MINISTERIO DE OBRAS PÚBLICAS,
TRANSPORTE, VIVIENDA
Y DESARROLLO URBANO

GOBIERNO DE
EL SALVADOR
UNÁMONOS PARA CRECER

POLITICAS INSTITUCIONALES EN MATERIA DE INFORMÁTICA.

GERENCIA DE INFORMARICA INSTITUCIONAL, JUNIO 2016

INDICE

CONSIDERANDO:

1. Que la Tecnología Informática es de vital importancia para el desarrollo de las actividades administrativas dentro del Ministerio de Obras Públicas, Transporte y de Vivienda y Desarrollo Urbano (MOPTVDU).
2. Que el uso de la Tecnología Informática por parte de los funcionarios y empleados del ministerio debe estar regulado a fin de facilitar la comunicación interna y externa, proteger información y proteger el equipo tecnológico existente.
3. Que las Normas Técnicas de Control Interno Específicas del Ministerio de Obras Públicas, Transporte y de Vivienda y Desarrollo Urbano, publicadas en el diario oficial número 58, tomo 394, de fecha 23 de marzo de 2012; en los artículos del 106 al 116, facultan a la Gerencia de Informática Institucional a definir políticas para el uso y administración de los recursos de tecnología de información del Ministerio, los cuales deben estar aprobados por el ministro.
4. Que con el fin de evitar el uso indebido de los equipos y herramientas informáticas, se hace necesario definir políticas que garanticen el buen uso de la tecnología informática.

POR TANTO:

El Ministerio de Obras Públicas, Transporte y de Vivienda y Desarrollo Urbano, a través de la Gerencia de Informática Institucional emite las POLITICAS INSTITUCIONALES EN MATERIA DE INFORMÁTICA.

POLITICAS INSTITUCIONALES EN MATERIA DE INFORMÁTICA

1.0 Objetivos

Aplicar normativa restrictiva sobre el uso de los Recursos Informáticos mediante controles en Administración, Procedimientos y Requerimientos para asegurar la protección adecuada a la información contenida en los Equipos Informáticos instalados en la Institución.

2.0 Alcance

Las políticas están orientadas a todos los empleados de la Institución, ubicados en las diferentes áreas que utilicen o tengan acceso a equipos informáticos de cualquier tipo o clase, conectados/a a red local mediante cualquier medio.

3.0 Políticas

Las políticas están orientadas a las áreas de acción bien definidas; las cuales se detallan a continuación: Políticas de Administración, sobre el uso de Internet, el uso de Correo Electrónico, Desarrollo de Aplicaciones Mecanizadas, de Prevención, Manejo y Contenido de Epidemias; y de Contingencias.

3.1 Políticas de Administración

La modernización del Estado requiere del uso eficiente de la tecnología y sabiendo que la información en el Sector Público es una herramienta estratégica para mejorar el desempeño y aprovechamiento de los recursos, así como para apoyar las acciones que se realicen para atender los retos de equidad y calidad de los servicios que proporciona el Ministerio de Obras Públicas, Transporte, y de Vivienda y Desarrollo Urbano.

La administración de recursos informáticos de la red del MOPTVDU es responsabilidad de la Gerencia de Informática Institucional (GII). Las funciones de administración incluyen la administración de los Servidores de Internet, Correo Electrónico, Bases de Datos propias del MOPTVDU, supervisión del tráfico de la red, la seguridad de accesos a la red y servicios, como Dominios, Active Directory, Servidores WINS, servidores DHCP, los Firewalls, Proxys y/o la instalación de nuevos enlaces; hardware de conectividad tales como Hubs, Routers, Switches, o analizadores de protocolos.

La GII puede quitar de la red y confiscar sin advertencia cualquier dispositivo sospechoso de violación de esta política.

3.1.1 Hardware

3.1.1.1 De la Adquisición de Equipo Informático

- La Gerencia de Informática Institucional velará para que el hardware de la institución este acorde al buen funcionamiento de los software que utilizan los empleados del MOPTVDU; para tal efecto, validara las especificaciones técnicas de los equipos para que la Institución cuente con dispositivos de tecnología que agilicen los procesos internos del MOPTVDU.
- Todo jefe de Unidad Organizacional que detecte necesidades específicas de adquisición de hardware, hará la consulta a la Gerencia de Informática Institucional para que a través de ésta se valide dicha necesidad y se hagan las consolidaciones de varias Unidades, si es el caso, y luego continuar con los procedimientos de compras establecidos por la GACI, según especificaciones técnicas validadas por la Gerencia de Informática Institucional.
- Todo hardware adquirido, independientemente del proceso utilizado (compra, donación o producto de transferencia de tecnología), deberá ser recibido por la Gerencia de informática Institucional acompañado de una

copia de Acta de Recepción emitida por la Unidad de Activo Fijo de la Gerencia Administrativa Institucional.

