DECRETO No. 24

EL PRESIDENTE DE LA CORTE DE CUENTAS DE LA REPÚBLICA,

CONSIDERANDO:

I. El acelerado incremento y desarrollo de las Tecnologías de Información y Comunicación (TIC), en las entidades gubernamentales y la automatización de sus procesos con tendencia en la prestación de servicios a los ciudadanos en forma remota.

II. La aplicación de las TIC ocasiona nuevas formas de "riesgos en tecnología para las entidades", por lo cual se vuelve imprescindible controlar y fiscalizar de manera especializada la administración de los recursos tecnológicos.

III. Que las entidades públicas en su mayoría no han normalizado la administración y riesgos en lo concerniente a planificación y organización de recursos, adquisición e implementación, entrega y soporte de servicios, monitoreo y evaluación, seguridad de la información entre otros aspectos de las tecnologías de información y comunicación.

IV. Que la Ley de la Corte de Cuentas de la República, en su Art. 5, numeral 2), establece la atribución de dictar las políticas, normas técnicas y demás disposiciones para la práctica del control interno en las entidades sujetas a la fiscalización.

POR TANTO:

En uso de las facultades conferidas por el artículo 195, numeral 6 de la Constitución de la República de El Salvador y el artículo 5, numeral 2 y artículo 24 numeral 1 de la Ley de la Corte de Cuentas de la República,

DECRETA el siguiente:

REGLAMENTO PARA EL USO Y CONTROL DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN EN LAS ENTIDADES DEL SECTOR PÚBLICO

CAPÍTULO I

DISPOSICIONES GENERALES

Art. 1.- El presente reglamento tiene por objeto establecer, normas, principios, lineamientos y estándares, aplicables a las tecnologías de información y comunicación, para la optimización de recursos tecnológicos, que utilicen los sujetos a que se refiere el artículo 3 de la Ley de la Corte de Cuentas de la República y estipular los mecanismos que impulsarán su desarrollo y promoción en todo el ámbito del Estado, y tomando en cuenta que conforme surjan nuevas tecnologías se hace necesario implementar nuevos controles internos de seguridad, integridad y confiabilidad de los sistemas informáticos que se utilizan en el desarrollo de sus actividades.

Definiciones

Art. 2.- A los efectos del presente Reglamento, se entenderá por:

1) **Amenaza:** es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

2) **Automatización:** La automatización es un sistema donde se trasfieren tareas realizadas habitualmente por operadores humanos a un conjunto de elementos tecnológicos, que sirven para estandarizar los procesos de trabajo; desarrollar componentes reutilizables y configurables; y automatizar actividades rutinarias con las tecnologías adecuadas.

3) **Característica de la información:** Debe cumplir con la normativa interna de la Información y Comunicación, entre las cuales se mencionan la veracidad, oportunidad, disponibilidad, confiabilidad, confidencialidad.

4) **Ciclo de vida del desarrollo de sistemas:** Proceso que se sigue para construir, entregar y hacer evolucionar el sistema de información, desde la concepción de una idea hasta la entrega y retiro del sistema.

5) **COBIT:** Objetivos de Control para Información y Tecnologías Relacionadas (COBIT, en inglés: Control Objectives for Information and Related Technology). es una guía de mejores prácticas, dirigida al control y supervisión de tecnología de la información (TI). Posee una serie de recursos que pueden servir de modelo de referencia para la gestión de TI en la Organización.

6) **Contingencia:** interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

7) **Control de cambios:** Conjunto de procedimientos para administrar las configuraciones de los sistemas de información, mantener la calidad del software y la capacidad. Se basa en las solicitudes de cambios.

8) **Datos redundantes:** La redundancia hace referencia al almacenamiento de los mismos datos varias veces en diferentes lugares o en el mismo sistema de información.

9) **DMZ:** Tiene que ver con la seguridad informática, una zona desmilitarizada (conocida también como DMZ, sigla en inglés de demilitarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente en Internet.

10) **Estándares abiertos:** Especificaciones técnicas, publicadas y controladas por alguna organización que se encarga de su desarrollo, las cuales han sido aceptadas por la industria, estando a disposición de cualquier usuario para ser implementadas en un software libre u otro, promoviendo la competitividad, interoperatividad o flexibilidad.

11) **Estudio de factibilidad:** Análisis financieros, económicos y operativos de una inversión (dada una opción tecnológica -estudio de prefactibilidad). En la fase de pre-inversión la eventual etapa subsiguiente es el diseño final del proyecto.

