



MINISTERIO
DE VIVIENDA

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El presente documento ha sido elaborado por la Unidad de Tecnologías de la Información, la revisión y validación de la información estuvo a cargo de los siguientes funcionarios:

Licda. Berthalia de Escobar
Directora Administrativa

Responsables de Formulación y Redacción:
Carlos Alberto Trigueros / Jefe UTI
Henry Osvaldo López / Coordinador UTI

Responsable de revisión
Arq. Alfredo Alfaro
Jefe Unidad de Desarrollo Institucional

SEPTIEMBRE DE 2021

Contenido

I. INTRODUCCIÓN.....	2
II. OBJETIVO GENERAL.....	2
III. OBJETIVOS ESPECIFICOS	2
IV. BASE LEGAL.....	2
V. POLÍTICAS.....	2
Políticas de Seguridad	2
Políticas de uso de Correo Electrónico.....	5
Políticas de Desarrollo de Aplicaciones Mecanizadas.....	6
Política de Gestión del Riesgo Informático	6
Políticas de Contingencia.....	7
SITIOS WEB.....	7
Responsabilidades Generales.....	8
Sanciones.....	8
De la divulgación	8
ANEXO A	9
ESTANDARES DE DESARROLLO DE APLICACIONES.....	9
I. INVESTIGACIÓN.....	11
II. DISEÑO.....	13
III. INGENIERIA.....	14
IV. IMPLEMENTACION	15
V. MANTENIMIENTO:.....	15

I. INTRODUCCIÓN

La modernización del estado requiere del uso eficiente de las tecnologías de la Información, considerando que la información en el Sector Público es una herramienta estratégica para mejorar el desempeño y utilización de los recursos, con la finalidad de cumplir los objetivos institucionales, así como también apoyar acciones que garanticen la calidad de los servicios que proporciona el Ministerio de Vivienda.

La administración de recursos informáticos de la red del MIVI es responsabilidad de la Unidad de Tecnologías de la Información (UTI). Asimismo, el desarrollo de normativas con el fin de preservar los sistemas y la información del Ministerio de Vivienda, garantizando la integridad, confiabilidad y disponibilidad de la información.

II. OBJETIVO GENERAL

Establecer Políticas y estándares generales para el uso adecuado de las tecnologías de Información a todo el personal del Ministerio de Vivienda, que garanticen la efectividad de utilización de los recursos informáticos asignados.

III. OBJETIVOS ESPECÍFICOS

Delimitar normas de tecnologías de la información relativas a la seguridad, usuarios, contraseñas, uso de internet y correo electrónico que se deben de respetar para contar con el acceso a la información, el dominio y los sistemas con que cuenta el Ministerio.

IV. BASE LEGAL

- Normas Técnicas de Control Interno Especificas del Ministerio de Vivienda, Art. 70, Políticas de Seguridad.

V. POLÍTICAS

Políticas de 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 Ministerio de Vivienda. Esta política se aplicará para prohibir el acceso, divulgación, modificación, cambio, destrucción, pérdida 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 Ministerio de Vivienda en cumplimiento a los convenios establecidos, si lo hubiera, 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 UTI. Para garantizar la uniformidad de las configuraciones, se elaborará la documentación de apoyo necesaria.
 - La UTI 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

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 Unidad de Tecnologías de la Información proporcionará este identificador como parte del proceso de autorización. Los identificadores concedidos expiran cuando la dependencia interviniente solicita expresamente a la Unidad de Tecnologías de la Información las cesaciones de acceso para dicho identificador de usuario, o cuando se compruebe un uso indebido. Será obligación de cada Gerente, Director y Jefe de unidad 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 UTI.
- 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 Dirección, Gerencia o Jefe de la Unidad 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.

Políticas de uso de Internet

- Es política de 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 autorizados, 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, Limewire, 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 UTI.

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 MIVI 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 UTI. 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 UTI a través del encargado de administrar 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 Unidad de Tecnologías de la Información (UTI). 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 MIVI”, se solicitara al Área de Redes, Seguridad y Soporte Técnico para su respectiva habilitación. Los mensajes que informan sobre virus, serán enviados solamente por la UTI. Si le ha llegado o tiene alguna información al respecto informe a dicha Unidad de Tecnologías de la Información.
- 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 MIVI. Esto es considerado una falta grave, por lo que la Unidad de Tecnologías de la Información 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 UTI.
- 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 Unidad de Tecnologías de la Información velará por el cumplimiento de estas disposiciones, y deberá informar a los titulares el mal uso que se haga de esta herramienta.

Políticas de Desarrollo de Aplicaciones Mecanizadas

Todo nuevo desarrollo de sistemas será solicitado a la Unidad de Tecnologías de la Información y será su responsabilidad dar el seguimiento correspondiente a fin de satisfacer a la unidad solicitante.

El Área de Desarrollo de Sistemas y Diseño Web, 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 Unidad de Tecnologías de la Información. La unidad solicitante trabajará en la elaboración de los términos de referencia para ser enviados a la Gerencia de Adquisiciones y Contrataciones Institucional (GACI); una vez se realice el contrato, será la unidad solicitante la responsable de administrar la ejecución del proyecto, apoyada por la Unidad de Tecnologías de la Información.