3.1.1.2 De la Instalación de Equipo Informático

- Todo el equipo informático (computadoras, accesorios, etc.), que esté o sea conectado a la Red de Datos del MOPTVDU, o aquel que en forma autónoma se tenga y que sea propiedad de la institución debe de sujetarse s lo establecido por esta Gerencia de Informática Institucional.
- La Gerencia de Informática solicitara a la Unidad encargada del control de Activos Fijos del MOPTVDU el registro de todos los equipos informáticos que sean propiedad del MOPTVDU.
- El equipo de la institución que sea de propósito específico y tenga una misión crítica asignada, requiere estar ubicado en un área que cumpla con los requerimientos de: seguridad física, condiciones ambientales, alimentación eléctrica y su acceso a la red de datos del MOPTVDU.
- La protección física de los equipos informáticos corresponde a quienes en un principio se les asigna, y corresponde notificar los movimientos en caso de que existan, a las autoridades correspondientes (Gerencia de Informática, Activos Fijos).
- Todos los Directores, Gerentes o Jefes de Área del MOPTVDU deberán notificar a la Gerencia de Informática Institucional el ingreso de cualquier equipo informático que no es propiedad del MOPTVDU y que va a estar siendo utilizado en la red de la Institución.

3.1.1.3 Del Mantenimiento de Equipo Informático

- Corresponde a la Gerencia de Informática Institucional, la realización del mantenimiento preventivo y correctivo de los equipos.

- En el caso de los equipos se les realice mantenimientos preventivos o correctivos por terceros, la coordinación al respecto será responsabilidad de la Gerencia de Informática.
- Se autorizará el mantenimiento preventivo y correctivo de bienes que sean propiedad del MOPTVDU.

3.1.1.4 De la Reubicación del Equipo Informático.

- Todos los Directores, Gerentes o Jefes de Área del MOPTVDU deberán solicitar a la Gerencia de Informática Institucional reubicación, reasignación, y todo aquello que implique ubicación de los equipos informáticos.
- En caso de existir movimientos (reasignación, traslado) de equipos de informática (computadoras, impresores, monitores, baterías de respaldo y otros), la Gerencia de Informática Institucional notificará a la unidad encargada del control de Activos Fijos del MOPTVDU los cambios realizados.
- El equipo de informática a reubicar o trasladar sea de cualquier Viceministerio, Dirección y Gerencia se hará únicamente bajo la autorización de la Gerencia de Informática Institucional.

3.1.1.5. Del control de accesos

I. Del Acceso a Áreas Críticas, bajo el control de la Gerencia de Informática

- La Gerencia de Informática deberá proveer de la infraestructura de seguridad requerida con base en los requerimientos específicos de cada área.
- El acceso de personal se llevará acabo de acuerdo a las normas y procedimientos que dicta la Gerencia de Informática Institucional.
- Bajo condiciones de emergencia o de situaciones de urgencia manifestadas, el acceso a las áreas de servicio crítico estará sujeto a las que especifiquen las autoridades superiores de la institución.

II. Del control de acceso al equipo informático.

- Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.
- Las áreas donde se tiene equipo de propósito general cuya misión es crítica estarán sujetas a los requerimientos que la Gerencia de Informática dicte.
- Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, la Gerencia de Informática Institucional tiene la facultad de acceder a cualquier equipo informático que no esté bajo su supervisión.

III. Del Control de Acceso Local a la Red.

- El Área de Soporte Técnico de la Gerencia de Informática es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.
- La Gerencia de Informática Institucional es la responsable de difundir las Políticas para el uso de la Red-MOP y de vigilar su cumplimiento.
- El acceso a equipo especializado de tecnología (servidores, enrutadores, bases de datos, Switch, Racks, etc.) conectado a la red es administrado por la Gerencia de Informática Institucional.
- Todo el equipo informático que esté conectado a la Red de Datos de Datos o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, debe de sujetarse a los procedimientos de acceso que emite la Gerencia de Informática Institucional.

IV. Del Control de Acceso Remoto.

- La Gerencia de Informática Institucional es la responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles.
- Para el caso especial de los recursos de accesos remotos a terceros deberán ser autorizados por el Ministro del MOPTVDU.
- El acceso remoto que realicen personas ajenas a la institución deberá cumplir las normas que emite la Gerencia de Informática Institucional.

V. De acceso a los Aplicaciones o Sistemas de Control Interno.

- Tendrá acceso a los sistemas o aplicativos de control solo el personal del MOPTVDU que cuente con un usuario y contraseña y que el Director, Gerente o Jefe haya autorizado.
- El manejo de información que se considere de uso restringido deberá ser instalada únicamente en usuarios autorizados por las autoridades superiores del MOPTVDU con el objeto de garantizar su integridad.
- La instalación y uso de los sistemas de información se rigen por las políticas y procedimientos establecidos por la Gerencia de Informática. Los servidores de bases de datos son dedicados, por lo que se prohíben los accesos de cualquiera, excepto para el personal del departamento de Informática autorizado por el Gerente de la misma unidad.
- El control de acceso a cada sistema de información (aplicación) será determinado por la unidad responsable de generar y procesar los datos involucrados.

3.1.2 Software

3.1.2.1. De la adquisición de software.

- La Gerencia de Informática Institucional propondrá los mecanismos para adquisición de programación con licencia.
- Del presupuesto que se le otorga a las diferentes áreas del MOPTDVU una cantidad deberá ser aplicada para la adquisición de software con licencia.
- Corresponderá a la Gerencia de Informática emitir las normas para el tipo de licenciamiento, cobertura, transferibilidad, certificación y vigencia.
- De acuerdo a los objetivos de la Gerencia de Informática deberá respaldar la adquisición y asesoramiento en cuanto a software de última versión.
- La Gerencia de Informática autorizará la instalación de software de dominio público que provenga de sitios oficiales y seguros.