12) **Firma digital:** Una firma digital es un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente determinar la entidad originadora de dicho mensaje.

13) **Gobernabilidad de las TIC:** Una estructura de relaciones y procesos para dirigir y controlar la Entidad a fin de lograr sus objetivos y metas, agregando efectividad al mismo tiempo que se equilibra el riesgo con el uso de TIC en sus procesos.

14) **Gobierno electrónico:** Modelo de gestión pública que se fundamenta en el uso intensivo de las tecnologías de información para proveer medios ágiles, confiables y efectivos de información, comunicación y participación de los ciudadanos, para la prestación segura y directa de servicios, y que tiene como objetivo fundamental transformar al Estado como resultado de las mejoras de los procesos y el aumento de la eficiencia y transparencia del Poder Público, generados por dichas tecnologías.

15) **Huellas de auditoría en la base de datos:** Elementos o líneas que permitan rastrear los caminos que siguen los datos a través del programa y que se utilizan para comprobar la ejecución de las validaciones de datos previstos.

16) **Integridad de la información:** La información sólo puede ser modificada por quien está autorizado y de manera controlada.

17) **Integridad de la plataforma tecnológica:** Es la capacidad de la Plataforma de realizar la corrección y completitud de los datos en toda la red.

18) **ITIL:** Librería de Infraestructura de Tecnología de Información (TI), es un conjunto de lineamientos sobre la administración y procuración de servicios operativos de TI.

19) **Impacto:** Consecuencia de la materialización de una amenaza.

20) **ISO 27000:** Estándar para la seguridad de la información.

21) **Modelo de madurez:** El Modelo de Madurez, consiste en un método que evalúa el grado de control sobre los procesos de TI de una organización en una escala de 0 a 5, donde el menor (0) significa "No existe" y el mayor "Optimizado" (5).

22) **Pared de fuego en Informática:** Conocido como cortafuegos (firewall en inglés), es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Existen además dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico de información sobre la base de un conjunto de normas y otros criterios.

23) **Plataforma tecnológica:** Son los elementos de Hardware y software como servidores, estaciones de trabajo PC´s, redes con que cuenta una Entidad.

24) **Plan de Contingencia:** Conjunto de pasos o procedimientos necesarios para recuperar y estabilizar las operaciones informáticas en la Entidad, en caso de producirse una eventualidad que afecte la operación normal de los sistemas de información. Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de una compañía.

25) **Propiedad Intelectual:** Es toda creación del intelecto humano. Los derechos de propiedad intelectual protegen los intereses de los creadores al ofrecerles prerrogativas en relación con sus creaciones.

26) **Riesgo:** Evento fortuito e incierto resultante de las acciones humanas, sistemas de información o por la acción de una causa externa que puede intervenir en el cumplimiento de la misión, visión, objetivos y metas que han sido definidos por la Entidad, causando perjuicios directos e indirectos.

    Se mide por medio de una combinación del impacto y la probabilidad de ocurrencia.

27) **Seguridad de la información:** Es el conjunto de medidas preventivas y reactivas de las instituciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

28) **Talento Humano:** Capacidad de la persona que integra habilidades, destrezas, experiencias y aptitudes propias.

29) **TIC:** Conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de información.

    Las TIC (Tecnologías de la Información y Comunicación) son aquellas tecnologías que se necesitan para la gestión y transformación de la información, y muy en particular el uso de ordenadores y programas que permiten crear, modificar, almacenar, administrar, proteger y recuperar esa información.

30) **Ubicuidad en TIC:** Significa estar en todas partes al mismo tiempo.

    La tecnología nos permite estar en diferentes lugares al mismo tiempo, la profunda conexión entre lo real y lo virtual, la disponibilidad de la información a cualquier hora, desde cualquier lugar y con una variedad de dispositivos tecnológicos, que modifican la forma de acceder a la información y al conocimiento.

31) **VPN:** Es una red virtual que se crea dentro de otra red real, como puede ser Internet.

32) **Vulnerabilidad:** posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

CAPÍTULO II

ORGANIZACIÓN DE TIC

Art. 3.- Cada entidad del sector público debe establecer una Unidad de Tecnologías de Información y Comunicación, ubicada a un nivel jerárquico que le permita ejercer la gobernabilidad e independencia funcional dentro de la entidad, conforme a su nivel de madurez tecnológico y de acuerdo a su tamaño, alcance y ámbito de gestión. La escala de madurez se clasifica, según las siguientes categorías:

0 No existe: Los procesos gerenciales no son aplicados: No existen procesos reconocidos. La organización no ha reconocido que existe un problema que debe ser resuelto.

