**UNIDAD DE INFORMÁTICA**

**OFICINA DE PLANIFICACION DEL AREA METROPOLITANA DE SAN SALVADOR**





**Políticas y procedimientos de los controles generales de las Tecnologías de Información y Comunicación.**

**SAN SALVADOR, 26 DE ENERO DE 2016**

**Ámbito de aplicación**

Las políticas definidas en este documento son de aplicación para toda la Oficina de Planificación del Área Metropolitana OPAMSS, cuyas actividades se apoyan en instrumentos informáticos.

**Actualizaciones de este manual**

Este instrumento rige una vez que el COAMSS lo apruebe y haya ordenado su puesta en marcha de manera oficial. Deberá ser revisado y actualizado formalmente por lo menos una vez cada año, siendo responsabilidad de la jefatura de la Unidad de Informática de realizar este proceso.

Durante el proceso de implementación cualquier usuario podrá hacer observaciones, con el objetivo de mejorar y/o modificar cláusulas o políticas, las cuales se harán llegar a la jefatura de la Unidad de Informática.

**Tabla de Contenido**

**[Resumen](#_Toc441659417)** [5](#_Toc441659417)

**[Objetivos](#_Toc441659418)** [5](#_Toc441659418)

***[Objetivo General](#_Toc441659419)*** [5](#_Toc441659419)

***[Objetivos Específicos:](#_Toc441659420)*** [5](#_Toc441659420)

**[Supervisión de las políticas](#_Toc441659421)** [5](#_Toc441659421)

**[Violación a las políticas](#_Toc441659422)** [5](#_Toc441659422)

**[1.](#_Toc441659423)****[Políticas Generales](#_Toc441659423)** [6](#_Toc441659423)

**[2.](#_Toc441659424)****[Políticas Administrativas](#_Toc441659424)** [6](#_Toc441659424)

***[2.1.](#_Toc441659425)******[Políticas para el planeamiento y administración de actividades](#_Toc441659425)*** [6](#_Toc441659425)

***[2.2.](#_Toc441659426)******[Políticas sobre los servicios que ofrece la Unidad de Informática](#_Toc441659426)*** [6](#_Toc441659426)

***[2.3.](#_Toc441659427)******[Políticas para el acceso físico la Unidad Informática y área de servidores](#_Toc441659427)*** [7](#_Toc441659427)

***[2.4.](#_Toc441659428)******[Políticas para la documentación y mantenimiento de manuales de la Unidad de Informática](#_Toc441659428)*** [7](#_Toc441659428)

***[2.5.](#_Toc441659429)******[Políticas para la adquisición de nuevas tecnologías](#_Toc441659429)*** [7](#_Toc441659429)

***[2.6.](#_Toc441659430)******[Políticas sobre inventario de equipo](#_Toc441659430)*** [8](#_Toc441659430)

***[2.7.](#_Toc441659431)******[Políticas sobre reparación de equipos](#_Toc441659431)*** [8](#_Toc441659431)

**[3.](#_Toc441659432)****[Políticas relativas a sistemas de Información](#_Toc441659432)** [8](#_Toc441659432)

***[3.1.](#_Toc441659433)******[Políticas generales para el desarrollo de sistemas de información](#_Toc441659433)*** [8](#_Toc441659433)

***[3.2.](#_Toc441659434)******[Políticas para el desarrollo interno de sistemas de información](#_Toc441659434)*** [9](#_Toc441659434)

***[3.3.](#_Toc441659435)******[Políticas para el desarrollo externo (“outsourcing”) de sistemas de información](#_Toc441659435)*** [9](#_Toc441659435)

***[3.4.](#_Toc441659436)******[Políticas sobre mantenimiento de sistemas de información](#_Toc441659436)*** [10](#_Toc441659436)

***[3.5.](#_Toc441659437)******[Política para el manejo de los estándares para el desarrollo y la documentación.](#_Toc441659437)*** [10](#_Toc441659437)

***[3.6.](#_Toc441659438)******[Política para el Análisis de requerimientos.](#_Toc441659438)*** [10](#_Toc441659438)

***[3.7.](#_Toc441659439)******[Política para la implementación de un nuevo sistema](#_Toc441659439)*** [11](#_Toc441659439)

**[4.](#_Toc441659440)****[Políticas relativas a bases de datos.](#_Toc441659440)** [11](#_Toc441659440)

***[4.1.](#_Toc441659441)******[Políticas para la creación de bases de datos](#_Toc441659441)*** [11](#_Toc441659441)

***[4.2.](#_Toc441659442)******[Políticas para la migración de información de bases de datos](#_Toc441659442)*** [12](#_Toc441659442)

***[4.3.](#_Toc441659443)******[Políticas sobre instalación de bases de datos](#_Toc441659443)*** [12](#_Toc441659443)

***[4.4.](#_Toc441659444)******[Políticas sobre administración y mantenimiento de bases de datos](#_Toc441659444)*** [12](#_Toc441659444)

***[4.5.](#_Toc441659445)******[Políticas de tiempos de almacenamiento de información en bases de datos](#_Toc441659445)*** [12](#_Toc441659445)

**[5.](#_Toc441659446)****[Políticas relativas a redes y telecomunicaciones](#_Toc441659446)** [13](#_Toc441659446)

***[5.1.](#_Toc441659447)******[Políticas para el uso de las redes de datos](#_Toc441659447)*** [13](#_Toc441659447)

**[6.](#_Toc441659448)****[Políticas relativas al servicio de Internet y correo electrónico](#_Toc441659448)** [14](#_Toc441659448)

***[6.1.](#_Toc441659449)******[Políticas para el acceso a servicios de Internet y correo electrónico](#_Toc441659449)*** [14](#_Toc441659449)

**[7.](#_Toc441659450)****[Políticas relativas al hardware](#_Toc441659450)** [16](#_Toc441659450)

***[7.1.](#_Toc441659451)******[Políticas de responsabilidad](#_Toc441659451)*** [16](#_Toc441659451)

***[7.2.](#_Toc441659452)******[Políticas de mantenimiento del hardware instalado](#_Toc441659452)*** [17](#_Toc441659452)

***[7.3.](#_Toc441659453)******[Políticas de resguardo de Activos informáticos](#_Toc441659453)*** [17](#_Toc441659453)

***[7.4.](#_Toc441659454)******[Políticas para el desecho de equipos electrónicos](#_Toc441659454)*** [17](#_Toc441659454)