3.1.2.2. De la instalación de software.

- Corresponde a la Gerencia de Informática a través del Área de Soporte Técnico emitir las normas y procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo.
- En los equipos tecnológicos únicamente se permitirá la instalación de software con licenciamiento apropiado y de acuerdo al cumplimiento de la ley de la propiedad intelectual.
- La Gerencia de Informática en coordinación con las Áreas de Soporte Técnico y de Desarrollo de Sistemas, serán las responsables de brindar asesoría y supervisión para la instalación de software informático.
- Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, actualización, parches de seguridad, privilegios de acceso, y otros que se apliquen).
  El software que desde el punto de vista de la Gerencia de Informática pudiera poner en riesgo los recursos de la institución, no será instalado en ningún equipo.
- La protección lógica de los sistemas corresponde a quienes en un principio se les asigna y les compete notificar cualquier inconsistencia a la Gerencia de Informática.

3.1.2.3. De la actualización del software.

- La adquisición y actualización de software para equipo especializado informático y de telecomunicaciones se llevará a cabo de acuerdo a programación propuesta por la Gerencia de Informática Institucional siempre que sea necesario.
- Corresponde a la Gerencia de Informática autorizar cualquier adquisición y actualización del software.
- Las actualizaciones del software de uso común o más generalizado se llevarán a cabo de acuerdo al plan de actualización desarrollado (si

existiere) por la Gerencia de Informática a través del Área de Soporte Técnico.

3.1.2.4. De la auditoria de software instalado.

- La Gerencia de Informática a través del Área de Soporte Técnico es la responsable de realizar revisiones periódicas para asegurar que sólo licencias autorizadas esté instalada en las computadoras de la institución.
- Corresponderá a la Gerencia de Informática, a través de la Área de Soporte Técnico, programar y notificar de las visitas para realizar la revisión a los equipos informáticos.

3.1.2.5. Del software propiedad de la institución.

- Todo software adquirido por la institución sea por compra, donación o cesión es propiedad de la institución y mantendrá los derechos que la ley de propiedad intelectual le confiera.
- La Gerencia de Informática en coordinación con la Unidad de Activos Fijos de la institución deberá tener un registro de todos los Software propiedad MOPTVDU.
- Todos los sistemas desarrollados o adquiridos a través de los recursos de la Gerencia de Informática, específicamente en el Área de Desarrollo de Sistemas, se mantendrán como propiedad de la institución respetando la propiedad intelectual del mismo.
- Los datos, las bases de datos, la información generada por el personal, que residen en los servidores de la GII deben estar resguardados en medios magnéticos y bajo la responsabilidad de la Gerencia de Informática Institucional.
- Corresponderá a la Gerencia de Informática promover y difundir los mecanismos de respaldo y salvaguarda de los datos, así como los sistemas desarrollados por la Área de Desarrollo de Sistemas.

3.1.2.6. Sobre el uso de software académico.

- Cualquier software que requiera ser instalado para trabajar sobre la Red deberá ser evaluado por la Gerencia de Informática Institucional.
- Todo el software propiedad de la institución deberá ser usado exclusivamente para asuntos relacionados con las actividades del Ministerio.

3.1.3 Infraestructura Física

La Gerencia de Informática Institucional en coordinación con la Gerencia Administrativa Institucional velaran porque la infraestructura se mantenga de acuerdo a las políticas siguientes:

- Los terremotos no pueden evitarse. El edificio debe de ser anti-sísmico; pero si fallase, debemos estar protegidos con las copias de respaldo guardadas en caja fuerte en lugares seguros.
- En las instalaciones de Informática deben existir extintores, instalados en las salas de Soporte Técnico y del cuarto de servidores.
- Se debe contar con control de temperatura en el cuarto de servidores, a fin de conocer con exactitud la temperatura del sitio para hacer las correcciones del caso.
- La limpieza debe ser diaria, evitando la papelería u otros artículos innecesarios.
- Se prohíbe fumar en las oficinas del Informática, a fin de prevenir un incendio. Deben existir detectores de humo en todas las instalaciones de Informática.
- Los equipos centrales de Informática dentro del centro de datos deben estar a una temperatura media de 15 a 23 grados centígrados con un sistema de aire acondicionado independiente e ininterrumpido.

El edificio de la GII debe de contar con un sistema de aire acondicionado central que mantenga las instalaciones de 18 a 25 grados.

- Todo el Sistema Eléctrico debe ser diseñado con el tipo de cable adecuado, centralizando todas las conexiones en un tablero de seguridad. Los cables eléctricos se ubican en las partes bajas, y los cables de señal de información serán aéreos.
- La corriente eléctrica que llega de las distribuidoras de electricidad nacionales, deben pasar por un transformador central y luego llegar al UPS, el cual deba de abastecer de energía a los servidores centrales de la Institución.
- Con el fin de tener instalada una buena polarización de todo el piso del cuarto de Servidores, que garantice una disminución de la estática en dicho lugar, se debe poseer una instalación metálica unida al polo a tierra de la red del edificio. Por encima de esta red se coloca el doble piso, el cual también sirve para ocultar todos los cables que unen los Sistemas Centrales con los usuarios.
- Para evitar riesgos de inundaciones, las instalaciones de Informática no deben estar ubicadas cerca de tuberías de agua ni los techos deben tener goteras. Contra las tormentas eléctricas, se debe contar con las instalaciones necesarias que protejan el equipo y el software de riesgos de rayos, cualquier descarga eléctrica o variaciones de voltajes.
- Las instalaciones que alberguen equipo de computación deberán estar correctamente polarizadas, y unidas entre sí para efecto de garantizar una red de polarización efectiva.
- El cuarto de servidores permanecerá constantemente cerrado, teniendo acceso solamente el Personal Autorizado por la Gerencia de Informática.
- El cuarto de servidores es el lugar más privado, el cual es controlado por el Administrador de Redes. Por norma, nadie debe entrar al mismo. Personal de Informática entrará únicamente para ayudar al Administrador en casos especiales. Se excluye de esta política a los titulares y al personal de

mantenimiento o servicio, siempre que sea para actividades propias de su cargo, con la supervisión del Gerente de Informática.

