INSTITUTO SALVADOREÑO DEL SEGURO SOCIAL

MANUAL DE POLÍTICAS Y ESTÁNDARES

DIVISIÓN DESARROLLO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DGCI Julio de 2013

HOJA DE APROBACIÓN

Fecha de Elaboración: Julio de 2013

AUTORIZADO POR:

Ing. José Pedro Rivera
Jefe División Desarrollo de Tecnologías de la Información y Comunicación

Licda. Ana Beatriz Estrada de Carbajal
Jefe Unidad de Desarrollo Institucional

REVISADO POR:

POR:

Licda. Maritza García de Flores
Jefe Depto. Soporte Técnico a Usuario

Ing. Arnoldo Antonio Tejada Luna
Jefe Depto. Soluciones Integrales en Tecnologías de la Información y Comunicación

POR:

Ing. Ana Teresa Siu
Jefe Sección Control de Calidad

Inga. Alicia B. Azucena Martínez
Jefe de Sección
Desarrollo y Gestión de Procesos

Licda. Claudia María Campos
Jefe de Departamento
Gestión de Calidad Institucional

ELABORADO POR:

Ing. Williams Moto
Analista de Desarrollo Institucional

PERSONAL QUE PARTICIPA EN LA ACTUALIZACIÓN DEL DOCUMENTO

PARTICIPANTE	CARGO	Sección
Licda. Lorena Mendoza	Jefe de Sección	Implementación de Sistemas
Licda. Irma Elizabeth Ganuza Aguirre		Asistencia, Mantenimiento y Soporte Tecnológico
Ing. Agustín Guzmán		Análisis, Diseño, Desarrollo y Mantenimiento de Sistemas
Juan Carlos Cárcamo		Comunicaciones, Seguridad y Redes
Lic. Sergio Rivera		Administración de Bases de Datos y Sistemas Operativos
Ing. William Henríquez	Analista	Control de Calidad
Licda. Yolanda G. Sánchez		
Ing. Marco Ortiz		

REGISTRO DE ACTUALIZACIÓN DE DOCUMENTOS

VERSIÓN 0.0

CREACIÓN DEL DOCUMENTO:

Lic. Juan F. Argumedo	Ing. José Pedro Rivera	Lic. Juan F. Argumedo
Solicitado por	**Elaborado por**	**Aprobado por**
Agosto 2005	Agosto 2005	Agosto 2005

REGISTROS DE ACTUALIZACIONES:

Ing. Ricardo Avendaño	Lic. Ricardo Trujillo	Ing. Ricardo Avendaño	1.0
Solicitado por	**Elaborado por**	**Aprobado por**	**VERSIÓN**
Septiembre 08	Septiembre 08	Octubre 08	

Se agregaron las políticas siguientes:

- Inventario de Activos
- Adquisición de bienes informáticos
- Protector de Pantalla
- Seguridad Lógica
- Centros de Cómputo en Centros de Atención

Ing. Ana Teresa Siu	Licda. Claudia Campos de Mayen	Ing. Ana Teresa Siu	2.0
Solicitado por	**Elaborado por**	**Aprobado por**	**VERSIÓN**
Octubre 2010	Mayo 2011	Mayo 2011	

Se actualizo todo el Manual basado en mejores prácticas.

El día 09 de Septiembre de 2011 se realizaron las siguientes adendas al documento, debido a observaciones de Auditoria:

- Modificación de Política General # 8 (página 10).
- Modificación de Apartado 17. Seguridad en los Sistemas de Información, numeral 6 (página 62).
- Eliminación de Apartado 17. Seguridad en los Sistemas de Información, numeral 13 (página 62).
- Modificación de Apartado 17. Seguridad en los Sistemas de Información, nuevo numeral 13 (página 63).
- Adición de Apartado 17. Seguridad en los Sistemas de Información, numerales 15 y 16 (página 63).
- Modificación de página 64 debido a que desplazo el texto.

Ing. Ana Teresa Siu	Ing. Williams Moto	Ing. José Pedro Rivera	3.0
Solicitado por	**Elaborado por**	**Aprobado por**	**VERSIÓN**
Agosto 2012	Abril 2013	Julio 2013	

Actualización de los numerales detallados a continuación en base a requerimiento por observaciones de Auditoría Interna.