**[8.](#_Toc441659455)****[Políticas relativas al software](#_Toc441659455)** [18](#_Toc441659455)

***[8.1.](#_Toc441659456)******[Políticas sobre el uso de licencias de software](#_Toc441659456)*** [18](#_Toc441659456)

***[8.2.](#_Toc441659457)******[Políticas para la instalación de Software](#_Toc441659457)*** [18](#_Toc441659457)

**[9.](#_Toc441659458)****[Políticas relativas a la seguridad](#_Toc441659458)** [19](#_Toc441659458)

***[9.1.](#_Toc441659459)******[Políticas generales de seguridad de acceso](#_Toc441659459)*** [19](#_Toc441659459)

***[9.2.](#_Toc441659460)******[Políticas de seguridad de acceso a sistemas operativos](#_Toc441659460)*** [21](#_Toc441659460)

***[9.3.](#_Toc441659461)******[Políticas de seguridad de acceso a sistemas de información](#_Toc441659461)*** [21](#_Toc441659461)

***[9.4.](#_Toc441659462)******[Políticas de seguridad de acceso a bases de datos](#_Toc441659462)*** [22](#_Toc441659462)

***[9.5.](#_Toc441659463)******[Políticas de seguridad de acceso a redes](#_Toc441659463)*** [22](#_Toc441659463)

***[9.6.](#_Toc441659464)******[Políticas de ubicación de los centros de procesamiento de información y comunicaciones](#_Toc441659464)*** [22](#_Toc441659464)

***[9.7.](#_Toc441659465)******[Políticas de ambiente de los centros de procesamiento de información y comunicaciones](#_Toc441659465)*** [23](#_Toc441659465)

***[9.8.](#_Toc441659466)******[Políticas sobre “ Responsabilidad de los usuarios al momento de usar los equipos informáticos”](#_Toc441659466)*** [23](#_Toc441659466)

***[9.9.](#_Toc441659565)******[Políticas relativas al cumplimiento de los procedimientos](#_Toc441659565)*** [24](#_Toc441659565)

# **Resumen**

El proceso de establecer políticas y procedimientos sobre controles generales y de aplicación en las tecnologías de información y comunicación, brinda una oportunidad de proveer un ambiente más estable y productivo a la comunidad de usuarios que utilizan los recursos informáticos.

Estas políticas y procedimientos son una directriz (o instrucción) que el usuario está obligado a seguir, cuando sea provisto de acceso a los recursos informáticos y a la red.

Es una práctica común para muchas entidades comerciales, gubernamentales o educativas hacer que sus usuarios firmen un acuerdo de cumplimiento de las políticas antes de proveérseles de una identificación de red. Las políticas son documentos que definen el uso que se dará a los recursos informáticos, de red, entre otros y establecer condiciones de conducta “en línea”.

# **Objetivos**

## ***Objetivo General***

Mantener la confiabilidad, disponibilidad e integridad de la información, así como facilitar el mejor aprovechamiento de los recursos informáticos y las telecomunicaciones, para alcanzar la misión institucional.

## ***Objetivos Específicos:***

* Utilizar los recursos tecnológicos de información y comunicación en forma responsable y apropiada, de conformidad con las disposiciones dadas en este manual y otras de carácter institucional.
* Minimizar las interrupciones de los servicios asociadas a los sistemas informáticos y comunicaciones, ocasionados por uso inapropiado o por daños causados en forma accidental o intencional.
* Adquirir tecnología acorde a las necesidades institucionales aprovechando al máximo las capacidades de los usuarios y el presupuesto asignado para esta materia.

# **Supervisión de las políticas**

La supervisión del cumplimiento de las “Políticas Generales sobre Tecnologías de Información”, queda a cargo de la Unidad de Informática; razón por la cual está facultada para verificar en cualquier momento el cumplimiento de estas políticas y de las normativas vigentes en materias de tecnologías de información y comunicación.

# **Violación a las políticas**

La infracción o incumplimiento de las políticas sobre tecnologías de información y comunicación, será notificado a la jefatura correspondiente a fin de que ésta proceda según corresponda. Este documento se estará revisando y/o actualizando por parte de la Unidad de Informática, con la finalidad de estarlo mejorando.

**Políticas para los servicios de tecnologías de información y comunicación**

# **Políticas Generales**

* 1. La Unidad de Informática, será una unidad administrativa funcionalmente independiente, que le permitirá la ejecución de procesos de planeación, coordinación, ejecución y supervisión estratégica de los proyectos e inversiones de tecnología de información a nivel institucional.
  2. Las políticas de tecnologías de información serán aprobadas por el COAMSS y divulgadas adecuadamente a través de la Unidad de Recursos Humanos. Estas políticas serán materia obligada en los procesos de inducción a los nuevos usuarios.
  3. Todos los usuarios de OPAMSS, deberán conocer los documentos de Políticas relativos a Tecnología de Información y regirse en su actuar por los principios consignados en ellos.
  4. La Unidad de Informática será responsable por la definición y ejecución de los presupuestos que OPAMSS asigne en materia de tecnología de información.
  5. Concienciar a todos los usuarios de OPAMSS, sobre su obligación de conocer y aplicar la normativa en materia de seguridad de TI para lograr un cambio favorable en la cultura organizacional.

# **Políticas Administrativas**

## ***Políticas para el planeamiento y administración de actividades***

* + 1. La Unidad de Informática contará con un Plan Operativo con el cual se orientarán las actividades.
    2. En los proyectos relacionados con desarrollo de aplicaciones, deberá aplicarse una metodología formal basada en los enfoques de ciclo de vida de sistemas y orientación a objetos mediante proceso unificado, para asegurar la adecuada administración y desarrollo.

## ***Políticas sobre los servicios que ofrece la Unidad de Informática***

* + 1. La Unidad de Informática creará un registro de los servicios que ofrece a toda la institución.
    2. Los servicios ofrecidos por la Unidad de Informática, se solicitarán formalmente y siguiendo los procedimientos que se emitan para ese fin.

## ***Políticas para el acceso físico la Unidad Informática y área de servidores***

* + 1. En general la oficina de la Unidad Informática es de acceso restringido, dadas las características del trabajo que se desarrolla en dicha área.
    2. Los usuarios de las diferentes áreas podrán ingresar a la unidad, para efectos de solicitar servicios o consultas.