- La autorización para el acceso del personal al equipamiento de conectividad y a los servidores de datos debe ser gestionada ante el jefe del Área de Redes y Seguridad.
- Los usuarios no pueden acceder a ningún recurso informático hasta que sean debidamente autorizados.
- La autorización de acceso a los recursos es exclusiva del usuario al que le es asignada y no es transferible a otros usuarios o dispositivos.

3.1.4 Infraestructura Red de PC´s

Identificaciones de usuarios

- Todos los usuarios que acceden a recursos informáticos de la red requieren de una única e intransferible identidad, normalmente llamado "username" (nombre de usuario) para una persona, y un "hostname" (o nombre de máquina) para una computadora personal. Esta identidad se usa para representar un usuario o dispositivo en los ambientes informáticos de la red. La Gerencia de informática Institucional proporcionará este identificador como parte del proceso de autorización. Los identificadores concedidos expiran cuando la dependencia interviniente solicita expresamente a la Gerencia de Informática Institucional las cesaciones de acceso para dicho identificador de usuario, o cuando se compruebe un uso indebido. Será obligación de cada Gerente o Director/a informar la baja de los usuarios de su área que cesen en su función para que sea dado de baja el permiso de acceso existente.
- A menos que por otra parte se especifique explícitamente, el puerto de red autorizado de un dispositivo está incluido como la parte del mismo. La desconexión de un dispositivo de su puerto autorizado y conexión a otro

puerto de la red es una violación de este código. Laptops y computadoras móviles deben ser autorizadas para usar cualquier puerto de la red.

- El mal uso de la identidad de un usuario o un dispositivo constituye falsificación o falsedad. Las acciones que involucren accesos desautorizados, impropios o el mal uso de recursos informáticos de la red están sujetas a sanciones disciplinarias.

Las contraseñas

- Los usuarios tienen la responsabilidad de resguardar el acceso a los recursos informáticos con las contraseñas confidenciales que les fueron confiadas. Estas contraseñas deben construirse de manera que sean difíciles de suponer o adivinar por otros usuarios, deben expirar periódicamente y poseer una longitud mínima.
- Todas las acciones realizadas bajo los auspicios de un identificador de usuario y sus consecuencias legales son responsabilidad del usuario titular del identificador. Toda sospecha de vulnerabilidad en la seguridad debe ser notificada inmediatamente a la GII.
- Independientemente de las circunstancias, las contraseñas individuales de las cuentas de correo o de usuario de la red, no deberán compartirse o divulgarse a terceros sin la debida autorización de la Gerencia respectiva; efectuarlo supone responsabilidad por las acciones de terceros al usuario autorizado.
- Se deberán escoger contraseñas de un mínimo de seis caracteres y que sean difíciles de descifrar. No deberán ser palabras escogidas del diccionario, detalles personales o relacionados a la actividad que realiza.

3.1.5 Seguridad

- Toda la información que se encuentre contenida o circule en la red de computadoras de la Institución y que no ha sido específicamente identificada como propiedad de terceros, será tratada como parte de la información perteneciente al MOPTVDU. Esta política se aplicará para prohibir e/ acceso, divulgación, modificación, cambio, destrucción, perdida o abuso no autorizado de la información.
- Adicionalmente, es política de la Institución, proteger aquella información perteneciente a terceros y que haya sido confiada al MOPTVDU en cumplimiento a los convenios establecidos, si lo hubieran, y a los estándares de la Industria.
- La instalación y configuración de sistemas operativos, programas, aplicaciones y otras tareas administrativas de los equipos informáticos definidos en el alcance de la presente política, será realizado exclusivamente por personal técnico previamente autorizado para tal fin y de acuerdo a los estándares definidos por la GII. Para garantizar la uniformidad de las configuraciones, se elaborará la documentación de apoyo necesaria.
- La GII continuamente evalúa otros productos, para la sustitución de los actuales, y de ofrecer ventajas sobre lo instalado, gestionara los fondos para su adquisición.
- Con la puesta en marcha de estas directrices para la utilización del recurso informático, además de las medidas de protección a la red como Firewall y otros, se trata de garantizar la Integridad de la información y el rápido acceso a la misma, así como su disponibilidad por lo que la instalación de cualquier software adicional, deberá ser previamente autorizado. Debe resaltarse la frase **"cualquier software"**, ya que en Internet existen disponibles copias de software en versiones Shareware, Freeware o Trial (prueba por tiempo limitado) y de acuerdo a recientes advertencias de fabricantes de antivirus, algunos Hackers están incluyendo virus o troyanos que se instalan junto con el programa ofrecido, burlando de esta forma la seguridad del equipo.

3.2 Políticas de uso de Internet

Es política da la Institución, proporcionar acceso a la red local e Internet para optimizar la obtención de recursos e información necesarios para complementar el trabajo encomendado a los empleados autorizados. Por lo que el administrador de la red y los miembros del equipo de trabajo realizan monitoreo de seguridad y desempeño de la red, a partir de lo cual pueden establecerse restricciones o limitaciones a la utilización de estos privilegios.