- Numeral 5. Control y Administración de los Recursos hasta el sub-numeral 5.6.
- Sub-numeral 5.8 Navegación en la Web.
- Sub-numeral 6.1 Servicio de Correo Electrónico Interno.
- Numeral 7. Adquisición de Bienes Informáticos.
- Numeral 8. Atención de Requerimientos.
- Numeral 10. Administración de Recursos Informáticos.
- Numeral 11. Ejecución y Traslado de Backups a la Bóveda de Seguridad Externa.
- Numeral 13. Implementación de Sistemas de Información.
- Sub-numeral 15.3, sección "C" política # 3 y 4.
- Sub-numeral 15.5 ampliación en política #1.
- Numeral 17. Seguridad en los Sistemas de Información, política # 6.

De acuerdo al surgimiento de la Sección Control de Calidad, se realizó el levantamiento de:

- Objetivos y políticas de la Sección Control de Calidad.

También se aplicó:

- Control de calidad a todo el documento.

Además, se realizó:

- Actualización general del documento con los nombres de las diferentes áreas según estructura organizativa.

CONTENIDO

CAPITULO I. GENERALIDADES DEL MANUAL DE POLÍTICAS Y ESTÁNDARES

1. INTRODUCCIÓN

En cumplimiento a las Normas Técnicas de Control Interno Específicas del ISSS; así como para lograr la mayor eficiencia en las complejas operaciones del ISSS, es preciso establecer políticas las cuales sean cumplidas por los responsables de su ejecución con la mayor fidelidad en todo momento.

Este Manual ha sido diseñado para ser un documento dinámico y como tal, deberá ser revisado para su actualización durante el desarrollo de la vida del Instituto. Las revisiones y actualizaciones podrán ser hechas a iniciativa de los Funcionarios del Instituto y deberán siempre conservar o mejorar la calidad, el control y la eficiencia de los procedimientos.

Debido a que este Manual será el patrón bajo el cual operarán las Dependencias del Instituto y contra el cual serán medidas en su eficiencia por las auditorias que se realicen, las revisiones y enmiendas del mismo serán permitidas solamente con la aprobación del Departamento Gestión de Calidad Institucional.

Todos los cambios o adiciones que se aprueben serán parte integrante del Manual y deberán ser incorporados a este documento en los mismos formatos del original. El Instituto tendrá así un Manual completo y permanentemente actualizado que servirá como base para sus operaciones.

2. USO Y ACTUALIZACIÓN

Este manual es de uso exclusivo del personal que labore en la División Desarrollo de Tecnologías de la Información y Comunicación y deberá hacerse del conocimiento de los Usuarios que laboran en la Institución por parte de la División Desarrollo de Tecnologías de la Información y Comunicación, únicamente las políticas que son responsabilidad de ellos implementarlas y dar seguimiento.

Las Jefaturas de la División Desarrollo de Tecnologías de la Información y Comunicación, deberán mantener en buenas condiciones y poner a disposición del personal un ejemplar del Manual para consulta y análisis del trabajo.

El personal de nuevo ingreso deberá estudiar el Manual como parte de su inducción y adiestramiento en el trabajo.

Las revisiones y enmiendas del mismo serán permitidas solamente una vez al año con la aprobación del Departamento de Gestión de Calidad Institucional (serán permitidas más de una vez al año siempre que exista un acuerdo de Dirección General que lo ampare), quien será responsable de documentar y distribuir los manuales actualizados a los tenedores del Manual, para ello existe un registro de actualizaciones donde aparece un apartado que muestra la creación del

documento y quienes participaron en la elaboración del mismo; así como las causas de la modificación.

3. OBJETIVO DEL MANUAL

El Manual de Políticas y Estándares ha sido diseñado para lograr los objetivos siguientes:

- Servir de guía al personal, brindando los lineamientos específicos para mantener una administración adecuada de los servicios prestados.

- Lograr la mayor eficiencia, calidad y control en las complejas operaciones del Instituto, ahorrando tiempo y esfuerzo en la ejecución del trabajo, al evitar la duplicidad de funciones dentro de los Procesos.

- Servir de guía al personal involucrado en la administración y control de los Procesos del Instituto.

4. MARCO LEGAL

NTCIE ISSS Mayo 2008.
CAPÍTULO III.
ACTIVIDADES DE CONTROL.
Documentación, actualización y divulgación de políticas y procedimientos.

Art. 48 al 51.
CAPÍTULO V.
NORMAS RELATIVAS AL MONITOREO.
Monitoreo sobre la marcha.
Art. 102.

