Niveles de Servicio con Responsable de proceso de negocio que requiere el servicio	Catálogo de Servicios actualizados con los Acuerdo de Nivel de Servicio (SLA)
3	Catálogo de Servicios actualizados con los Acuerdo de Nivel de Servicio (SLA)	Informar a la institución del nuevo catálogo de servicios	Coordinador de Niveles de Servicio con Responsable de proceso de negocio que requiere el servicio	Catálogo de Servicios divulgado

Mejora continua de los servicios

El Coordinador de Niveles de Servicio monitorea el cumplimiento de los acuerdos de niveles de servicio establecidos para los servicios que entrega el Departamento de Informática. Asimismo, debe establecer la causa raíz y si amerita un plan de acción para corregir los resultados obtenidos.

El Coordinador de Niveles de Servicio actualiza los acuerdos de niveles de servicio a la luz de los cambios en los servicios y cambios en los procesos de la institución que afecten los servicios.

El Coordinador de Niveles de Servicio analiza las tendencias de la demanda de los servicios según los registros que se generen en el Escritorio de Servicios.

Estándar de adquisición de soluciones en Tecnologías de Información

21. Objetivo

El proceso y los requisitos de las adquisiciones que lleva a cabo del Departamento de Informática están definidas en la Ley de Contratación Administrativa y su reglamento, sin embargo existen una serie de elementos que deben ser considerados dentro de los aspectos técnicos durante la definición del objeto de la contratación y la definición del alcance de los elementos técnicos. Por lo tanto este estándar sirve como guía para evaluar las cláusulas de las contrataciones para recursos de TI con los requisitos mínimos necesarios.

22. Alcance

Este instructivo aplica para todos los términos técnicos de contratación que el Departamento de Informática debe construir y enviar a la Proveeduría institucional para ejecutar una adquisición.

23. Responsables

La aplicación de este instructivo es responsabilidad del Jefe del Departamento de Informática .

24. Definiciones

Accesibilidad: Que tan abierto es el proveedor para comunicar y obtener sus servicios o producto, desde el punto de vista de localización, negociación con el cliente, establecimiento de relaciones de largo plazo, etc.

Agilidad en los trámites: Que tan ágil es el proveedor para atender solicitudes de la Defensoría.

Asesoría técnica y servicio postventa: Determina si el proveedor atiende sus compromisos post venta, tales como asesorar técnicamente al cliente o bien atención de garantías.

Capacidad: Contar con los atributos necesarios para realizar o lograr.

Costos de complejidad: corresponden a costos de transición y/o migración, costos por administración de riesgos técnicos, la flexibilidad de incorporar adicionales o agregados en el futuro, los costos de integración con el resto de la plataforma existente y la vida útil de la inversión en cuanto a necesidad de actualizaciones en la tecnología.

Cotización: Oferta que el proveedor presenta a solicitud de la organización contratante.

Desempeño: La implantación real o el logro de un proceso.

Información y comunicación: Mide en qué grado el proveedor se preocupa por mantener informados a los clientes de la organización sobre nuevas opciones, mejoras, o capacidades que le pueden ayudar a mejorar su negocio.

Oferta: Cotización que el proveedor presenta a solicitud de la organización contratante.

Plan estratégico de TI: Un plan a largo plazo, Ej., con un horizonte de tres a cinco años, en el cual la gerencia del negocio y de TI describen de forma cooperativa cómo los recursos de TI contribuirán a los objetivos estratégicos empresariales (metas)

Plan Táctico de TI (Plan Operativo de TI): Un plan a mediano plazo, Ej., con un horizonte de seis a dieciocho meses, que traduzca la dirección del plan estratégico de TI en las iniciativas requeridas, requisitos de recursos y formas en las que los recursos y los beneficios serán supervisados y administrados

Portafolio de Servicios: Una agrupación de servicios, administrados y vigilados para optimizar el retorno sobre la inversión.

Portafolio de Proyectos: Una agrupación de programas y proyectos, administrados y vigilados para optimizar el retorno sobre la inversión.