Los usuarios deberán abstenerse de:

- Visitar sitios de Internet cuyo contenido sea ilegal, obsceno u ofensivo.
- Realizar instalaciones de accesos no autorizado, ya sea por Conmutación Telefónica (Dial-Up) o Conexión Dedicada (Red Lan), debido al riesgo implícito de intrusión o infección.
- Usar programas o aplicaciones potencialmente peligrosas para el rendimiento de la red, tales como uso inadecuado de servicios de mensajería instantánea pública (Messenger y variaciones), así como gestores de descarga Peer to Peer o basados en redes Gnutella (Ka zaan, Limew ire, Edonkay, etc.) debido al detrimento causado en la red.
- Subir (upload), Descargar (download), o transmitir software o cualquier material protegido por derechos de autor perteneciente a terceros o a la Institución sin previa autorización de la GII.

3.3 Políticas de uso de Correo Electrónico

- Como una herramienta de mejora a la productividad, la Institución impulsa la utilización del correo electrónico para la agilización de las comunicaciones. Todos los mensajes generados o conducidos por las

redes de comunicación, serán considerados propiedad del MOPTVDU y no propiedad de los usuarios de los servicios de comunicación.

- Si los usuarios necesitan compartir información de sus computadoras, pueden utilizar las ventajas de la mensajería electrónica supervisada, directorios públicos en las redes de área local y cualquier otro medio que haya sido previamente autorizado por la GII. Como una forma de prevención al acceso no autorizado de estos recursos compartidos.
- Los usuarios en general no deben interceptar o exponer, o ayudar a la interceptación o exposición de los mensajes electrónicos de la red Institucional. La GII a través del encargado de administrar de la Red de datos institucional, tiene claro el deber de respetar los derechos de privacidad de cada usuario.
- Se enfatiza que el usuario deberá evitar la distribución y propagación de mensajes no solicitados o envío de Archivos Anexos (Attachments) a un elevado número de destinatarios, lo cual sature el desempeño del Servidor de Correo.
- La cantidad máxima a transmitir de archivos adjuntos es de 10Mb. Se debe de utilizar una herramienta de compresión si el o los archivos son grandes, ejemplo: Winzip, freezip u otros que le proporcione la Gerencia de informática Institucional (GII). Considere usar la utilidad de anexar archivos, solo cuando sea necesario.
- Cada cuenta de correo es personal y cada empleado es el ÚNICO responsable de su cuenta.
- El envío de correo a un Grupo que incluya "Todos los usuarios del MOPTVDU", es de uso exclusivo de los Titulares del Despacho y Directores. Los mensajes que informan sobre virus, serán enviados solamente por la GII. Si le ha llegado o tiene alguna información al respecto informe a dicha Gerencia.
- Es prohibido utilizar los recursos de la Institución para enviar correos con material que ofende la moral y buenas costumbres o que esté fuera de los objetivos del MOPTVDU. Esto es considerado una falta grave, por lo que la

GII informará a Recursos Humanos para que haga la amonestación por escrito con copia a los titulares.

- Evite enviar o remitir correos de tipo "Cadena". Estos son los que piden reenviar a todos sus conocidos; ignórelo e infórmelo a la GII.
- Cuando se recibe correo de un desconocido y si contiene un anexo, no lo abra y elimínelo, ya que puede contener virus.
- Cree sus propios grupos de destinatarios frecuentes de correo, en su Libreta personal de Direcciones. Esto le hará más fácil el trabajo.
- Sea muy selectivo con los destinatarios de sus correos. No envíe mensajes "con copia" a personas innecesarias, ya que esto duplica la cantidad de mensajes y consumo de ancho de banda.
- De a sus mensajes un título claro (en el mismo campo "Asunto"). Esto permite al que lo recibe, hacerse una idea de lo que le llega, y evaluar si se desea abrirlo o no.

La Gerencia de Informática Institucional velara por el cumplimiento de estas disposiciones, y deberá informar a los titulares el mal uso que se haga de esta herramienta.

3.4 Políticas de Desarrollo de Aplicaciones Mecanizadas

- Todo nuevo desarrollo de sistemas será solicitado a la Gerencia de Informática Institucional y será su responsabilidad dar el seguimiento correspondiente a fin de satisfacer a la unidad solicitante.
- El Área de Desarrollo de Sistemas deberá priorizar el sistema que se va a desarrollar, de acuerdo a la importancia y necesidades de las unidades organizativas. La opción de tercerizar una aplicación o de desarrollarla internamente, será propuesta por la Gerencia de Informática. La unidad solicitante trabajara en la elaboración de los términos de referencia para ser enviados a la GACI; una vez se realice el contrato, será la unidad solicitante

la responsable de administrar la ejecución del proyecto, apoyada por la Gerencia de Informática Institucional.

- Todo nuevo desarrollo de sistemas a realizarse por el Área de Desarrollo de Sistemas, deberá contemplar los estándares establecidos, los cuales están descritos en el Anexo A.