## ***Políticas para la documentación y mantenimiento de manuales de la Unidad de Informática***

* + 1. Será política de la Unidad de Informática, documentar formalmente todas las actividades que realice en el desarrollo de los servicios que brinda a la Institución.
    2. La Unidad de Informática mantendrá un archivo de gestión de documentos, debidamente ordenado y clasificado para el registro de la documentación propia de la unidad. correspondencia y de actividades técnicas que desarrolla. Mantendrá, como mínimo, dentro de sus archivos de gestión, las siguientes documentaciones:
* Documentación de planeamiento estratégico de Tecnologías de Información.
* Documentación de planes anuales operativos.
* Documentación de inventario de equipos de cómputo, periféricos y de telecomunicaciones.
* Documentación de inventario de software instalado en equipos.
* Documentación del mantenimiento preventivo y correctivo de equipos de cómputo, periféricos y telecomunicaciones.
* Documentación de licencias de software adquiridos.
* Documentación de proyectos formalmente desarrollados.
  + 1. La Unidad de Informática tendrá en su archivo de gestión un compendio de manuales que contendrá como mínimo:
* Políticas y procedimientos sobre controles generales de las Tecnologías de Información y Comunicación. Estas incluyen las políticas y procedimientos sobre controles de Aplicación.
* Manual de uso aceptado de los Recursos Informáticos.
* Manual de contingencia para los Recursos Informáticos.
* Manual de respaldo de información.
* Manual de seguridad de los Recursos Informáticos.

## ***Políticas para la adquisición de nuevas tecnologías***

* + 1. Todos los procesos institucionales de adquisición de recursos informáticos, deben ser valorados y aprobados previamente por la Unidad de Informática.
    2. Para la adquisición de nuevos recursos de hardware, software y otros dispositivos tecnológicos, será política de la Unidad de Informática recomendar aquellos que ofrezcan calidad comprobada y sean referentes en el mercado nacional.
    3. Para el trámite de adquisición de nuevos recursos informáticos, la Unidad de Informática asesorará y apoyará a las diferentes áreas, en la definición de las características tecnológicas y evaluación de ofertas mediante recomendaciones técnicas.
    4. Para la adquisición de nuevos recursos, la Unidad de Informática se fundamentará en los reglamentos y normativas de compras definidos para la Institución o proyecto de cooperación según sea el caso.

.

## ***Políticas sobre inventario de equipo***

* + 1. La Unidad de Informática mantendrá un inventario de los equipos con las características de cada uno de ellos.
    2. La Unidad de Informática deberá revisar el inventario de los equipos por lo menos una vez al año, realizando los cambios que sean necesarios. Hará un informe a la Administración sobre las diferencias y/o deficiencias encontradas.

## ***Políticas sobre reparación de equipos***

* + 1. Todos los usuarios deben acatar el procedimiento que La Unidad de Informática implemente para controlar los servicios de reparación y la calidad de los mismos.
    2. La obtención de fondos presupuestarios para la adquisición de repuestos y accesorios será gestionada a través de La Unidad de Informática, quedando condicionado a la factibilidad presupuestaria.
    3. La Unidad de Informática tendrá un control de las garantías de los equipos adquiridos para hacer cumplir los compromisos contractuales. Los equipos no cubiertos procederán a ser reparados en las oficinas de OPAMSS. Podrá además ser enviado a talleres externos especializados y el costo será gestionado a través de la UACI, quedando también condicionado a la factibilidad presupuestaria.

# **Políticas relativas a sistemas de Información**

## ***Políticas generales para el desarrollo de sistemas de información***

* + 1. En general para el desarrollo de sistemas “in house” o “outsourcing”, todas las Unidades de OPAMSS, deben armonizar sus procedimientos de captura y registro de información. Se debe estudiar la justificación y evaluar la factibilidad para llevar acabo creación o modificación del sistema o nuevo proyecto.
    2. La Unidad de Informática, en colaboración con el/la analista de sistemas desarrollará y dará mantenimiento a los sistemas de información que la organización requiera, de acuerdo a los recursos humanos y tecnológicos que tenga a su disposición para este fin.
    3. La unidad de informática junto a la unidad que esta crea conveniente según el caso, debe homologar y fomentar la utilización de las herramientas de apoyo disponibles en la metodología aplicada y que cumpla con los requisitos mínimos exigibles por los controles institucionales.

## ***Políticas para el desarrollo interno de sistemas de información***

* + 1. El desarrollo de aplicaciones o sistemas se hará bajo el concepto de tecnología web.
    2. El desarrollo de sistemas de información se hará mediante proyectos debidamente formalizados, administrados y de acuerdo con la metodología y estándares.
    3. Las solicitudes de nuevos sistemas de información a desarrollar, deberán ser formalmente presentadas por las Jefaturas.
    4. Las solicitudes de cambios o nuevos requerimientos de sistemas deben ser formalmente firmados por la jefatura del área solicitante y contar con la aprobación de Dirección Ejecutiva o la Subdirección correspondiente, antes de realizar el análisis o cualquier diseño inicial.
    5. El proceso de desarrollo de sistemas debe contemplar las etapas de determinación de requerimientos, análisis del sistema, diseño del sistema, desarrollo de la programación, implementación, pruebas, puesta en producción.

## ***Políticas para el desarrollo externo (“outsourcing”) de sistemas de información***

* + 1. La Unidad de Informática podrá recurrir al desarrollo sistemas de información por “outsourcing”, cuando no cuente con el recurso humano y/o tecnológico necesario, para llevar a cabo los desarrollos de forma interna, además cuando otros factores como el tiempo no lo permitan.
    2. Las solicitudes de nuevos sistemas de información a desarrollar en la modalidad de “outsourcing”, deberán ser formalmente presentadas por las Jefaturas, en forma escrita e indicando en éstas los requerimientos generales por cubrir.
    3. El control y monitoreo del avance de proyectos de sistemas de información por “outsourcing” estará a cargo por el/la analista de sistemas.
    4. La Unidad de Informática estará pendiente que las empresas contratadas para el desarrollo de sistemas de información, brinden la capacitación a sus usuarios en administración, uso y mantenimiento del nuevo sistema de información.
    5. Los sistemas de información desarrollados por empresas externas, deberán ser entregados por éstas, de manera formal y debidamente documentados, incluyendo los entregables de documentación definidos por la Unidad de Informática en los términos de referencia.
    6. Los programas desarrollados o adquiridos externamente serán de uso exclusivo de OPAMSS, y no se permite el uso para funciones que no correspondan a las operaciones normales, excepto que exista algún convenio de cooperación con otras instituciones.

## ***Políticas sobre mantenimiento de sistemas de información***

* + 1. Será considerado como mantenimiento de sistemas de información todas las acciones que impliquen modificaciones, correcciones, mejoras o adiciones a los sistemas de información, que soliciten los usuarios de cualquier dependencia de OPAMSS debidamente autorizados por la jefatura respectiva.
    2. La Unidad de Informática definirá el procedimiento y las formalidades necesarias que orienten la forma en que serán desarrolladas las actividades de mantenimiento de sistemas de información.
    3. En caso de requerirse mantenimiento de sistemas de información tipo “outsourcing”, se aplica las mismas políticas anteriores “Políticas para el desarrollo externo (“outsourcing”) de sistemas de información”.