Programa: Una agrupación estructurada de proyectos independientes que incluye el alcance completo del negocio, del proceso, de las personas, de la tecnología y las actividades organizacionales que se requieren (tanto necesarias como suficientes) para lograr un resultado de negocios claramente especificado.

Proyecto: Un conjunto estructurado de actividades relacionadas con la entrega de una capacidad definida a la organización (la cual es necesaria, aunque no suficiente para lograr un resultado de negocio requerido) con base en un cronograma y presupuesto acordado.

Responsabilidad en el cumplimiento de contrato: Se entiende por cumplimiento de contrato como la capacidad del proveedor para cumplirle a la organización con lo pactado en la oferta y en el contrato para adquisición de recursos de Tecnologías de Información, la capacidad para cumplir con las cláusulas establecidas en el mismo.

Responsabilidad y ética en los negocios: Es el grado de responsabilidad y ética del proveedor al hacer negocios con sus clientes. Busca evitar establecer relaciones con proveedores que puedan comprometer la objetividad, que evaden regulación o bien que ofrecen productos y servicios de dudosa procedencia.

Tratamiento de quejas y no conformidades: Efectividad del proveedor para resolver las quejas y no conformidades que le plantea la institución cuando de él depende directamente su atención, o bien la efectividad para establecer un canal de contacto con un Tercero que pueda ayudar al cliente a resolver sus no conformidades.

Adquisición de Tecnología

Durante la adquisición de bienes relacionados con tecnologías de la información (hardware y software), la persona responsable del Departamento de Informática que valida si se debe o no ejecutar la compra, debe evaluar adicionalmente los elementos relacionados con el mantenimiento y la seguridad de los sistemas de información, por lo tanto se deberán considerar los siguientes criterios:

1. Verificar que el usuario final confirma haber ejecutado una adecuada validación de los requerimientos de negocio, y que comprende si hay alguna brecha entre las reglas de negocio y la funcionalidad del bien requerido. Adicionalmente confirma que ha considerado el plan de acción en caso de existir una brecha que requiera ser administrada.
2. Evaluar que los mecanismos de control de acceso y autorización estén acordes a las políticas y procedimientos de accesos que tiene la organización.
3. Cuando hay datos afectados de por medio:
    a. Verificar las técnicas de integridad de la información que se aplicarán.
    b. Verificar la necesidad de respaldar la información y establecer un responsable de la solicitud de dicho respaldo, el responsable delimitará las reglas básicas como frecuencia, hora del día, etc. y debe validar el cumplimiento de dichas reglas. El Departamento de Informática coordinará con el responsable el esquema de respaldo.
    c. Verificar la necesidad de establecer pistas de auditoría y evaluar con el usuario la factibilidad de esta acción.
4. En relación con el objeto de contratación:
    a. Verificar que no tiene asociada alguna vulnerabilidad que pueda ser catalogada como un riesgo relevante para TI
    b. Verificar que es capaz de cumplir los controles generales que regularmente establece la clasificación de datos
    c. Validar que mantiene reglas básicas para resguardar la integridad de las transacciones
    d. Validar que sea compatible con la arquitectura de información existente, eso incluye sistemas, datos, seguridad e infraestructura.
    e. Verificar si se requiere de integraciones con otros elementos de hardware y/o software ya existentes, y si son factibles dichas integraciones.
    f. Validar que se van a proveer manuales de documentación y de uso.

Consideraciones adicionales:

1. El Departamento de Informática de la Defensoría de los Habitantes será la única dependencia autorizada para realizar copias de seguridad del software relacionado con los objetos de contratación adquiridos.
2. Las instalaciones de software requeridas en las máquinas de la Defensoría de los

Habitantes, se realizará únicamente a través del Departamento de Informática.

3. El software proporcionado por el Departamento de Informática no puede ser copiado o suministrado a terceros en el caso de que el mismo corresponda a software propietario o sea parte de un licenciamiento institucional.

Política interna para el desarrollo y mantenimiento de Sistemas de Información.

Norma de desarrollo de software

25. Objetivo

Garantizar la integridad y disponibilidad de las aplicaciones que se desarrollan internamente para la institución, con el fin de reducir los riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción y así apoyar la operatividad del negocio.