3.5 Políticas de Contingencia

Con la finalidad de contar con alternativas de actuación ante situaciones imprevistas se dan las siguientes políticas:

- Establecer mecanismos de comunicación para contactar inmediatamente a cada miembro de la GII Debe disponerse de la direcciones de residencia, números telefónicos fijo y/o celular, correo electrónico, etc. Toda esta información debe ser compartida por las personas antes señaladas y por los titulares del Ministerio de Obras Públicas.
- Definir un área específica en una de las oficinas que pertenecen al MOPTVDU y que se encuentra fuera del Plantel La Lechuza (Ej.: VMT, etc), para que en caso de emergencia se pueda trasladar la Gerencia de Informática, rápidamente.
- Instalar una planta eléctrica que suministre energía a la GII, para ponerla en funcionamiento cuando las circunstancias lo demanden.
- Poseer en existencia repuestos básicos de funcionamiento de PC para atender necesidades urgentes.

4.0 SITIOS WEB

- Con el objetivo de tener sitios Web especializados para brindar a la ciudadanía y al mundo entero, un espacio informativo de las principales actividades realizadas, en proceso o por realizar del Ministerio de Obras Públicas, Transporte y Vivienda y Desarrollo Urbano, se establece como

política que en la Gerencia de Informática Institucional debe existir un servidor dedicado para esta misión.

- Debe existir un sitio Web principal de la institución cuya dirección sea *www.mop.gob.sv*, y un sitio Web para el Viceministerio de Transporte y otro para el Viceministerio de Vivienda y Desarrollo Urbano correspondientes a las direcciones *www.vmt.gob.sv* y *www.vivienda.gob.sv*.
- El diseño, desarrollo y mantenimiento de los sitios WEB corre a cargo del Webmaster, que pertenece a la Gerencia de Informática Institucional; La administración del contenido, es controlada por la Gerencia de Comunicaciones Institucional y las unidades de comunicaciones correspondientes a los viceministerios de Transporte y Vivienda y Desarrollo Urbano.
- Las funciones del Webmaster son las de establecer el "Arte" o presentación que lleva el sitio, así como la programación del comportamiento interactivo acorde a los "Estándares de Sitios Web Gubernamentales" de la Dirección de Innovación Tecnológica e Informática del Gobierno de El Salvador.
- La periodicidad con que se cambia dicho "arte", para evitar una monotonía visual, debe ser como mínimo seis meses y el contenido debe ser actualizado como mínimo cada semana.
- Para recopilar la información a ser actualizada, cada gerente de área debe nombrar a un responsable de su departamento y este enviarla a la Gerencia de Comunicaciones Institucional (GCI); la GCI debe depurarla información y darle el visto bueno, antes de ser enviada al Webmaster para su incorporación correspondiente en la sección adecuada de la página WEB.
- La gestión del contenido e interacción de las redes sociales es responsabilidad de la Gerencia de Comunicaciones Institucional, la Gerencia de Informática Institucional brindará la asesoría técnica en la gestión y uso de las diferentes redes sociales.
- El marco normativo para el uso de las redes sociales es la "Guía de los lineamientos y políticas para la gestión de información y mensajes difundidos a través de los medios sociales de las instituciones públicas de

Dirección de Innovación Tecnológica e Informática del Gobierno de El Salvador.

5.0 Responsabilidades Generales

Como se define a continuación, la Gerencia de Informática Institucional ha sido designada para establecer una línea clara de autoridad y responsabilidad.

Deberá verificar el cumplimiento de los estándares de seguridad proporcionados en este documento, incluyendo el hardware, software y respaldo de la información con los encargados de cada área. El respaldo de la información debe responder a procedimientos previamente establecidos por la Gerencia de Informática Institucional.

6.0 Sanciones

Todo empleado que tenga asignado o utilice equipo de computación deberá conocer las Políticas en Materia de Informática, por lo cual no existirá excusa para no cumplirlas, la GII dará un primer llamado de atención por vía escrita a aquellos usuarios de equipo que no respeten dichas políticas con copia al jefe inmediato superior; si esta condición persiste, se iniciara el procedimiento sancionatorio respectivo de acuerdo al Artículo No 41de la Ley del Servicio Civil o el Artículo N° 166 del Reglamento Interno del MOPTVDU, según corresponda.

7.0 Transitorio

Dicho documento entrará en vigencia a partir de la fecha de su autorización.

8.0 De las reformas al documento

Estas políticas serán anualmente revisadas y actualizadas.

9.0 De la divulgación

Las políticas serán divulgadas a todos los usuarios de la red por medio de la Intranet del Ministerio de Obras Públicas, Transporte y de Vivienda y Desarrollo Urbano.

San Salvador, a los treinta días del mes de Julio del año dos mil dieciséis.

Gerson Martínez
Ministro de Obras Públicas, Transporte
y de Vivienda y Desarrollo Urbano.

ANEXO A

ESTANDARES DE DESARROLLO DE APLICACIONES

A continuación se enuncia el software considerado como estándar en esta institución:

Área	Categoría	Software
Sistemas operativos	Servidor	Microsoft Windows Server
		Linux en las distribuciones: Debian, Ubuntu, RedHat, CentOS, OpenSuse y Suse Enterprise.
	Cliente	Microsoft Windows
		Mac OS
		Linux en las distribuciones Ubuntu, OpenSuse y CentOS.
Sistema de Administración de Bases de Datos	Servidor	Microsoft SQL Server
		MySQL
		Postgres
		Oracle
	Monousuario	Microsoft Access
		LibreOffice Base
Lenguajes de programación	Aplicaciones de consola	Microsoft C# / Visual Basic .NET
		Microsoft Visual Basic 6.0
	Aplicaciones de escritorio	Microsoft C# / Visual Basic .NET
		Microsoft Visual Basic 6.0
		Java
	Aplicaciones Web	Microsoft C# / Visual Basic .NET
		Java
		PHP
		Javascript
		HMTL
	Aplicaciones móviles	Microsoft C#
		Java
		Objetive - C
Entornos de Desarrollo Integrados	Microsoft C# y Visual Basic .Net	Visual Studio .NET
		Notepad++
		Sublime Text