## ***Política para el manejo de los estándares para el desarrollo y la documentación.***

* + 1. La Unidad de Informática junto a la unidad que esta crea conveniente, se apegaran a una metodología estándar para el análisis y desarrollo de sistemas donde se definan los aspectos más importantes del ciclo de vida de desarrollo de sistemas y tecnología de información de la institución.
    2. Los estándares de análisis y desarrollo incluirán el estándar general para toda la documentación generada, incluyendo toda la documentación técnica (análisis, diseño, documentación de los programas, manuales de usuario).
    3. La Unidad de Informática junto a la unidad que esta crea conveniente, son responsables de dar a conocer y vigilar la correcta aplicación de la metodología estándar para el desarrollo de sistemas, por todas y cada una de las personas involucradas en el desarrollo de una aplicación.

## ***Política para el Análisis de requerimientos.***

* + 1. Para todo requerimiento autorizado debe desarrollarse un análisis de requerimientos cuyo fin debe ser establecer las especificaciones formales que describan las necesidades de información que deben ser cubiertas por el nuevo sistema.
    2. En la definición de los requerimientos deben participar los usuarios de todas las unidades a las que afecte el nuevo sistema.
    3. Una vez presentados los requisitos del nuevo sistema o la modificación solicitada, se deben definir las diferentes alternativas de construcción con sus ventajas e inconvenientes.

## ***Política para la implementación de un nuevo sistema***

* + 1. La Unidad de Informática debe contemplar un plan de instalación del sistema o modificación a liberar en el ambiente de producción.
    2. El plan de instalación del sistema debe ser definido desde las primeras etapas (análisis), con el fin de considerar todos los factores que influirán en la implementación.
    3. Se debe validar que el sistema desarrollado o la modificación realizada, cumple con los requisitos establecidos en la fase de análisis.
    4. El sistema desarrollado o la modificación realizada, debe ser aceptado formalmente por los usuarios antes de ser liberado a producción.
    5. El sistema desarrollado o la modificación realizada, se debe poner en producción formalmente y pasará a estar en mantenimiento sólo cuando haya sido aceptado y esté preparado todo el entorno en el que se ejecutará.
    6. Si existe un sistema anterior, el sistema nuevo se pondrá en producción de forma coordinada con la retirada del anterior, migrando los datos si es necesario.
    7. Los usuarios responsables deberán firmar un acta de aceptación del sistema y que éste cumple con los requisitos iniciales.

# **Políticas relativas a bases de datos.**

## ***Políticas para la creación de bases de datos***

* + 1. La Unidad de Informática en colaboración con el/la analista de sistemas, serán los encargados de diseñar física y lógicamente las bases de datos, que utilizarán los sistemas de información que se desarrollen internamente.
    2. La Unidad de Informática permitirá la creación de bases de datos a empresas contratadas para este fin o para el desarrollo de sistemas de información, siempre que se desarrollen según los estándares definidos en términos de referencia, y que entreguen la documentación técnica especificada en dicho documento.
    3. En la creación de nuevas bases de datos se deberá generar la documentación necesaria y suficiente, que permita comprender su estructura física y lógica, así como su contenido.

## ***Políticas para la migración de información de bases de datos***

* + 1. Toda migración de base de datos deberá ser realizada por personal técnico capacitado interno o personal externo, el cual deberá ser supervisado por un profesional de la Unidad de Informática.
    2. Antes de cualquier proceso de migración se deberán realizar los respaldos respectivos, así como realizar previamente una prueba de la migración en un servidor de pruebas, para garantizar que el proceso de migración funciona correctamente.
    3. En las actividades de migración de información a bases de datos, se deberá seguir el procedimiento definido por la Unidad de Informática para evitar atrasos y complicaciones, así como dejar documentado en una bitácora todo lo realizado para futuras migraciones.

## ***Políticas sobre instalación de bases de datos***

* + 1. Toda instalación de base de datos deberá ser realizada por el personal técnico capacitado, o en su defecto por personal de empresas contratadas para estos efectos, bajo la supervisión de la Unidad de Informática.
    2. Antes de cualquier instalación deberán realizarse los respaldos respectivos para evitar accidentes y garantizar la recuperación de la base de datos.
    3. Para la instalación de bases de datos se deberá seguir el procedimiento definido por la Unidad de Informática para prevenir que se den atrasos o complicaciones, así como dejar documentado en una bitácora todo lo realizado.

## ***Políticas sobre administración y mantenimiento de bases de datos***

* + 1. Todo mantenimiento a las bases de datos deberá ser realizado por personal técnico capacitado interno o externo, quienes deberán ser supervisados por el profesional responsable de esa tarea de la Unidad de Informática.
    2. Antes de cualquier proceso de mantenimiento a la base de datos, se deberán realizar los respaldos respectivos para estar prevenidos contra cualquier accidente que se pudiera presentar.
    3. Todo cambio o ajuste hecho en el proceso de mantenimiento, se deberá dejar documentado en una bitácora para efectos de control y seguimiento.

## ***Políticas de tiempos de almacenamiento de información en bases de datos***

* + 1. La Unidad de Informática deberá garantizar la conservación permanente de toda la información almacenada en las bases de datos de los servidores, que esté directa o indirectamente relacionada con las actividades de OPAMSS.
    2. La información deberá ser conservada durante el período que se defina en la tabla de plazos de conservación, labor en la cual tendrá concurso el SIM-CEIN.
    3. Todo acceso a las bases de datos del OPAMSS deberá contar con los mecanismos adecuados y controlados, que garanticen su seguridad, su integridad y la confidencialidad de la información almacenada.
    4. Toda transacción que se ejecute en las bases de datos, dejará las pistas adecuadas de auditoría, para poder ejercer un control adecuado, de todas las modificaciones que se hagan en éstas mediante el uso de bitácoras.
    5. Deberán de mantenerse y aplicarse sistemas de respaldos para todas las bases de datos de OPAMSS, con el fin de garantizar su conservación.
    6. Deberán existir planes de recuperación de la información de las bases de datos, para garantizar la continuidad del servicio que se presta por medio de los sistemas de información.