ACUERDO DE DIRECCIÓN GENERAL Nº 2008-01-0026.
Oficialización y cumplimiento de los documentos normativos creados, modificados o actualizados por el Departamento de Desarrollo Institucional.

CAPITULO II. CONTENIDO DEL MANUAL DE POLÍTICAS Y ESTÁNDARES

1. INTRODUCCIÓN

Con el fin de homogenizar el uso de los servicios de cómputo y garantizar al mismo tiempo un adecuado esquema de operación que permita el flujo de información entre las diversas áreas del Instituto, la División Desarrollo de Tecnologías de la Información y Comunicación ha elaborado una serie de documentos, los cuales contienen políticas que habrán de ser de cumplimiento general en el uso de los equipos asignados a cada dependencia.

La difusión y verificación de la aplicación de las políticas plasmadas en los citados documentos, será responsabilidad de cada área ya que su cumplimiento redundará en el beneficio tanto para el área involucrada como para el Instituto, por que permitirán la optimización de la instalación, operación y mantenimiento de la infraestructura de cómputo.

2. OBJETIVO GENERAL

Poseer una herramienta que permita regular, normar y difundir el uso correcto, selección, aprovechamiento y mantenimiento de los equipos y servicios informáticos, así como promover y fomentar la estandarización, optimización y racionalización de los mismos.

3. POLÍTICAS INCLUIDAS

- Políticas y estándares de calidad.
- Control y administración de los recursos.
- Comunicaciones.
- Adquisición de bienes informáticos.
- Atención de requerimientos.
- Creación de usuarios para correo electrónico institucional.
- Administración de recursos informáticos.
- Ejecución y traslado de backups a la bóveda de seguridad externa.
- Procesamiento de órdenes de trabajo para ejecución de proceso, programa o impresión de listados.
- Implementación de sistemas de información.
- Política para clasificación de la información.

- Seguridad lógica.
- Centros de cómputo de centros de atención.
- Seguridad en los sistemas de información.
- Estándares para el diseño y desarrollo de bases de datos Oracle.
- Estándar Natural Adabas.
- Estándares Visual basics, Visual fox pro.
- Estándares utilizados para la entrega de software.
- Estándares del contenido de Manual de Usuario y Manual Técnico.
- Estándares de desarrollo SAP- ABAP.

4. POLÍTICAS GENERALES

1. Cuando por necesidades del Instituto se requiera la adecuación de las normas, políticas o procedimientos plasmados en el presente, ya sea por la modificación de éstos, por la asignación de más funciones o por disminución de las mismas, deberá solicitarse la intervención de la División Desarrollo de Tecnologías de la Información y Comunicación para su análisis y actualización.

2. El contenido de los manuales será de conocimiento a través de la División Desarrollo de Tecnologías de la Información y Comunicación, para el personal que labore en cualquiera de las Dependencias y que por las características de su trabajo utilice equipos de cómputo.

3. Cuando existan dudas en la interpretación de las políticas plasmadas en los manuales, la División Desarrollo de Tecnologías de la Información y Comunicación, aclarará las mismas.

4. Dadas las características físicas de los equipos de cómputo que serán instalados en el Instituto, así como las condiciones requeridas para su adecuada operación, es necesario observar las políticas que se enuncian con el fin de garantizar su máximo rendimiento.

5. Los datos registrados en los sistemas de información desarrollados internamente o adquiridos, son responsabilidad del usuario que los ingresa.

6. En caso de adquirir software elaborado por terceros, la División Desarrollo de Tecnologías de la Información y Comunicación emitirá opinión técnica sobre el

cumplimiento de las políticas incluidas en este manual para valorar la aceptación del software en conjunto con los usuarios.

7. Para SAFISSS, cuyo producto final es un sistema informático (creado por terceros) se adopta la metodología estándar de la herramienta para su implementación, puesta en marcha y sostenimiento del sistema, así como las políticas y estándares vigentes establecidos en este documento.

8. El modelo de ciclo de vida de desarrollo de sistemas tendrá como mínimo las fases de Análisis y Diseño, Desarrollo, Control de Calidad, Implementación y Mantenimiento. En el documento de Normas y Procedimientos se detallará los procesos asociados a cada una de las fases.

5. POLITICAS Y ESTANDARES DE CALIDAD

5.1 OBJETIVO GENERAL

Definir las políticas y estándares de calidad para la evaluación de los servicios y productos proporcionados por la División de Desarrollo de Tecnologías de la Información y Comunicación.