	Java y PHP	Eclipse
		NetBeans
		Notepad++
		Sublime Text
Paquetes de Ofimática	Procesadores de texto	Microsoft Word
		LibreOffice Writer
	Hojas de cálculo	Microsoft Excel
		LibreOffice Calc
	Herramientas de presentación	Microsoft PowerPoint
		LibreOffice Impress
	Clientes de correo electrónico y agendas	Microsoft Outlook
		Mozilla Thunderbird
	Gestión de Proyectos	Microsoft Project
		ProjectLibre
	Navegadores Web	Microsoft Explorer
		Microsoft Spartan
		Google Chrome
		Mozilla Firefox
		Safari
	Utilitarios	Adobe Flash Player
		Adobe Reader
		PDF Creator
Diseño gráfico	Diseño Asistido por computadora	AutoCad
		Civil 3D
		IntelliCAD
	Diseño Gráfico en Mapas de Bits y Vectoriales	Adobe Photoshop
		Adobe Illustrador
		Adobe Fireworks
		Gimp
		InkScape
		Corel Draw
	Sistemas de Información Geográficos	ESRI ArcGIS
		ESRI ArcReader
		ESRI ArcView
		AutoCAD TrueViewer
		GVSIG
		Google Earth

Los casos de excepción deberán ser previamente autorizados por la Gerencia de Informática Institucional.

Por lo que cualquier otro software instalado en los equipos, ya sea procesador de textos, hoja de cálculo, manejadores de bases de datos, diseño gráfico, etc., reportados en el inventario de la institución, que no estén dentro de los estándares deberán ser justificados plenamente para proceder a su adquisición en el caso de no contar con la licencia de uso respectiva.

El desarrollo de sistemas por parte de la Gerencia de Informática Institucional, inicia cuando la Unidad solicitante llena una "Solicitud de Sistema" (ver formato, final del capítulo) la cual deberá ser enviada a La Gerencia de Informática, debidamente firmada y autorizada por el responsable del Viceministerio o Unidad Corporativa.

El desarrollo de un proyecto de sistemas de información contempla las siguientes etapas:

I. INVESTIGACIÓN

En esta área está considerado lo concerniente a la Especificación de los Requerimientos del Usuario, Análisis del problema y Plan de Desarrollo

Especificación de Requerimientos: Estos pueden ser generados por muchas razones, ya sea para obtener mejor velocidad de procesamiento, mayor exactitud y consistencia en los datos, consulta más rápida de información, integración de distintas áreas organizacionales, seguridad y reducción en los costos de operación. Cualquiera que sea la causa que lo origine, se deberá establecer con exactitud la clarificación del requerimiento, tomando en consideración su factibilidad técnica, operativa y económica. Las actividades a seguir son las siguientes:

Clarificación del Requerimiento:

a) Aclarar y entender la petición del proyecto:
   - Qué se está actualmente haciendo?
   - Qué se requiere?
b) Determinar el tamaño del proyecto:
   - Se trata de algo nuevo o algo que ya existe?
   - Cuánto tiempo se estima su elaboración?
   - Que cantidad de personas se involucraría en el proyecto?
c) Costos y beneficios estimados:
   - Costo estimado para el desarrollo
   - Costo de capacitación del personal
   - Se reducirán los costos de operación?
   - Se minimizará el costo de los errores?

Factibilidad Operativa:

Evaluar la existencia de apoyo total para el sistema por parte de la Unidad Solicitante para evitar la resistencia al cambio al realizarlo. Para esto se debe tomar en cuenta si el resultado final realmente mejorara el rendimiento de los usuarios; si los procedimientos actuales son obsoletos e inadecuados; prever que los resultados esperados del nuevo sistema realmente mejoraran la productividad, sin perder control sobre ninguna de las áreas existentes.

En esta evaluación debe de incorporarse directamente a los usuarios del requerimiento, ya que ellos son los garantes de la operatividad del mismo y responsables por los resultados obtenidos. Con esto no sólo se pretende dicha garantía, sino que la participación directa de ellos, los convierte en propietarios del mismo y su aporte será orientado al beneficio mismo de la agilización de sus funciones. Dicha integración de los usuarios se hará con la conformación de un

Comité de Desarrollo del Proyecto, conformado por el analista programador asignado al trabajo y de usuarios directos con pleno conocimiento y experticia en el campo sujeto a mecanizar.

Factibilidad Técnica:

Se debe evaluar, la existencia de los equipos necesarios y de la infraestructura tecnológica para su funcionamiento integrado, capacidad adquisitiva y recursos humanos disponibles y necesarios. Determinar el volumen de datos a almacenar para establecer los requerimientos mínimos de los equipos y prever su expansión o mejora en caso de incrementar dicho volumen; es decir, proyectar el sistema para que su ciclo de vida sea de mayor plazo posible. Proyectar los factores de cambio posible y el crecimiento tecnológico y de usuarios, a mediano plazo.