1 Inicial: Los procesos no están planificados y se encuentran desorganizados: No existen procesos estandarizados aunque sí procedimientos que suelen ser aplicados de forma individual o conforme las necesidades que se presentan en un momento determinado.

2 Repetitivo: Los procesos siguen un patrón regular: Los procesos se han desarrollado a un determinado nivel y procedimientos similares son seguidos por diferentes personas que realizan la misma tarea dentro de la empresa. No hay entrenamiento o comunicación formal de estos procedimientos. Las responsabilidades están en manos del individuo.

3 Definido: Los procesos están documentados y comunicados: Los procedimientos han sido estandarizados, documentados y comunicados por medio de entrenamiento. Sin embargo, está pendiente el cumplimiento de dichos procesos por cada individuo, con lo cual es poco probable que las desviaciones sean detectadas. Los procedimientos por si solos no son sofisticados pero son la formalización de mejores prácticas.

4 Gerenciado: Los procesos son monitoreados y medidos: Es posible la medición y monitorización conforme a los procedimientos y realizar acciones donde existan procesos que no parezcan estar funcionando con efectividad. Los procesos están bajo constantes mejoras y se proveen de buenas prácticas. Las herramientas de automatización son empleadas de manera limitada o fragmentada.

5 Optimizado: Basados en mejores prácticas y están automatizadas. Los procesos han sido refinados a nivel de mejores prácticas, basados en resultados de mejoras continuas y modelos de madurez respecto de otras organizaciones. Las TI son usadas para automatizar de manera integral el flujo de trabajo, suministrando herramientas para mejorar la efectividad y la calidad, haciendo que la organización se adapte de manera rápida a los cambios del entorno.

Art. 4.- La entidad debe de definir y mantener actualizado el Manual de Organización y Funciones de la Unidad de TIC y de Puestos para el personal, de manera que las funciones y responsabilidades queden claramente establecidas.

Art. 5.- La Unidad de TIC deberá proponer a la máxima autoridad la adopción de mejores prácticas (estándares abiertos) y controles para la gestión de las TIC, que se requiera para el logro de los objetivos.

Art. 6.- La Unidad de TIC debe realizar un proceso de planificación de TIC de acuerdo con la planeación estratégica institucional, que facilite la consecución de sus logros futuros.

Art. 7.- El Plan Estratégico de TIC debe:

a) Contener los objetivos e iniciativas estratégicas del área de TIC, que deben estar acordes a los objetivos estratégicos institucionales;

b) Definir cómo los objetivos estratégicos de TIC serán alcanzados y medidos, establecer los indicadores de desempeño de conformidad con los objetivos estratégicos de TIC;

c) Contemplar el presupuesto operacional y de inversiones, las estrategias de suministro y de adquisición (contratación de servicios y adquisición de equipos) y los requisitos legales;

d) Ser formalmente aprobado y divulgado para que sea ejecutado por las partes interesadas.

Art. 8.- La Unidad de TIC debe de elaborar los planes anuales operativos diseñados de tal manera que defina los objetivos a cumplir y alineado con los objetivos estratégicos y/o operativos institucionales, actividades a desarrollar, programación, indicadores de gestión y su seguimiento, recursos de TIC, responsables y fechas de ejecución.

Art. 9.- La gestión de las Tecnologías de Información y Comunicación, es responsabilidad de la máxima autoridad y de la Unidad de TIC, la cual debe contar con los recursos que garanticen el cumplimiento de los objetivos institucionales.

Art. 10.- La Unidad de TIC, elaborará y ejecutará el presupuesto asignado para la gestión de las tecnologías de información y comunicación institucional y los proyectos tecnológicos viables a desarrollar, conforme a su nivel de madurez tecnológico de acuerdo a su tamaño, alcance y ámbito de gestión, los objetivos estratégicos y operativos de la institución y acorde con el plan de compras institucional.

CAPÍTULO III

GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Art. 11.- La Unidad de TIC, deberá adoptar una metodología de gestión de riesgos, debiendo documentar el proceso de identificación, análisis, administración y evaluación de riesgos de TIC.

Art. 12.- La Unidad de TIC, se asegurará que los controles internos diseñados mitiguen en gran medida los riesgos residuales obtenidos en el análisis de riesgos, siendo factible y con menor inversión la administración de éstos.