# **Políticas relativas a redes y telecomunicaciones**

## ***Políticas para el uso de las redes de datos***

* + 1. La Unidad de Informática será la dependencia responsable de la administración y uso de la red interna de datos.
    2. La Unidad de Informática garantizará el acceso controlado en la red interna de datos a los usuarios de OPAMSS que así lo requieran.
    3. Los usuarios accederán a la red de datos por medio de un código de acceso que les asignará el administrador de la red.
    4. El código de acceso a redes que se asigne será único y exclusivo para cada usuario, el cual será responsable por su uso.
    5. Todas las operaciones que se efectúen por medio de las redes internas serán responsabilidad única del usuario al que se le asignó el código relacionado con las mismas.
    6. La Unidad de Informática monitoreará periódicamente los accesos a la red interna mediante herramientas de seguridad y administración.
    7. No es permitido a ningún funcionario, excepto a los técnicos de redes, manipular los componentes activos de la red (switches, routers, dispositivos inalámbricos, cableado, etc.).
    8. No está permitida la conexión de equipos con nombres o direcciones no registrados.
    9. No se permite el empleo de mecanismos para la manipulación de direcciones de red o cualquier otro uso que pueda afectar a la topología o a la estructura lógica de la red.
    10. Los equipos electrónicos de gestión e infraestructura de la red de OPAMSS serán instalados, configurados y mantenidos exclusivamente por la Unidad de Informática.
    11. Ningún usuario está autorizado a utilizar analizadores del tráfico que circula por la red de OPAMSS. De igual manera está prohibido utilizar herramientas de rastreo de puertos o que permitan detectar vulnerabilidades. El uso de estas herramientas sólo está permitido a los administradores de la red y bajo situaciones especiales (incidentes de seguridad, denuncias de usuarios, etc.) que lo justifiquen.
    12. La Unidad de Informática pondrá en funcionamiento herramientas de control que posibiliten detectar, analizar y bloquear accesos no permitidos, (aquellos que no guarden relación con aspectos de trabajo) que pongan en riesgo la seguridad de los recursos informáticos y atenten contra su desempeño.

# **Políticas relativas al servicio de Internet y correo electrónico**

## ***Políticas para el acceso a servicios de Internet y correo electrónico***

* + 1. Los servicios de Internet y correo electrónico serán administrados por la Unidad de Informática.
    2. Para la comunicación oficial de OPAMSS debe utilizarse la cuenta de correo institucional, en la medida de las posibilidades.
    3. El acceso a los servicios de Internet y correo electrónico estarán disponibles para todos los usuarios de OPAMSS, si las condiciones de infraestructura tecnológica y administrativa lo permiten.
    4. El correo electrónico institucional es una herramienta de comunicación e intercambio oficial de información y no una herramienta de difusión indiscriminada de información.
    5. El uso de los servicios de Internet y correo electrónico deberá ser exclusivamente para apoyar y mejorar la calidad de las funciones administrativas y técnicas.
    6. La Unidad de Informática asignará las cuentas de correo de acuerdo a las licencias disponibles.
    7. Está prohibido facilitar u ofrecer las cuentas de correo a terceras personas.
    8. El servidor principal de correo electrónico debe mantener actualizada la herramienta de detección de virus para los correos entrantes y salientes.
    9. Se prohíbe a los empleados formar parte de cadenas de mensajes o SPAM, ya que esto contribuye a la saturación de las redes de telecomunicación y facilita la divulgación de su cuenta de correo y la proliferación de virus en la red.
    10. Se prohíbe a los usuarios que tengan acceso al servicio de correo electrónico abrir mensajes de procedencia desconocida.
    11. El funcionario que tenga acceso a servicios de correo electrónico debe evitar divulgar su cuenta a personas o entes desconocidos.
    12. Ningún equipo que esté designado como servidor debe tener asociada una cuenta de correo electrónica.
    13. Los mensajes de correo electrónico deben ser considerados como documentos formales y deben respetar todos los lineamientos referentes al uso inapropiado del lenguaje.
    14. Los usuarios deben realizar revisiones periódicas de los mensajes almacenados con el fin de no mantener información innecesaria.
    15. La Unidad de Recursos Humanos deberá notificar al Departamento de TI cuando se deba crear, cerrar o inhabilitar.
    16. El usuario debe atender a los avisos de actualización automática del programa de detección de virus e informar la Unidad de Informática, cuando la actualización no se realice satisfactoriamente.
    17. Los valores de seguridad, de aceptación de cookies y los certificados de los navegadores o browser no deberán ser cambiados, excepto por indicaciones de la Unidad de Informática.
    18. Para el envío de mensajes se aplicarán las siguientes reglas:
* Se utilizará siempre el campo de Asunto, a fin de resumir el tema del mensaje.
* No se enviarán mensajes a personas desconocidas, a menos que se trate de un asunto oficial que las involucre.
* No se enviarán mensajes a listas globales, a menos que el propietario sea la persona autorizada por el superior para enviar mensajes que involucren a toda la Institución.
* La divulgación de mensajes de interés general (actividades internas, invitaciones, notas luctuosas, entre otros) deberá coordinarse con la Unidad de Comunicaciones, la cual definirá el procedimiento para tal fin.
  + 1. Está prohibida la utilización abusiva del correo electrónico y de las listas de distribución incluyendo la realización de prácticas tales como:
* En caso de que fuera necesario un envío masivo se recomienda usar las listas de distribución o usar el campo de "copia oculta" (Bcc ó Cco) para poner la lista de destinatarios, o bien ponerse en contacto con la Unidad de Informática.
* Actividades comerciales privadas.
* Propagación de cartas encadenadas o participación en esquemas piramidales o actividades similares.
* El insulto, la amenaza o la difamación a cualquier persona.
* Suscribirse a periódicos, revistas, semanarios, buscadores de parejas, chats; ni a ningún otro tipo de actividades o boletines electrónicos que no sea el estrictamente relacionado con el área profesional de trabajo del funcionario.
* Descargar archivos de música, programas, videos, pornografía y cualquier otro tipo de información que no guarde estricta relación con el área profesional del funcionario. La Unidad de Informática procurará tomar las previsiones del caso para que se bloquee por medio de software especializado, el acceso no autorizado a los servicios antes mencionados.