26. Alcance

Este documento aplica para controlar todos los procesos de desarrollo de software que se dan en la institución, con recursos internos.

27. Responsables

La aplicación de este instructivo es responsabilidad del Jefe de Informática.

28. Definiciones

Ambiente de desarrollo: Conjunto de componentes de hardware y software donde se efectúan los procesos de construcción, mantenimiento (como ajustes, cambios y correcciones) y pruebas de sistemas de información.

Ambiente de producción: Conjunto de componentes de hardware y software donde se efectúan los procesos normales de procesamiento de datos, con sistemas e información reales.

BD: Base de datos, colección de datos almacenados en un computador, los cuales pueden ser accedidos de diversas formas para apoyar los sistemas de información de la institución.

Confidencialidad de la información: Protección de información sensible o de acceso restringido contra divulgación no autorizada.

DBA: Administrador de base de datos.

Datos: Objetos en su sentido más amplio (es decir, internos y externos), estructurados y no estructurados, gráficos, audio, video, entre otros.

Desarrollo: Etapa del ciclo de vida del desarrollo de sistemas que implica la construcción de las aplicaciones.

Disponibilidad de la información: Capacidad de acceso y usabilidad de los activos de Informática, por parte de entidades autorizadas.

Integridad de la información: Precisión y suficiencia de la información, así como su validez de acuerdo con los valores y expectativas del negocio.

Modelo de información: Representación de los procesos, sistemas y datos, y sus interrelaciones, mediante los cuales fluye toda la información organizacional.

Pistas de auditoría: Información que se registra como parte de la ejecución de una aplicación o sistema de información y que puede ser utilizada posteriormente para detectar incidencias o fallos. Esta información puede estar constituida por atributos como: la fecha de creación, última modificación o eliminación de un registro, los datos del responsable de dichos cambios o cualquier otro dato relevante que permita dar seguimiento a las transacciones u operaciones efectuadas. Las pistas de auditoría permiten el rastreo de datos y procesos; pueden aplicarse progresivamente (de los datos fuente hacia los resultados), o bien regresivamente (de los resultados hacia los datos fuente).

Programas (códigos) fuentes: texto que contiene las instrucciones del programa escritas en lenguaje de programación.

Requerimientos: necesidad documentada sobre el contenido, forma o funcionalidad de un producto o servicio. Los requerimientos son declaraciones que identifican atributos, capacidades, características y/o cualidades que necesita cumplir un sistema (o un sistema de software) para que tenga valor y utilidad para el usuario. Los requerimientos muestran qué elementos y funciones son necesarias para un proyecto.

Seguridad: Conjunto de controles para promover la confidencialidad, integridad y disponibilidad de la información.

Usuario responsable del módulo: es el usuario o usuarios encargado(s) de velar porque el módulo del sistema a su cargo funcione según la lógica de los procesos de la institución así como las leyes, reglamentos.

Usuario final: es el usuario o usuarios que utilizan un módulo informático como herramienta para la realización de alguna función que tenga asignada.

29. Política de Desarrollo de Software

Usuario responsable del módulo

El departamento de Informática conjuntamente con el departamento de Planificación mantendrá una lista de los módulos de los sistemas y asociado a cada módulo de los sistemas, tendrá la lista de los usuarios responsables de aprobar cambios en dichos módulos. Normalmente un usuario responsable de un módulo se refiere a la persona que dirige un proceso dentro de la institución. En el anexo 1 de este documento se muestra el formato.

Propósito de la política

El propósito de esta política de desarrollo es estandarizar los pasos que la institución seguirá en el desarrollo interno de software, y así asegurar la integridad, disponibilidad y confidencialidad de los Sistemas de Información.

Cumplimiento regulatorio y legal de los requerimientos o cambios a los sistemas de información

El usuario responsable del módulo y el usuario que solicita el cambio o el desarrollo de software, son los responsables de validar y respaldar el cumplimiento regulatorio y normativo correspondiente a la operación de la solución solicitada, por lo tanto se exime al personal de Informática involucrado en el desarrollo de software de validar o interpretar la aplicación de las regulaciones provenientes de áreas operativas.