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

Política de Gestión del Riesgo Informático

La Alta Dirección y todo el recurso humano de la Unidad de Tecnologías de la Información del MIVI, gestionarán e implementarán acciones de control que le permitan la identificación, evaluación y administración de aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de los objetivos institucionales, con fines de fortalecer el sistema de control interno y la autoevaluación.

De esta forma, será responsabilidad de cada uno de los funcionarios y servidores públicos de la Unidad de Tecnologías de la Información, no sólo identificar los riesgos, sino también, realizar el seguimiento y control a los mismos, para que la gestión del riesgo sea efectiva, evitando o minimizando así las consecuencias negativas de su materialización y maximizando las oportunidades de mejoramiento.

Por tanto, la entidad se compromete a:

1. Realizar periódicamente actividades de difusión y sensibilización sobre la importancia de la gestión del riesgo Informáticos de la UTI.
2. Identificar y determinar los riesgos institucionales en materia de Tecnología, de forma tal que la gestión del riesgo se realice de manera consciente y objetiva.
3. Dar cumplimiento a las disposiciones en materia de identificación y control sobre los riesgos informáticos en la contratación y convenios que realiza la Institución.
4. Realizar evaluaciones periódicas de los procedimientos en uso para el control de los riesgos.
5. Monitorear cambio de entorno.

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 Unidad de Tecnologías de la Información debe disponerse de la dirección 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 Vivienda.
- Instalar una planta eléctrica que suministre energía a la UTI, como respaldo eléctrico y ponerla en funcionamiento cuando las circunstancias lo demanden.
- Poseer en existencia repuestos básicos de funcionamiento de PC para atender necesidades urgentes.

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 Vivienda, se establece como política que en la Unidad de Tecnologías de la Información debe existir un servidor dedicado para esta misión.
- Debe existir un sitio Web principal de la institución cuya dirección sea www.vivienda.gob.sv,
- El diseño, desarrollo y mantenimiento de los sitios WEB corre a cargo del Webmaster, que pertenece a la Unidad de Tecnologías de la Información; La administración del contenido, es controlada por la Unidad de Comunicaciones.
- 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 director, Gerente y Jefe de Unidad debe nombrar a un responsable y este deberá enviarla periódicamente a la Gerencia de Comunicaciones, Prensa y Protocolo; quien a criterio debe depurar la 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, Prensa y Protocolo; la Unidad de Tecnologías de la Información brindará la asesoría técnica en la gestión y uso de las diferentes redes sociales.
 - El marco normativo para el uso de las redes sociales deberá seguir los lineamientos y políticas para la gestión de información y mensajes difundidos a través de los medios sociales de las instituciones públicas, a partir de comunicación de Secretaria de Comunicaciones de la Presidencia y/o la Dirección de Innovación Tecnológica e Informática del Gobierno de El Salvador.

Responsabilidades Generales

Como se define a continuación, la Unidad de Tecnologías de la Información 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 Unidad de Tecnologías de la Información.

Sanciones

Todo empleado que tenga asignado o utilice equipo informático deberá conocer las Políticas en Materia de Informática, por lo cual no existirá excusa para no cumplirlas, la Unidad de Tecnologías de la Información 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, el caso será informado a la Dirección Administrativa y se iniciará el procedimiento sancionatorio respectivo de acuerdo a lo establecido en el Capítulo VII, Régimen Disciplinario, de la Ley del Servicio Civil, art. 41 y siguientes; así como a lo establecido en el Capítulo V, Régimen Disciplinario, del Reglamento Interno y de funcionamiento del Ministerio de Vivienda, art. 49 y siguientes, según corresponda.

De la divulgación

Las políticas serán divulgadas a todos los usuarios de la red del Ministerio de Vivienda, a través de los medios correspondiente.

ANEXO A

ESTÁNDARES 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	
		Objective - 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 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 Illustrator
		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 Unidad de Tecnologías de la Información.

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 Unidad de Tecnologías de la Información, inicia cuando la Unidad solicitante presenta nota de solicitud, la cual deberá ser enviada a la Unidad de Tecnologías de la Información, debidamente firmada y aprobada por el responsable de la Dirección, Gerencia o Unidad y con el visto bueno de la Dirección Administrativa del Ministerio de Vivienda

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?
 - ¿Qué 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, sobre todo 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 porqué 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 Gerencia de Adquisiciones y Contrataciones, previo aval del jefe de la Unidad de Tecnologías de la Información.

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 Siguiete etapa.

III. INGENIERÍA

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 correspondiente 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 Siguiete.

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. IMPLEMENTACIÓN

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 de la Unidad solicitante, deberá remitir una “Nota de Aceptación” o “Nota de Insatisfacción”, a la jefatura UTI. 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 de acuerdo al requerimiento administrativo correspondiente

Políticas de Seguridad de la Información

Para todo cambio que se deba realizar en las presentes políticas, será la Unidad de Tecnologías de la Información previa aprobación de la Dirección Administrativa, quien someterá a consideración del Titular de la institución las actualizaciones, modificaciones y/o anulaciones que cumplan con los procedimientos establecidos para dichos efectos.

El presente documento entra en vigencia a partir del mes de septiembre de 2021.



Licda. Irma Michelle Martha Ninnette Sol de Castro
Ministra de Vivienda Ad-Honorem

v