# **Políticas relativas al hardware**

## ***Políticas de responsabilidad***

* + 1. El hardware que se encuentra en el área de servidores y los armarios de comunicaciones es responsabilidad directa del personal de la Unidad de Informática, que tendrá que velar por su uso y cuidado.
    2. Los otros equipos de cómputo quedan bajo la responsabilidad del usuario al que se asignen. Estos tendrán la obligación de cuidarlos, mantenerlos limpios y velar por su buen funcionamiento. En el caso de existir algún problema con el equipo deberán de reportarlo inmediatamente a la Unidad de Informática para que se proceda con su revisión.
    3. Los equipos portátiles (laptops, tabletas), serán asignados a los usuarios con el objetivo de cumplir sus funciones y no deberán utilizarlo para uso personal.
    4. Es responsabilidad del usuario custodiar los equipos portátiles asignados; por lo que deberá tomar las medidas de seguridad correspondiente dentro y fuera de la institución para evitar el robo del equipo o información. En caso de robo, deberá reportarlo inmediatamente al área de Administración y a la Unidad de Informática, además de realizar la respectiva denuncia a la autoridad policial respectiva.
    5. Queda entendido que los recursos informáticos asignados a cada usuario lo serán en calidad de herramienta de trabajo; como tal se encuentran permanentemente bajo dominio y control de OPAMSS, sin perjuicio del derecho a la privacidad de la información almacenada.
    6. Es responsabilidad de la Unidad de Informática hacer cumplir las garantías respectivas de cada uno de los equipos; para tal razón se deberán respetar los sellos de garantía que vienen adheridos a los equipos, y velar porque el usuario final no los despegue.
    7. Es responsabilidad de la Unidad de Informática valorar la necesidad de sustituir algún equipo cuando ya éste no garantice la funcionalidad y operatividad adecuada.

## ***Políticas de mantenimiento del hardware instalado***

* + 1. Los usuarios tienen el deber de informar sobre el rendimiento de cada equipo, para que sea valorado y de ser necesario mejorado.
    2. Las ampliaciones, modificaciones o adquisición de equipo de cómputo, así como la actualización y compra de software, se harán únicamente por recomendación de la Unidad Informática.
    3. En el caso de fallas técnicas del equipo de cómputo, la Unidad de Informática realizará un diagnóstico preliminar, con el objeto de procurar la solución, o en su defecto, girar las instrucciones del procedimiento a seguir para su reparación.
    4. Los equipos de cómputo no podrán ser desmantelados, cambiados, abiertos ni reparados por los usuarios de las oficinas. Asimismo, sus componentes (entiéndase “mouse”, disco duro, teclado, memoria, fuente de poder, tarjeta madre, entre otros) no podrán ser removidos por personal no autorizado.

## ***Políticas de resguardo de Activos informáticos***

* + 1. La Unidad de Informática llevará y mantendrá el inventario de los recursos informáticos así como el control de la ubicación de los equipos de cómputo en las dependencias de OPAMSS, así como de las licencias de uso del software adquirido.
    2. Los equipos de cómputo no podrán ser trasladados a otras oficinas que no sean las de OPAMSS, salvo para alguna situación específica siempre que se cuente con la debida autorización de la Dirección Ejecutiva, lo cual se hará del conocimiento de la Unidad de Informática y al área de Administración.

## ***Políticas para el desecho de equipos electrónicos***

* + 1. Los equipos electrónicos a ser desechados, será revisados por la Unidad de Informática, generando un acta de desecho la cual será entregada a la Administración como evidencia de su daño u obsolescencia para que proceda con el respetivo desecho.
    2. OPAMSS procurará la entrega de sus desechos tecnológicos a empresas recicladoras que cumplan con las normativas vigentes de protección al medio ambiente.

# **Políticas relativas al software**

## ***Políticas sobre el uso de licencias de software***

* + 1. La Unidad de Informática dará la asesoría necesaria a los usuarios de OPAMSS en el tema de licencias. Los usuarios deben asegurarse que disponen de las licencias adecuadas al uso que hagan del respectivo software, ya sea mediante licencias adquiridas de forma centralizada por OPAMSS (para software de uso común), por la adquisición individual de las correspondientes licencias, o bien por el uso de software libre. De no ser así, la responsabilidad recaerá totalmente sobre el usuario.
    2. La Unidad de Informática llevará un registro actualizado de los equipos y las licencias vigentes en OPAMSS para informar a las respectivas instancias.
    3. Se prohíbe la instalación de software propiedad de OPAMSS en equipos que no pertenezcan a la institución. En los casos de convenios de cooperación debe existir una cláusula que así lo permita.
    4. Se gestionará mediante presupuestos, la compra de licencias de “software” con la finalidad de que siempre en OPAMSS tengamos al día el uso de licencias.
    5. La Unidad de Informática removerá cualquier programa de las máquinas cuando no exista licencia. Se llevará un registro de los programas instalados ilegalmente, para que, ante la reincidencia de mantener programas instalados en forma ilegal, se proceda a reportar el asunto a la Unidad de Recursos Humanos o ante las autoridades superiores, para aplicar la sanción que corresponda por desobediencia según el Reglamento Interno de OPAMSS, lo cual debe tipificarse como falta grave. Para ello, la Unidad de Informática cuidará de no violentar el derecho a la privacidad de las personas, solicitando previamente la autorización al usuario para proceder con la remoción del programa ilegal.
    6. Los medios de instalación originales o acceso a los portales de descarga serán custodiados por la Unidad de Informática.

## ***Políticas para la instalación de Software***

* + 1. La Unidad de Informática es la responsable de la instalación de los programas de software en cada una de las computadoras de OPAMSS.
    2. Queda completamente prohibido que los usuarios realicen instalaciones de cualquier tipo de software en sus computadoras. De requerir un software específico debe solicitarse a la Unidad de Informática para que se valore la necesidad de su instalación.
    3. Todo software que se instale en las computadoras de OPAMSS deberá contar con su respectiva licencia y su instalación deberá ser autorizada por la jefatura de la Unidad de Informática.
    4. Queda prohibida la instalación del software adquirido por OPAMSS en equipos que no sean de su propiedad.
    5. El personal de la Unidad de Informática deberá mantener un inventario de software y programas instalados en cada una de las computadoras. Este inventario deberá revisarse y actualizarse una vez al año.
    6. Para la administración y el manejo seguro de la información que se almacena en los computadores de OPAMSS y para evitar su utilización por personas no autorizadas, se utilizarán los sistemas operativos que ofrezcan mayor seguridad.
    7. Conforme se adquieran nuevas versiones del Software, la Unidad de Informática realizara la respectiva instalación en los equipos de la institución.
    8. El software que debe residir en el disco duro de cada computadora y ser utilizado por los usuarios, es aquél que haya instalado la Unidad de Informática. En consecuencia, por ningún motivo los usuarios del OPAMSS, podrán instalar en los discos duros de las computadoras, ni utilizar por medio de discos compactos, llaves USB u otro medio, software no autorizado.
    9. En caso de que los usuarios requieran instalar, ejecutar, o copiar de Internet programas (software) diferentes al instalado en sus equipos, deberán coordinar previamente la Unidad de Informática. Lo anterior, con el fin de evitar riesgos legales o de funcionamiento de los equipos.