No obstante es responsabilidad del personal de Informática velar por las regulaciones o políticas asociadas a la confidencialidad, integridad y disponibilidad de la información, por lo tanto cuando algún involucrado de Informática considere que dichas regulaciones o políticas están siendo irrespetadas será su responsabilidad comunicarlo a la Jefatura de Informática.

Para cualquier solicitud de desarrollo de software que la Jefatura de Informática considere riesgosa en términos de confidencialidad, integridad y disponibilidad de los datos se podrá solicitar una validación a la Comisión CITI para analizar la validez de la acción y/o eximir al departamento de Informática de cualquier acción inadecuada sobre los datos por acatamiento de dicho requerimiento.

Clasificaciones de las solicitudes de desarrollo de software

Para poder establecer un adecuado seguimiento y control del desarrollo de software, así como mediciones adecuadas de sus acuerdos de niveles de servicio y planteamiento de acciones correctivas en caso que sean necesarias, se deberán clasificar las solicitudes de la siguiente forma:

1. **Mantenimiento correctivo**: son todas aquellas solicitudes que un usuario final plantea al usuario responsable del módulo para atender uno o varios errores en el sistema de información, se clasifican en:
    a. **Urgente:** son errores en los sistemas y requieren atención inmediata porque están afectando el acuerdo de nivel de servicio y/o algún proceso de trabajo. Los criterios a utilizar para validar si se está haciendo una solicitud de este tipo son: afectación de servicios o productos finales que se generan en la institución, atrasos en otros servicios que dependen del módulo afectado o cantidad de personas con denegación de servicio.
    b. **Regular:** son errores que no requieren atención inmediata por lo tanto ésta se planifica dentro del trabajo regular.
    c. **Usuario:** errores que comete el usuario y no implica ninguna modificación de código por lo tanto solo se le indica al usuario su error y se cierra la solicitud.

2. **Mantenimiento preventivo:** son todas aquellas solicitudes hechas por el mismo departamento de Informática, al conocer que existe una oportunidad de mejora o un error en los sistemas de información.
3. **Mejoras al sistema**: son todas aquellas opciones que incluyen el desarrollo de pequeñas mejoras en opciones ya existentes, los reportes son considerados dentro de esta clasificación.
4. **Nuevas funcionalidades**: son todas aquellas solicitudes que incluyen desarrollo de funciones completamente nuevas al sistema de información, esto puede incluir módulos completos.

Protocolos de trabajo

Mantenimiento correctivo – urgente

1. El usuario reporta error del sistema a través de una llamada, este es el único caso que puede atenderse un servicio sin solicitud formal. Aun así el registro del incidente debe hacerse posterior a su solución.
2. Establecer el impacto a los servicios, delimitar acciones a seguir para atender la emergencia, y analizar las diferentes opciones funcionales con el dueño del proceso afectado, esto lo deben analizar conjuntamente la jefatura de Informática, el responsable de desarrollo, y los involucrados en la solución del error. Tiempo máximo de respuesta es de 1 día. Si el error es producto de un cambio regular al sistema de información se debe evaluar restablecer la versión anterior de éste.
3. Comunicar a los afectados el plan de acción y la duración de éste.
4. Aplicar la corrección y restablecer los servicios.
5. Incluir la solicitud de servicio, y para:
    a. Soluciones definitivas: analizar causa raíz y validar si el error ha sido erradicado
    b. Soluciones temporales: analizar causa raíz y establecer un plan de acción para hacer la corrección definitiva.

Mantenimiento correctivo – regular

1. El usuario reporta error a través de una solicitud de servicio formal en el sistema.
2. Se valida la descripción que el usuario hace del error, se debe validar que la causa raíz del error está clara.
3. Se calendariza y asigna a un responsable de desarrollo la atención del error.
4. El responsable asignado aplicará el resto de las actividades de desarrollo de software.

Mantenimiento correctivo – usuario

1. El usuario reporta error a través de una solicitud de servicio formal en el sistema.
2. Se explica al usuario la función del sistema de información, si el usuario requiere una funcionalidad diferente debe hacer una solicitud de servicio para atender su requerimiento y no un error.