CAPÍTULO IV

PROYECTOS DE TECNOLOGÍAS DE INFORMACION Y COMUNICACIONES

Art. 13.- La Unidad de TIC, efectuará diagnóstico de las necesidades y requerimientos tecnológicos de las dependencias de la Entidad y deberá proyectar las mejoras de las tecnologías de información y comunicaciones, considerando los costos de transición, viabilidad, capacidad técnica, instalaciones, riesgos tecnológicos, vida útil y tasas de crecimiento de la infraestructura tecnológica.

Art. 14.- La Entidad deberá contar con una comisión responsable de la ejecución de los proyectos de TIC, desde la fase de inicio hasta la puesta en marcha del proyecto, definiendo responsabilidades de cada miembro de la comisión.

CAPÍTULO V

SISTEMAS DE INFORMACIÓN

Art. 15.- La Unidad de TIC implementará la metodología para el ciclo de vida del desarrollo de sistemas, asegurando que los sistemas de información sean eficaces, seguros, íntegros, eficientes y económicos, que impidan la modificación no autorizada; asimismo, se ajuste al cumplimiento de las leyes, reglamentos y normativa vigente que les sean aplicables y considerar además lo siguiente:

a) Se deberá priorizar y fomentar el desarrollo de los sistemas de información con recursos internos de la entidad.

b) Definir una adecuada separación de las funciones en los ambientes de desarrollo y producción.

c) Procedimientos de actualización en los manuales de usuario y técnico, para el uso de los sistema en producción y que se encuentra documentado el Control de cambios (versiones del Sistema) y los requerimientos se encuentren autorizados, realizados en el Sistema dentro del mismo.

Art. 16.- La Unidad de TIC debe contar con políticas y procedimientos para el procesamiento de la información, desde su origen, relacionados con la captura, actualización, procesamiento, almacenamiento y salida de los datos, que asegure que la información sea completa, precisa, confiable y válida para la toma de decisiones.

Controles de cambio

Art. 17.- La Unidad de TIC, deberá identificar los cambios en las soluciones automatizadas, conforme a un análisis técnico, económico y operativo, con las diferentes alternativas de solución, analizando el impacto de la implementación de cambios, planificando las pruebas para reducir incidentes, caídas de red, e implementando y documentando los cambios exitosos y en tiempo disponible.

Tercerización de servicios de TIC

Art. 18.- Al contratar servicios tecnológicos con terceros, la Unidad de Tecnologías de Información y Comunicación deberá justificar la tercerización del servicio de software, siendo responsables de administrar los aspectos técnicos en la adquisición de los bienes y/o servicios de tecnología de información y comunicación.

Debe efectuarse una efectiva administración del riesgo, considerando acuerdos de confidencialidad, contratos de garantía, viabilidad de la continuidad del proveedor, conformidad con los requerimientos de seguridad, proveedores alternativos, penalizaciones e incentivos, entre otros.

Art. 19.- La Unidad de TIC deberá implementar y gestionar la aprobación de una metodología estándar de desarrollo y adquisición de software, realizado con terceros. Documentando en un expediente o portafolio el ciclo de vida de desarrollo de sistemas de los proyectos tecnológicos.

Art. 20.- La Unidad de TIC deberá contar con registros para el control de la vigencia de las garantías de fábrica que cubran desperfectos y aseguren el funcionamiento de los equipos de tecnología de información y comunicación, para lo cual creará procedimientos en conjunto con la Unidad de Adquisiciones y Contrataciones Institucional.

Art. 21.- La Unidad de TIC, deberá emitir procedimientos de control para monitorear los servicios de enlaces brindados por terceros, asegurándose que se cumpla con la recepción del servicio, la confidencialidad e integridad de la información a la cual tengan acceso, y operación de la infraestructura tecnológica.

Convenios y donaciones relacionados con TIC

Art. 22.- La máxima autoridad conforme a sus necesidades podrá realizar convenios entre instituciones u organismos para apoyarse con recursos de tecnología de información y comunicaciones y para compartir información de las bases de datos, definiendo el objetivo de la información o registros a compartir y las políticas de seguridad para el acceso y confidencialidad de la información.

Art. 23.- La máxima autoridad y la Jefatura de la Unidad de TIC, definirán los procedimientos de los recursos tecnológicos a compartir con Entidades y Organismos Gubernamentales, definiendo los productos entregables, estándares de desarrollo de los sistemas a utilizar y la propiedad intelectual del software.

Art. 24.- Las entidades deberán documentar la recepción de donaciones de hardware, software y aplicativos, evaluando previamente los aspectos técnicos, como los códigos fuentes del software, manuales técnicos y de usuarios, mantenimientos y mejoras que podrá tener el software, aspectos operativos (funcionamiento del software) y legales (propiedad intelectual).