# **Políticas relativas a la seguridad**

## ***Políticas generales de seguridad de acceso***

* + 1. La Unidad de Informática es la responsable de la seguridad de acceso a los sistemas operativos, sistemas de información, bases de datos, y redes que operen en los equipos de cómputo de OPAMSS.
    2. La Unidad de Informática establecerá los mecanismos adecuados para el control, verificación y monitoreo de cambios en passwords, número de sesiones activas, seguridad lógica, física de todas las actividades relacionadas con el uso de tecnologías de información.
    3. Para evitar situaciones de peligro para OPAMSS, se desactivarán o bloquearán las cuentas de usuario a aquellas personas que estén en vacaciones, con permisos o incapacidades mayores a un mes, para lo cual debe informar la jefatura respectiva.
    4. En caso de despido de un funcionario, el permiso de acceso deberá desactivarse o bloquearse previamente a la notificación de la persona sobre la situación. La Unidad de Recursos Humanos deberá notificar al Departamento de TI cuando se deba crear, cerrar o inhabilitar los accesos a un funcionario.
    5. El administrador de los sistemas operativos, sistemas de información, bases de datos o redes asignará la clave de acceso al usuario.
    6. Las Jefaturas que esté a cargo de las diferentes unidades, son responsables de notificar por escrito a la Unidad de Informática sobre el ingreso, salida o traslado de un usuario a su cargo. Esto con el fin de que se creen, inhabiliten, modifiquen o eliminen los privilegios de acceso a las diferentes plataformas, dominios y dispositivos correspondientes.
    7. El encargado de seguridad informática no cambiará ninguna clave de acceso, si no es por solicitud expresa de su dueño. En caso de ser necesario y a solicitud de la jefatura se bloqueara los accesos de un usuario específico.
    8. Salvaguardar la confidencialidad de la clave de acceso (password) y abstenerse de facilitarla a terceros por cualquier motivo. Cada usuario será responsable de las acciones que se reporten ejecutadas con clave de acceso. En los casos de sustitución, se asignará al sustituto, un nombre de usuario y una clave de acceso transitoria y nunca la correspondiente a la persona sustituida.
    9. Cada usuario generará sus propias claves de acceso, cada cierto período de tiempo en la medida que las posibilidades técnicas que así lo permitan. Las conformará mediante el empleo de letras mayúsculas, minúsculas y números. El período lo establecerá la Unidad de Informática, dependiendo de la sensibilidad de la información.
    10. El usuario no debe dejar las claves de acceso escritas en medios o lugares donde puedan ser obtenidas por terceros (Ej.: monitor, carpetas, escritorio).
    11. Cuando el usuario olvide u extravié su clave de acceso, deberá acudir a la Unidad de Informática e identificarse como propietario de la cuenta para que se le proporcione una nueva.
    12. La clave de acceso nunca debe ser compartida o revelada; hacer esto responsabiliza al usuario que presto su clave de acceso todas las acciones que se realicen con la misma.
    13. La Unidad de Informática implementara estrategias para que se generen clases de acceso con niveles adecuados de seguridad.
    14. Los usuarios deberán aplicar medidas preventivas cuando se ausentan de las labores, antes de retirarse del lugar de trabajo donde se ubique el equipo de cómputo, el usuario deberá tomar las siguientes precauciones mínimas:
        - Concluir las sesiones activas de cualquier sistema informático al finalizar las tareas;
        - Proteger el equipo contra usos no autorizados mediante un mecanismo de bloqueo de seguridad autorizado por la Institución;
        - Cerrar la conexión con los servidores.
    15. Bajo ninguna circunstancia deberá compartirse la cuenta de usuario de Dominio o de computadora asignada por OPAMSS, ni la clave de acceso a dicha cuenta. Estas deberán manejarse conforme lo establezca la normativa interna de OPAMSS y el usuario a quien se le asigne será el único responsable del uso.
    16. Está prohibido el almacenamiento, la transmisión, transferencia y, difusión de datos de carácter personal en los equipos de OPAMSS, sin contar con autorización válidamente emitida por quien esté autorizado para ello.
    17. Los activos y recursos informáticos no deben conectarse a sistemas de cómputo ajenos a OPAMSS, a menos que sea estrictamente necesario para el cumplimiento de sus fines, en cuyo caso deben darse las siguientes condiciones:
        - Que se sigan los procedimientos de seguridad adecuados para proteger la información propiedad de OPAMSS o que esté bajo su custodia.
        - Que la conexión sea autorizada por la Unidad de Informática.

## ***Políticas de seguridad de acceso a sistemas operativos***

* + 1. La activación y desactivación de usuarios de dominio, estará a cargo del administrador de seguridad de la Unidad Informática.
    2. En la activación de usuarios de dominio, se crearán identificadores de usuario utilizando el estándar del primer nombre, seguido del primer apellido, ambos separados por un punto.
    3. Siempre que los sistemas operativos utilizados lo permitan, deberá controlarse el número de intentos de ingreso fallidos. Luego de 8 intentos, deberá bloquearse la cuenta del usuario y no permitir su ingreso al sistema. La cuenta debe estar bloqueada por 30 minutos y el administrador de seguridad podría desbloquearla antes por solicitud del usuario involucrado.
    4. En el caso que el sistema operativo lo permita, se deberán implementar las bitácoras de seguimiento a los accesos, donde se registren los ingresos al sistema y los intentos fallidos.

## ***Políticas de seguridad de acceso a sistemas de información***

* + 1. La activación y desactivación de usuarios de los sistemas de información estará a cargo del personal de la Unidad Informática.
    2. El administrador del sistema de información asignará la clave de acceso al usuario.
    3. Para otorgarle acceso a las diferentes aplicaciones, de acuerdo con las funciones que debe desempeñar el usuario, la jefatura correspondiente deberá hacer la solicitud formal al encargado de la Unidad Informática.
    4. En toda transacción que se realice en el sistema se deberá grabar el nombre del usuario, la fecha y la hora en que se realizó.

## ***Políticas de seguridad de acceso a bases de datos***

* + 1. La Unidad de Informática velará porque toda base de datos que sea instalada, cuente con los controles de seguridad que garanticen la confiabilidad de la información.
    2. El administrador de la base de datos asignará la clave de acceso al usuario.
    3. El sistema de seguridad deberá contemplar el bloqueo de claves luego de tres intentos fallidos de acceso, cuando la base de datos lo permita.
    4. La Unidad de Informática implementará controles para que todos los respaldos de información, se encuentren almacenados en medios externos como cintas de respaldo, CD´s o DVD´s.