Factibilidad Económica:

Como su nombre lo indica, está relacionado a las finanzas y sobre todo a que los beneficios financieros deben igualar o exceder los costos del proyecto. Para esto debemos considerar los costos de la investigación, del nuevo hardware y licenciamiento de software necesario para la aplicación considerada, contra los beneficios en forma de reducción de costos operativos, costos por errores, sobretodo el costo de no realizar nada.

Producto final de esta etapa es:

a) Informe escrito de toda la investigación realizada contemplando los tópicos antes mencionados, con sus recomendaciones correspondientes.
b) Prioridad y tiempo estimado de desarrollo.
c) Presupuesto Estimado del proyecto
d) Requerimientos de Personal a utilizar

e) Plan de Trabajo para la siguiente etapa del Ciclo.

II. DISEÑO

En el caso del Ministerio, consideraremos en esta fase al Área de Desarrollo de Sistemas, terminando esta etapa con la elaboración de un Plan de Desarrollo.

Es en esta etapa donde, Si la factibilidad de desarrollo del sistema quedara en un grado de duda, habrá que plasmar el por qué? de la negativa y sus alternativas de acción, siendo estas el desistir, el subcontratar o comprar una aplicación existente.

Si se desiste de la elaboración, se debe explicar la(s) causa(s), ya sea(n) esta(s) técnica(s), operativa(s) o económica(s). Si se va a contratar la elaboración o a comprar un producto existente en el mercado, se deberá elaborar los Términos Técnicos correspondiente para ser enviados a la Unidad de Adquisiciones y Contrataciones, previo aval del Gerente de Informática.

Al determinar que el proyecto será desarrollado, será requisito del Analista Programador, el elaborar un documento conteniendo:

- La Definición del Proyecto a solventar
- Listado de Requerimientos
- Definición del Marco Normativo de la situación actual
- Diagrama de Flujo de la situación actual
- Alternativas de solución y recomendaciones correspondientes.
- Plan de trabajo de la etapa subsiguiente

En lo concerniente al Diseño, se definirá cómo el sistema deberá ser implementado, por lo tanto, esta fase se reviste de gran importancia para el apego del sistema final a los requerimientos y mejoras de la situación actual encontrada.

Producto final de esta etapa es:

- Descripción General (Propósito, Alcances, Objetivos, Marco Normativo, etc.)
- Diagrama de Flujo del Sistema Propuesto
- Diccionario de Datos
- Diagrama de Entidad – Relación
- Modelo Conceptual de la Base de Datos
- Reglas del Proceso
- Usuarios y Roles
- Programación de trabajo de la Siguiente etapa.

III. INGENIERIA

Consiste en la elaboración de todos los programas fuentes y procedimientos administrativos que demanda la nueva aplicación a mecanizar; también se realizan pruebas con participación activa de los usuarios, para que vayan adquiriendo la capacitación y la cultura informática, con el uso del sistema. Cualquier inconsistencia dejada en la etapa de diseño deberá ser tratada y solventada en esta etapa, en beneficio de la óptima funcionalidad de la aplicación.

Para ello, el Analista Programador asignado, deberá de elaborar la documentación correspondientes a:

Descripción del Desarrollo: donde el analista debe mencionar las reglas de programación a utilizar; El lenguaje de programación a usar, la nomenclatura de los programas y reglas de codificación aplicadas.

- Descripción Jerárquica y funcional de procesos

- Diseño de pantallas y/o formularios de Entrada de datos y Salida de Información
- Programación de Procesos
- Descripción y diagramas de procedimientos y formularios
- Establecer puntos de Control para auditar el sistema
- Detalle de la preparación de Data, para pruebas
- Requerimientos técnicos y humanos para efectuarlas
- Programación de la Etapa Siguiente.

Es en esta fase donde consideramos, a medida avanza el desarrollo, el ir efectuando pruebas de manera de aceptar los procesos desarrollados y ajustar aquellos donde la aplicación tiene sus deficiencias. Todos estos cambios o mejoras que en el camino se van elaborando, deberá irse actualizando la documentación correspondiente.

Producto final de esta etapa es:

- Programas de computador 100% finalizados.
- Capacitación a usuarios del sistema mecanizado.
- Documentación de los procedimientos a usar en el nuevo proceso

IV. IMPLEMENTACION

Al ser finalizado el desarrollo del proyecto y verificado a través de pruebas efectuadas en paralelo a su elaboración, el Sistema es alimentado rutinariamente con datos de la Unidad Solicitante y en un período que no exceda los quince días hábiles, el Responsable del Viceministerio o Unidad solicitante, deberá remitir una "Nota de Aceptación" o "Nota de Insatisfacción", al Gerente de Informática. En el primer caso, se da por "Oficialmente Instalado" el sistema.

En el segundo caso, deberá someterse a discusión las observaciones planteadas al "Comité de Desarrollo del Proyecto" y levantar un informe al respecto. Es responsabilidad del Coordinador de Proyectos, el darle seguimiento, tanto a la "Nota de Insatisfacción" como a las conclusiones emanadas del "Comité de Desarrollo del Proyecto".

Producto final de esta etapa es:

- Aplicación mecanizada en completo funcionamiento.
- Manual del usuario
- Manual del analista-programador

V. MANTENIMIENTO:

El Mantenimiento de los sistemas, es sujeto a requerimientos de mejoras solicitadas por los usuarios a través de formularios diseñados para tal fin (se anexa formulario "Solicitud Mejora a Sistema Existente").