5.1.1 OBJETIVOS ESPECIFICOS

- Evaluar y monitorear el desarrollo, la implementación y puesta en marcha de los proyectos definidos en el plan de trabajo de la División de Desarrollo de Tecnologías de la Información y Comunicación. Así como aquellos proyectos designados por las autoridades del ISSS.

- Evaluar los mecanismos de control administrativo y operativos implementados en las diferentes áreas de la División de Desarrollo de Tecnologías de la Información y Comunicación, incluyendo las gestiones en los centros de atención donde hubiese un recurso asignado por la División de Desarrollo de Tecnologías de la Información y Comunicación.

- Evaluar el nivel de satisfacción de los usuarios que hacen uso de los servicios proporcionados por la División de Desarrollo de Tecnologías de la Información y Comunicación.

- Evaluar la aplicación de las políticas establecidas en el presente manual.

- Evaluar la infraestructura de TIC implementada y proyectada por la División de Desarrollo de Tecnologías de la Información y Comunicación.

5.2 POLITICAS:

1. El área de control de calidad deberá definir de forma anual un plan de trabajo, detallando las actividades a desarrollar con base a estándares de calidad. Dicho plan de trabajo podrá ser reprogramado de acuerdo a actividades o proyectos prioritarios no contemplados en dicho plan, o por instrucciones recibidas por las autoridades superiores.

2. El área de control de calidad realizará visitas a los diferentes centros de atención, para verificar la ejecución de los controles administrativos, operativos y técnicos; sin embargo, también se realizarán visitas cuando las circunstancias lo ameriten.

3. El área de control de calidad realizara visitas de seguimiento a las realizadas, con el propósito de verificar el cumplimiento de las recomendaciones suscitadas.

4. El área de control de calidad desarrollará actividades de acuerdo a la información o proyectos proporcionados por las diferentes secciones y departamentos de la División de Desarrollo de Tecnologías de la Información y Comunicación.

5. Cada área de la División de Desarrollo de Tecnologías de la Información y Comunicación deberá mantener sus propios controles internos de calidad hacia sus propios servicios o productos, independientemente de las actividades que desarrolle el área de Control de Calidad.

6. Todas las áreas de la División de Desarrollo de Tecnologías de la Información y Comunicación deberán proporcionar la información solicitada oportunamente por el área de control de calidad, para la ejecución de sus procedimientos.

7. Las áreas de la División de Desarrollo de Tecnologías de la Información y Comunicación no deberán proporcionar la información solicitada de forma limitada.

8. Las diferentes áreas de la División de Desarrollo de Tecnologías de la Información y Comunicación deberán proporcionar el apoyo solicitado por el área de control de calidad, a fin de proporcionar el acceso a los recursos informáticos necesarios para el desarrollo sus actividades.

9. El área de control de calidad no deberá revelar la información obtenida de las diferentes áreas de la División de Desarrollo de Tecnologías de la Información y Comunicación.

10. Los analistas de control de calidad deberá realizar un informe de las evaluaciones desarrolladas y presentarlo a su jefatura inmediata; sin embargo, no están autorizados para divulgarlo, a menos que la jefatura lo autorice.

11. Los analistas deberán recopilar la información a través de los formatos establecidos según la naturaleza de la actividad a desarrollar.

12. Los analistas no serán responsables de implementar las soluciones o ejecutar las recomendaciones como resultado de las evaluaciones realizadas.

6. CONTROL Y ADMINISTRACIÓN DE LOS RECURSOS

INTRODUCCIÓN

Con el propósito de lograr una adecuada administración de los recursos informáticos asignados a cada área, el presente apartado contiene las políticas a aplicar a efecto de evitar descontrol y pérdida de la información generada en las diversas áreas que integran la Institución.

6.1 ADMINISTRACIÓN DE COMPUTADORAS Y EQUIPO INFORMÁTICO

RESPONSABLES:	DEPENDENCIAS DEL ISSS

6.1.1 OBJETIVO

Contar con un método que permita utilizar, administrar adecuadamente y hacer más eficiente el uso de las computadoras y el equipo informático asignadas a cada área.

6.1.2 POLÍTICAS

1. Todas las computadoras personales deberán estar conectadas a algún servidor de red, a excepción de aquellas que por razones de uso específico, incompatibilidad, seguridad, distancia, falta de recursos, etc. no puedan ser conectadas.