Actividades de desarrollo de software

Incluye los pasos para: Mantenimiento Preventivo, Mejoras al sistema y Nuevas funcionalidades

1. **Solicitar el requerimiento funcional**. El usuario responsable del proceso afectado debe presentar una solicitud de servicio formal a la Comisión CITI donde describe el requerimiento funcional y donde se incluyen los campos mínimos requeridos. Puede ser que el nuevo requerimiento surja como una necesidad que tenga el usuario final, por lo que éste debe transmitirlo al usuario responsable del proceso para que sea debidamente canalizado.
2. **Analizar la factibilidad técnica y el impacto del requerimiento funcional.** Con el debido visto bueno de la Comisión CITI, el jefe de informática de la institución analiza la factibilidad técnica y el impacto del requerimiento para que éste sea aceptado o rechazado, además se debe considerar la pertinencia de la solicitud ya que podrían haber otras opciones en el sistema que ofrecen lo requerido. Una solicitud incompleta o con una descripción poco detallada del requerimiento podría ser rechazada. Además toda solicitud debe estar apegada a los macro procesos y procedimientos establecidos por el departamento de Planificación, en especial aquellos requerimientos que busquen automatizar un cambio drástico al proceso. Si la solitud es aprobada se valida el detalle del requerimiento funcional con el usuario solicitante, al que eventualmente se le podría solicitar mejorar o completar la descripción del requerimiento. Un módulo puede tener en proceso solo una solicitud de desarrollo a la vez (incluyendo las de soporte), con el fin de evitar la afectación de un mismo código fuente por medio de diferentes solicitudes, eventualmente el juicio del experto del Departamento de Informática se podrá aplicar para flexibilizar esta regla. Finalmente se le informa al solicitante el estado de su requerimiento.
3. **Finalizar la documentación del requerimiento:** Una vez analizado el requerimiento funcional se establecen pautas técnicas que podrían completar el requerimiento. Estas pautas podrían estar relacionadas con arquitectura o diseño de la solución, requisitos de desempeño, reutilización, estándares de desarrollo, interfaces de conexión, requisitos de BD, etc. Por lo que son apreciaciones que deben ser evaluadas en forma integral por el Departamento de Informática.
4. **Asignación de requerimiento**: la jefatura del Departamento de Informática valida el requerimiento y si está listo asigna el desarrollo a un programador y lo discute con él.
5. **Diseño del requerimiento**: cuando el programador inicia el desarrollo debe:
    a. Revisar y confirmar telefónicamente o personalmente el requerimiento funcional con el usuario (en caso de ser necesario).
    b. Estimar el tiempo de entrega y comunicarlo al usuario final para coordinar fechas de pruebas. Debe establecer las fechas requeridas en el formulario de solicitud de servicio, estas fechas podrán ser consultadas por el usuario.
    c. Diseñar la solución y en caso necesario ésta deberá ser discutida en el seno del Departamento de Informática para evaluar posibles impactos en otras áreas que pueden conducir a desarrollar una solución más compleja pero de mayor ventaja.
    d. Disponer de los programas fuentes sobre los cuales trabajará