Art. 25.- Los software procedentes de donaciones, deberán ser documentados en lo siguiente: Análisis de la adaptabilidad del sistema a los procesos que se automatizarán, necesidades de información de los usuarios, la funcionalidad de los procesos que serán automatizados con el nuevo software, la capacitación al personal técnico de la Unidad de TIC para la administración, mantenimientos y mejoras al sistema si éste lo permite y de los usuarios que operarán el sistema de información.

CAPÍTULO VI

SEGURIDAD DE LA INFORMACIÓN

Art. 26.- La máxima autoridad, gerencias y demás jefaturas, deberán asegurar la correcta administración de la seguridad de la información, estableciendo y manteniendo controles que permitan que la información cumpla con las características de confidencialidad, integridad, disponibilidad, confiabilidad y cumplimiento legal.

Art. 27.- La Unidad de TIC administrará adecuadamente la seguridad física y lógica de sus recursos; estableciendo políticas y procedimientos que permitan identificar, autenticar y autorizar el acceso a los sistemas de información, sistemas operativos y bases de datos y dar seguimiento a las transacciones que se ejecutan en los sistemas de información, bases de datos y sistemas operativos, así como el resguardo de servidores, switch y otros dispositivos.

Art. 28.- La Unidad de TIC debe de establecer políticas y procedimientos de prevención, detección y corrección de virus; la utilización del correo electrónico; restringir el tráfico de información hacia dentro y fuera de la red institucional (pared de fuego) en todos aquellos puntos con acceso a redes públicas de datos o VPN.

Seguridad de las bases de datos

Art. 29.- La Unidad de TIC, deberá garantizar la seguridad lógica a las bases de datos institucionales que resguardan información, evitando en la medida de lo posible la generación de datos redundantes o repetitivos. El usuario del sistema de información es el responsable del contenido de la información almacenada en las bases de datos.

Art. 30.- La Unidad de TIC deberá implementar y desarrollar políticas de control y designación de roles y responsabilidades de la administración de la base de datos y usuarios de los sistemas de información. De igual forma deberá documentar, los procedimientos de solicitud, creación, mantenimiento, eliminación del usuario y cambios de claves.

Art. 31.- La Unidad de TIC deberá garantizar que las bases de datos contengan huellas de auditoría, que registren los eventos de las fechas y actividades que realizan los usuarios, tales como: adición, eliminación, modificación de datos entre otros, con el fin de garantizar la identificación de los accesos a la información.

Art. 32.- La Unidad de TIC deberá garantizar la separación de funciones entre los administradores de base de datos, los desarrolladores de sistemas y los que procesan los datos en los sistemas de información automatizados.

Art. 33.- La Unidad de TIC deberá realizar planes de respaldo y resguardo en sitio remoto y procedimientos para la recuperación de datos, que permitan asegurar la información de acuerdo a su importancia y criticidad.

Seguridad de la infraestructura tecnológica

Art. 34.- La Unidad de TIC definirá políticas y procedimientos de seguridad que garantice la confiabilidad, integridad y compatibilidad de la plataforma tecnológica y que contemple el suministro de energía eléctrica para la continuidad del negocio en caso de fallas temporales en la red eléctrica.

Art. 35.- La Unidad de Tecnologías de Información y Comunicación, deberá implementar medidas de seguridad física y lógica para las redes institucionales, esquemas de red con DMZ, consolas de antivirus, manteniéndolos actualizados en la red. Para el caso de los equipos informáticos sin acceso a la red, se deberán de crear políticas para su actualización.

Art. 36.- La Unidad de TIC debe de elaborar y ejecutar un plan de Mantenimiento de Equipo Informático debidamente diseñado, que contenga objetivos, políticas, prioridades, programación de actividades en el que se identifique a los responsables de ejecutarlas y la determinación de los costos estimados; además, la identificación de metas programadas formuladas de manera precisa, factible, viable y medible, para que se pueda ejercer un seguimiento, evaluación de objetivos y su cumplimiento. Este plan deberá ser comunicado a los niveles responsables de su ejecución.

Art. 37.- La Unidad de TIC deberá de contar con la documentación de soporte de las operaciones que realicen (físicas o electrónicas), para justificar e identificar la naturaleza, finalidad y resultado de la actividad realizada. La documentación debe estar debidamente custodiada y contar con procedimientos para su actualización oportuna.