2. La División Desarrollo de Tecnologías de la Información y Comunicaciones, realizará la instalación del equipo informático mediante solicitud de requerimiento de usuario o proporcionará la asesoría para efectuarla.

3. Bajo ninguna circunstancia los equipos de cómputo deberán estar conectados a tomas de corriente comunes, en estos casos deberán estar conectadas a un UPS el cual no deberá ser colocado a la par del CPU o monitor de la computadora para evitar daños por el campo magnético que éste emite. Salvo excepción, por situación de contingencia de aquellas áreas en donde no existan suficientes tomas de acuerdo a la demanda de equipos conectados y por razón de no contar con recursos suficientes para realizar las conexiones necesarias.

4. La administración del equipo será responsabilidad absoluta de la persona encargada del mismo.

5. Todas las computadoras personales deberán estar aseguradas con un protector de pantalla protegido por una contraseña.

6. La instalación de software deberá realizarse de acuerdo a lo expuesto en la política **"Licencia y software en los equipos**".

7. Seguridad y protección física mínima para el equipo informático que deben cumplir áreas usuarias que laboran en instalaciones físicas no protegidas son:

   - Bloquear el equipo de cómputo manualmente cuando el usuario deje de operar el equipo.
   - Contar con los cobertores del equipo informático y cubrirlo cuando se deje de utilizar.
   - Apagar el equipo de cómputo siempre que se deja de utilizar.
   - Contar con mobiliario adecuado y ergonómico para el usuario que a la vez proteja el equipo de riesgos de agua por estar ubicados al nivel del suelo y otros elementos dañinos.
   - Mantener el área limpia y ordena donde se encuentre el equipo de cómputo.
   - No colocar el equipo cerca de ventanas y unidades de aire acondicionado y otros elementos dañinos para el equipo.
   - Mantener las medidas de seguridad y protección del equipo informático es responsabilidad del usuario y jefatura de dependencia donde se encuentre ubicado el equipo.
   - Seguir las medidas establecidas en el capítulo **16.1** Políticas de Seguridad Física, de este mismo Manual.

6.2 DEPURACIÓN Y RESPALDO DE INFORMACIÓN

RESPONSABLES:	ADMINISTRADOR DE SISTEMAS INFORMÁTICOS

6.2.1 OBJETIVO

Establecer las medidas de seguridad, a efecto de proteger contra pérdida o daño la información contenida en los equipos personales o en servidores de archivos y/o aplicaciones, así como optimizar el espacio de almacenamiento en disco, realizando actividades de depuración de archivos no necesarios.

6.2.2 POLÍTICAS

1. Deberán llevarse a cabo actividades de respaldo de la información en medios de almacenamiento magnéticos (discos flexibles, tapes backups, discos duros externos, DVD, etc.) que permitan evitar pérdidas graves durante alguna contingencia.

2. Dependiendo de la frecuencia de uso y volumen de información introducida en los sistemas, se sugieren los siguientes calendarios para realización de respaldos:

FRECUENCIA DE USO	RESPALDO DIARIO	RESPALDO SEMANAL	RESPALDO MENSUAL	RESPALDO TRIMESTRAL
DIARIO	X	X	X	
DE GRAN VOLUMEN			X	X

   Los respaldos de los sistemas de misión crítica serán realizados por personal de la Sección Administración de Bases de Datos y Sistemas Operativos de la División Desarrollo de Tecnologías de la Información y Comunicaciones.

3. El equipo solo deberá almacenar permanentemente el software institucional, sistemas desarrollados por la División Desarrollo de Tecnologías de la Información y Comunicaciones, por la propia Dependencia, o adquiridos a terceros en forma autorizada y la información generada por éstos. Es responsabilidad del usuario al que se le ha asignado el equipo velar por el cumplimiento de esta norma.

4. La información generada por los paquetes de software de apoyo deberá ser respaldada en medios magnéticos y no es responsabilidad de la División Desarrollo de Tecnologías de la Información y Comunicaciones, sino de cada usuario individual.

5. En el caso de existir información compartida entre diversas áreas, el respaldo será responsabilidad de la dependencia propietaria de la información.

6. El Administrador de Sistemas Operativos deberá realizar periódicamente actividades de depuración de archivos en los equipos de almacenamiento o servidores del centro de cómputo del ISSS, eliminando aquellos que no sean de utilidad. Esta tarea también debe ser realizada por los Técnicos de Mantenimiento y Soporte Tecnológico, en los Servidores y Equipos de Almacenamiento asignados en su respectiva dependencia o los centros de atención a su cargo.