6. **Desarrollo:** una vez que se cuenta con todos los elementos requeridos el programador procede a desarrollar la mejor solución al requerimiento, se deben considerar las políticas de desarrollo y los esquemas de pruebas y producción que se mantienen.
7. **Diseño de la prueba**: Mientras el programador procede a desarrollar el requerimiento, el usuario final puede iniciar el diseño de la prueba funcional, de forma tal que esté lista para la etapa de pruebas de usuario. La prueba debe abarcar las condiciones funcionales que el usuario considere importantes, además el usuario deberá indicar si es necesario actualizar los datos de la base de datos que será utilizada para la prueba. Las pruebas serán agregadas a la solicitud de servicio y deben incluir tanto el proceso de prueba como los conjuntos de datos a probar. El dueño del módulo debe ser notificado y tiene 1 día hábil para validar la prueba, si transcurrido este tiempo no hay cambios ésta se dará por aprobada. Si durante el paso de factibilidad técnica se ha considerado hacer verificaciones adicionales técnicas como pruebas integrales o de carga de trabajo, éstas deberán ser agregadas a las pruebas funcionales ya sea por el programador o el Jefe de Informática.
8. **Pruebas del programador**: una vez que el programador finaliza el desarrollo debe diseñar y ejecutar las pruebas para validar la calidad del código que generó. Adicionalmente debe evaluar si el desarrollo tiene algún impacto en otros módulos, de ser así debe validar la solución y ejecutar pruebas en los módulos que podrían ser afectados.
9. **Pruebas de usuario**: una vez finalizado el desarrollo se ejecutan las pruebas anteriormente diseñadas en las fechas coordinadas con el usuario final, se deben documentar los resultados de la prueba. Una vez que se da por finalizadas las pruebas se acepta el desarrollo del requerimiento por parte del usuario. Si después de 3 días hábiles de la fecha acordada con el usuario éste no ha iniciado las pruebas se procederá a cerrar la solicitud, el Jefe de Informática llevará una estadística de estos casos, y esta estadística se presentará a la Comisión CITI, ya que es sumamente importante informar de los recursos que se invirtieron en soluciones que nunca fueron utilizadas.
10. **Aceptación:** el usuario final acepta el requerimiento y el programador procede a actualizar la documentación de sistema de información. Si después de 3 días hábiles de haberse aceptado la prueba el usuario no ha aceptado el requerimiento se procede a dar por aceptado el requerimiento y empezar el proceso de pase a producción.
11. **Definición de la seguridad:** una vez aceptado el requerimiento el solicitante debe indicar los perfiles de puestos que tendrán acceso a la nueva opción o aclarar cualquier duda relacionada con el esquema de seguridad del nuevo desarrollo. No se ejecutarán pases a producción que dejen las opciones de seguridad abiertas.
12. **Capacitación**: Cuando el cambio tenga un impacto alto en el funcionamiento de las aplicaciones como para cambiar la forma de trabajo de los usuarios finales, se programa una capacitación con éstos. Al finalizar la capacitación, debe quedar constancia de la participación o ausencia de los usuarios
13. **Generar documentación relacionada con el desarrollo**: el programador debe generar o modificar la documentación técnica y de usuario asociada al cambio.
14. **Alistar el pase a producción**.

El programador debe:

a. Coordinar con el Jefe de Informática la fecha en que el desarrollo quedará en producción e informar dicha fecha al usuario final.
b. Alistar el pase a producción
   a. Validar estándares de base de datos (para los desarrollos que lo ameritan)
   b. Ejecutar pruebas de desempeño (para los desarrollos que lo ameritan)
   c. Programar los cambios en la base de datos con los documentos y los insumos para el pase de producción.
   a. Validar que el pase a producción esté correcto (tanto fuentes como ejecutables)
c. Establecer el esquema de recuperación de las funcionalidades originales en caso de error en las nuevas funcionalidades al ejecutar el pase a producción. Este esquema debe definir la tolerancia máxima de error en la funcionalidad según impacto al negocio.

15. **Pase a producción**: el programador ejecuta el pase a producción.
16. **Cierre de solicitud de servicio**: el programador debe cerrar la solicitud de servicio, si el pase a producción genera un error se debe abrir una boleta internamente para registrar el error y así poder medir la incidencia de error en pases a producción.

Anexo 1

Usuarios responsables de aprobar cambios a los sistemas

Sistema - Módulo	**Responsables de aprobar cambios**	
	Puesto	**Nombre**

Marco de gestión para la calidad de la información

30. Objetivo

Garantizar la calidad de la información considerando que debe mantener los atributos de Confidencialidad, Integridad y Disponibilidad, con el fin de reducir los riesgos y mantener los servicios de TI que soportan los servicios finales de la institución hacia el habitante

31. Alcance

Este documento aplica para mantener una mejora continua de la calidad de la información.

32. Responsables

La aplicación de este instructivo es responsabilidad del Jefe del Departamento de Informática.

33. Definiciones

Ambiente de desarrollo: Conjunto de componentes de hardware y software donde se efectúan los procesos de construcción, mantenimiento (como ajustes, cambios y correcciones) y pruebas de sistemas de información.

Ambiente de producción: Conjunto de componentes de hardware y software donde se efectúan los procesos normales de procesamiento de datos, con sistemas e información reales.