Art. 38.- La máxima autoridad y la Unidad de TIC, deberán emitir políticas que fomenten el flujo oportuno de información interna por medio del uso del correo electrónico institucional como medio oficial de comunicación, digitalización de documentos, utilización del sitio web institucional, intranet e internet. Deberán definir por escrito los controles generales de los recursos de tecnología de información, para asegurar la eficiencia, efectividad, confiabilidad y seguridad de la información.

Continuidad de las operaciones

Art. 39.- La Unidad de TIC, deberá contar con un plan de contingencia autorizado por la máxima autoridad de la entidad, este plan debe ser viable, que detalle las acciones, procedimientos y recursos financieros, humanos y tecnológicos, considerando los riesgos y amenazas de TIC que afecten de forma parcial o total la operatividad normal de los servicios de la Entidad, categorizando el tipo de acción a realizar en cuanto a la medición en tiempo para el restablecimiento de las operaciones tecnológicas, este plan debe probarse y actualizarse atendiendo la realidad tecnológica de la entidad al menos una vez al año. Deberá ser comunicado a los niveles pertinentes.

Art. 40.- El Área de TIC debe establecer y mantener actualizadas políticas y procedimientos para el respaldo y recuperación de la información, que le permitan tener acceso a la misma durante periodos de contingencias, causados por desperfectos en los equipos, pérdida de información u otras situaciones similares.

Art. 41.- La Unidad de TIC debe realizar un diagnóstico o estudio para determinar la necesidad de contar con cobertura de seguros para los principales equipos de cómputo y comunicaciones, que le permitan mitigar el riesgo provocado ante cualquier tipo de contingencia y desastre natural.

CAPÍTULO VII

ENTREGA Y SOPORTE DE SERVICIOS

Art. 42.- La Unidad de TIC deberá identificar y registrar los incidentes y problemas de TIC, categorizar, diagnosticar, resolver, controlar errores, evaluar problemas graves y reportar los informes que contienen los problemas resueltos y pendientes, el estatus de su procesamiento y las soluciones.

Art. 43.- La Unidad de TIC deberá emitir procedimientos de control para gestionar la configuración, cambios y liberación de versiones de software mediante la definición de planes y políticas.

Art. 44.- La Unidad de TIC deberá desarrollar procedimientos de control para la instalación y desinstalación de software y dispositivos de información y comunicación, los que deberán ser reinstalados para su funcionamiento y efectividad en el uso.

Licenciamiento de software

Art. 45.- Todo el software instalado en la entidad, deberá estar amparado con la respectiva licencia extendida por el fabricante, otorgando a la entidad el derecho de instalación y uso de los mismos, de conformidad a lo establecido por la ley.

Art. 46.- La Unidad de Activo Fijo deberá de elaborar y actualizar un inventario de Software y aplicaciones. La Unidad de TIC deberá controlar el software instalado en cada uno de los equipos informáticos institucionales.

Art. 47.- La Unidad de TIC es la responsable de la instalación de software libre, debiendo justificar los usuarios las necesidades de su uso.

El software libre instalado debe cumplir con los aspectos técnicos informáticos.

Art. 48.- La Unidad de Tecnologías de Información y Comunicación deberá mantener registros actualizados con las características técnicas de la infraestructura tecnológica, licencias de software, aplicativos, manejadores de base de datos y la documentación de los controles de cambios de los sistemas de información. Estos registros deberán conciliarse con los controles de inventarios de activo fijo y con los registros contables.

Gobierno electrónico

Art. 49.- Las entidades que han adoptado un modelo de gestión de gobierno electrónico para el manejo de contratos, transacciones económicas, compras, pagos, entre otros aspectos que se realizan on-line, deberán emitir procedimientos para el manejo de firma digital, estableciendo por escrito los procesos, funcionarios responsables, medidas de seguridad ante los riesgos identificados, alcance, confidencialidad en la comunicación, entre otros aspectos.

CAPÍTULO VIII

DISPOSICIONES FINALES

Art. 50.- Con el propósito de mantener actualizado el presente Reglamento, éste deberá ser revisado por una Comisión nombrada por el Presidente de esta Corte, cuando lo estime conveniente.

Art. 51.- El presente Reglamento entrará en vigencia a partir del día de su publicación en el Diario Oficial.

Dado en San Salvador, a los veinticuatro días del mes de junio del dos mil catorce.

LIC. ROSALÍO TÓCHEZ ZAVALETA,
PRESIDENTE DE LA CORTE DE CUENTAS DE LA REPÚBLICA.