## ***Políticas de seguridad de acceso a redes***

* + 1. El administrador de la Unidad Informática asignará las claves de acceso a los usuarios, además procederá conforme con la activación y desactivación de usuarios de las redes de OPAMSS.
    2. Para la utilización de las redes de datos, los nombres de usuario para las mismas se crearán siguiendo el esquema del dominio.
    3. Para otorgarle acceso a las redes de datos, de acuerdo con las funciones que debe desempeñar el usuario, la jefatura correspondiente deberá enviar la solicitud formal a la Unidad de Informática.

## ***Políticas de ubicación de los centros de procesamiento de información y comunicaciones***

* + 1. El centro de procesamiento de información y comunicaciones deberán estar ubicados dentro del edificio de OPAMSS, a menos que se disponga instalarlos en sitios externos especializados con la seguridad necesaria.
    2. El centro de procesamiento de información y comunicaciones debe estar completamente cerrados y con una única puerta de acceso, la cual deberá permanecer siempre cerrada. Las llaves de acceso estarán en custodia del personal de la Unidad Informática.
    3. Todo el cableado eléctrico que sea utilizado en los equipos de los centros de procesamiento de información y comunicaciones deberá ser totalmente independiente al cableado normal del edificio.
    4. Para efectos de cableado eléctrico y de datos se utilizarán las normas de cableado que se fundamenten en las mejores prácticas utilizadas en el mercado.

## ***Políticas de ambiente de los centros de procesamiento de información y comunicaciones***

* + 1. El área asignada para el centro de procesamiento de información y comunicaciones, debe estar dotado con las condiciones ambientales necesarias para garantizar un entorno físico conveniente para su funcionamiento.
    2. Este espacio del centro de procesamiento de información y comunicaciones deberá estar climatizado permanentemente a una temperatura que se encuentre entre los 18º y 21º para garantizar el mejor rendimiento de los componentes electrónicos y alargar la vida útil de los mismos.

## ***Políticas sobre “ Responsabilidad de los usuarios al momento de usar los equipos informáticos”***

* + 1. Los usuarios de OPAMSS usarán el equipo de cómputo en labores exclusivamente de trabajo y serán responsables por el uso adecuado de las herramientas tecnológicas.
    2. Los usuarios deberán abstenerse de utilizar los recursos informáticos de la institución para realizar actividades personales o con fines lucrativos. Los recursos asignados deberán ser utilizados únicamente para cumplir los objetivos organizacionales.
    3. No deberá consumir ni preparar alimentos en la mesa destinada para el computador, para evitar derrame de los mismos sobre los equipos, que pueden ocasionar trastornos en su operación.
    4. El costo por la reparación o sustitución de los equipos de cómputo a raíz de los desperfectos causados por situaciones de descuido en su uso, lo asumirá el usuario responsable, para lo cual se seguirá el respectivo procedimiento administrativo.
    5. Es prohibido a todos los usuarios de cualquier nivel, utilizar el equipo de la oficina para bajar de internet: juegos, música, videos, fotos, “screensavers” y todo archivo que provenga de fuentes no confiables; así como todo tipo de material pornográfico, que atenta contra el trabajo o el honor de las personas.
    6. Ningún usuario está autorizado para almacenar material pornográfico, u ofensivo en ningún medio de almacenamiento de las computadoras, dispositivos periféricos u otro dispositivo de almacenamiento, mucho menos propagarlo a otras personas.
    7. Los usuarios deben velar porque sus equipos tengan protección contra fallas de energía eléctrica o reducciones de voltaje. Para ello, deben instar a las jefaturas para que intercedan ante la Unidad de Informática a fin de proveer de estos dispositivos.
    8. Los usuarios deben utilizar antivirus actualizados para revisar todo medio antes de ingresarlo al equipo, con el propósito de evitar que éste sea contagiado al igual que la red institucional. Si no tienen instalado los antivirus tienen la responsabilidad de notificarlo a la Unidad de Informática.
    9. Los usuarios de equipos deben procurarse los conocimientos imprescindibles para el manejo de sus programas, así como realizar copias de seguridad de los datos que considere relevante en los recursos asignados del servidor, dicha medida puede resultar verdaderamente importante cuando los discos duros fallen de manera inesperada.
    10. Todo usuario es responsable de mantener respaldos de la información de acuerdo a sus necesidades en los recursos asignados del servidor. En caso de las aplicaciones el responsable por los respaldos es el administrador de Informática y si es del caso, el Administrador de la base de datos.
    11. Está prohibido conectarse a Internet utilizando equipos diferentes a los que oficialmente se encuentren en servicio.
    12. Las computadoras son propiedad de la institución y son asignadas a los usuarios para que desarrollen sus funciones en la institución, por tanto para efectos de OPAMSS, toda la información contenida en las mismas es de carácter público. En caso de requerirse por cualquier motivo acceder al equipo de un usuario, este no podrá alegar que la institución está violando su privacidad, por cuanto toda la información almacenada en los equipos es propiedad de OPAMSS; por tanto la información almacenada en las computadoras nunca puede ser de carácter privado.

## ***Políticas relativas al cumplimiento de los procedimientos***

* + 1. Todo usuario que reciba y tenga bajo su custodia bienes de OPAMSS, será responsable por el uso adecuado y el cuidado del equipo de cómputo asignado. Cualquier daño, pérdida, abuso o empleo ilegal que le sea imputable por falta al deber de cuidado, negligencia o dolo será responsabilidad del usuario principal y de las Jefaturas o encargados cuando se compruebe negligencia de su parte en su deber de control de los recursos informáticos asignados.
    2. Para una adecuada administración de los sistemas informáticos, y a fin de evitar intrusiones maliciosas, el personal de la Unidad Informática llevará a cabo revisiones periódicas en los equipos de cómputo, a fin de garantizar que se encuentran libres de códigos malignos, así como garantizar que los usuarios posean el software aprobado por OPAMSS. Dicha actividad se realizará en presencia del usuario encargado del equipo.
    3. Las jefaturas de cada unidad, serán las responsables de velar para que estas disposiciones se cumplan y reportarán a la Unidad de Informática cualquier inconveniente que se presente.
    4. La Unidad de Informática será el ente contralor de la administración de los recursos informáticos de OPAMSS.

**Cuadro de autorización**

|  |  |  |  |
| --- | --- | --- | --- |
| Fecha de Elaboración:  **26/01/2016** | Elaborado: | Revisado: | Autorizado: |
| **Ing. Jorge Barrera**  Administrador de Unidad Informática | **Ing. José Miguel Platero**  Jefe UFIA | **Arq. Yolanda Bichara**  Directora Ejecutiva |