BD: Base de datos, colección de datos almacenados en un computador, los cuales pueden ser accedidos de diversas formas para apoyar los sistemas de información de la institución.

DBA: Administrador de base de datos.

Datos: Objetos en su sentido más amplio (es decir, internos y externos), estructurados y no estructurados, gráficos, sonido, entre otros.

Desarrollo: Etapa del ciclo de vida del desarrollo de sistemas que implica la construcción de las aplicaciones.

Modelo de información: Representación de los procesos, sistemas y datos, y sus interrelaciones, mediante los cuales fluye toda la información organizacional.

Pistas de auditoría: Información que se registra como parte de la ejecución de una aplicación o sistema de información y que puede ser utilizada posteriormente para detectar incidencias o fallos. Esta información puede estar constituida por atributos como: la fecha de creación, última modificación o eliminación de un registro, los datos del responsable de dichos cambios o cualquier otro dato relevante que permita dar seguimiento a las transacciones u operaciones efectuadas. Las pistas de auditoría permiten el rastreo de datos y procesos; pueden aplicarse progresivamente

(de los datos fuente hacia los resultados), o bien regresivamente (de los resultados hacia los datos fuente).

Programas (códigos) fuentes: texto que contiene las instrucciones del programa escritas en lenguaje de programación.

Requerimientos: necesidad documentada sobre el contenido, forma o funcionalidad de un producto o servicio. Los requerimientos son declaraciones que identifican atributos, capacidades, características y/o cualidades que necesita cumplir un sistema (o un sistema de software) para que tenga valor y utilidad para el usuario. Los requerimientos muestran qué elementos y funciones son necesarias para un proyecto.

Seguridad: Conjunto de controles para promover la confidencialidad, integridad y disponibilidad de la información.

Usuario responsable del módulo: es el usuario o usuarios encargado(s) de velar porque el módulo del sistema a su cargo funcione según la lógica de los procesos de la institución así como las leyes, reglamentos

34. Marco de gestión para la calidad de la información

Contexto del marco

Como parte importante del quehacer diario del Departamento de Informática, se encontrarán errores o problemas que afectan la calidad de la información y por ende la entrega de los servicio de TI. La calidad de la información está vinculada a dos aspectos importantes:

1. El desarrollo de software, la forma en la cual se da tratamiento a los datos que se procesan y la existencia de cargas masivas de datos
2. La calidad de los datos que se ingresan a los sistemas de información por parte del usuario

Para ambos casos el Departamento de Informática debe aplica técnicas en su desarrollo de software que permita establecer controles que disminuyan los errores en la digitación, carga, procesamiento y utilización de los datos. Muchas de las técnicas están alineadas con la validación de datos de forma integral. Sin embargo en algunos casos esos controles no podrían cubrir la calidad necesaria y se podrían necesitar acciones de mejora continua para su corrección. Este marco provee la guía ya sea para establecer los controles que aseguran la calidad de los datos o corregir errores producto de la no calidad de la información.

Calidad de la información

Se considera información de calidad aquella que cumpla con los tres atributos importantes de seguridad, estos son:

1. **Confidencialidad de la información**: Protección de información sensible contra divulgación no autorizada.

2. **Integridad de la información:** Precisión y suficiencia de la información, así como su validez de acuerdo con los valores y expectativas del negocio.
3. **Disponibilidad de la información:** Capacidad de acceso y usabilidad de los activos de TI, por parte de entidades autorizadas.

Por lo tanto se considera de no calidad la información que no cumpla con estos requisitos y que debe de ser corregida para que se cumplan éstos

Medidas para asegurar la calidad de información

El Departamento de Informática debe asegurar en sus procesos relacionados con la gestión de la información, el cumplimiento de los requisitos de la calidad de información, para ello debe incluir controles o técnicas que permitan mantener dichos atributos. Para asegurar que dichos controles sean aplicados será utilizado el ciclo o espiral de mejora continua que implica las siguientes fases: planificar-hacer-verificar-actuar, como se muestra en la siguiente figura:

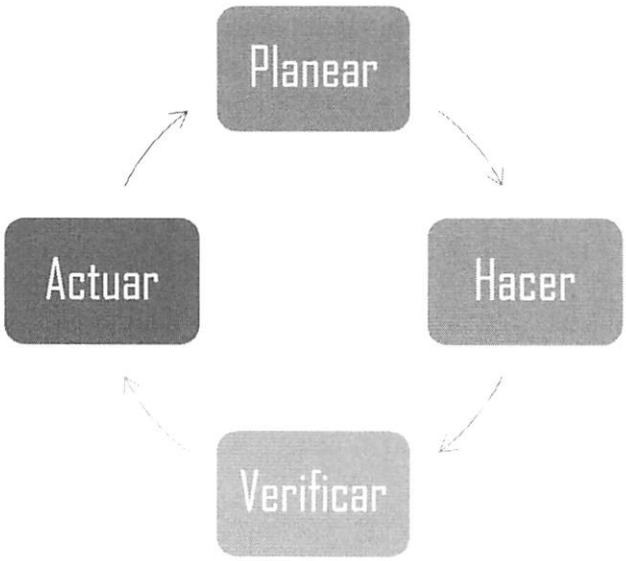

Figura 1: Ciclo de mejora continua

Cada vez que Departamento de Informática considere que debe agregar calidad a la información acudirá a dicho ciclo.

Planear (PLAN)

En esta etapa se establecen las actividades que deberán ser ejecutadas para obtener el resultado esperado (ya sea la implementación del control o la mejora esperada). Al basar las acciones en el resultado esperado, la exactitud y cumplimiento de las especificaciones a lograr se convierten también en un elemento a mejorar. Cuando sea posible conviene realizar pruebas de preproducción o pruebas piloto para probar los posibles efectos. Estas actividades podrían incluir:

1. Recopilar datos para profundizar en el conocimiento del proceso.

2. Detallar las especificaciones de los resultados esperados.
3. Definir las actividades necesarias para lograr el producto o servicio, verificando los requisitos especificados.
4. Establecer los objetivos y procesos necesarios para conseguir resultados necesarios de acuerdo con los requerimientos del cliente y las políticas organizacionales.
5. Evaluar fuentes de error de datos en el proceso

Algunas herramientas de planificación que se podrán utilizar son:

1. Planes de Acción
2. Diagrama de Gantt (planificación y seguimiento de actividades y proyectos)
3. Método de diseño intuitivo o diseño a prueba de errores.
4. Análisis de necesidades y expectativas del cliente.

Hacer (DO)

Se realizan los cambios para implantar la mejora propuesta. Generalmente conviene hacer una prueba piloto para probar el funcionamiento antes de realizar los cambios a gran escala.

Verificar (CHECK)

Pasado un periodo previsto de antemano, se recopilan y analizan los indicadores o datos de control, comparándolos con los requisitos especificados inicialmente en la etapa de planificación, para saber si se han cumplido y, en su caso, evaluar si se ha producido la mejora esperada. Esto implica monitorear la implementación del plan y evaluar si la ejecución ha sido exitosa y si se han obtenido los resultados esperados.

Algunas herramientas de evaluación que se podrán utilizar son:

1. Diagrama de Pareto: curva 80%-20% para organizar datos y centrar los esfuerzos en lo más importante.
2. Diagrama de Pescado: Estudio para localizar las causas de los problemas.
3. Cuadro de mando Integral: Modelo de gestión, con un soporte de información periódica para la dirección de los procesos de la empresa.
4. Listas de Control.

Actuar (ACT)

A partir de los resultados conseguidos en la fase anterior se procede a recopilar lo aprendido y a ponerlo en marcha. También suelen aparecer recomendaciones y observaciones que suelen servir para volver al paso inicial de Planificar y así el círculo nunca dejará de fluir. El cuarto paso tiene que ver con la necesidad de cerrar el ciclo con la realimentación para acercar los resultados obtenidos a los objetivos.

COMUNÍQUESE. Dado en la Ciudad de San José, a las nueve horas cuarenta y cinco minutos del dos de febrero de dos mil dieciocho. **Montserrat Solano Carboni. Defensora de los Habitantes de la República.**