6.3 EQUIPOS DE COMPUTO PROPIEDAD DE LOS USUARIOS

RESPONSABLES:	DEPENDENCIAS DEL ISSS

6.3.1 OBJETIVO

Normar la permanencia de equipos de cómputo que sean propiedad de los usuarios dentro de las instalaciones del Instituto.

6.3.2 POLÍTICAS

1. Todo el equipo de cómputo y periféricos propiedad de los usuarios son responsabilidad de éstos, por lo que la Institución no se hace responsable por la pérdida o deterioro de alguno de estos.

2. Al ingresar a las instalaciones, el propietario deberá informar al personal de seguridad del ingreso o salida del equipo de acuerdo a las políticas de "**Entrada / Salida temporal de los Equipos**".

3. Bajo ningún motivo se le podrá instalar software institucional a estos equipos ni tampoco se les dará servicio de mantenimiento, reparación o refacciones con recursos del Instituto.

4. En los casos que se utilicen computadoras personales para apoyar funciones o actividades del área, por lo cual se necesite la instalación de software, se hará mediante notificación escrita autorizada por el Jefe del Departamento Desarrollo de Sistemas, quien, verificará la necesidad de instalación solicitada y aprobará o rechazará la solicitud para proceder a la instalación.

5. Por ningún motivo estos equipos podrán salir de las instalaciones de la Institución con hardware o software de ésta, en caso contrario las responsabilidades derivadas serán del usuario infractor.

6.4 ENTRADA / SALIDA TEMPORAL DE LOS EQUIPOS

RESPONSABLES:	DEPENDENCIAS DEL ISSS

6.4.1OBJETIVO

Definir los pasos necesarios para controlar la entrada y salida de equipo no propiedad de la institución y la salida temporal de equipo de cómputo y comunicaciones que sí pertenezcan al Instituto.

6.4.2 POLITICAS

1. En todos los casos deberá llenarse el formato de entrada/salida de equipos.(Ver anexo 1)

2. En todos los casos, la responsabilidad del cuidado del equipo que ingrese o salga temporalmente del Instituto, será del firmante del formato de entrada y salida de equipo.

3. Bajo ninguna circunstancia los equipos deberán ingresar o salir del Instituto sin el formato de entrada y salida de equipo.

6.5 MANEJO ADECUADO DEL EQUIPO

RESPONSABLES:	DEPENDENCIAS DEL ISSS

6.5.1 OBJETIVO

Indicar los cuidados indispensables que los empleados a quienes se les ha asignado el equipo deberán tenerse con este para evitar descomposturas por mal manejo o descuido y preservar su correcto funcionamiento.

6.5.2 POLITICAS

1. El equipo deberá encontrarse en un lugar ventilado, fresco y libre de humedad.

2. Deberá ser conectado únicamente al toma corriente instalado para tal efecto, y en la cual no deberán conectarse otros aparatos eléctricos.

3. Asegurar limpieza periódica del equipo con esponja, espuma limpiadora, aire comprimido y nunca utilizar solvente u otro tipo de líquidos a fin de evitar daños por manejo inadecuado del mismo.

4. No desconectar las estaciones de trabajo del toma de corriente ni del nodo de la red.

5. No consumir bebidas y alimentos en las cercanías del equipo (líquidos o sólidos).

6. No fumar en el área en donde se ubica el equipo, sobre todo en los servidores de archivos y equipo central.

7. No acercar aparatos eléctricos al equipo (ventiladores, radios, fotocopiadoras, fax, etc.).

8. No introducir grapas, clips, broches, pasadores, etc., en el interior del equipo.

9. No dejar encendido el equipo por períodos prolongados cuando no se esté utilizando.

10. En caso de falla no tratar de reparar el equipo y dar aviso de inmediato a la Sección de Asistencia, Mantenimiento y Soporte Tecnológico, de equipos de la División Desarrollo de Tecnologías de la Información y Comunicaciones.

6.6 LICENCIAS Y SOFTWARE EN LOS EQUIPOS

RESPONSABLES	DEPENDENCIAS DEL ISSS,

6.6.1 OBJETIVO

Que las áreas cuenten con el software estándar de la Institución, para facilitar el flujo de información entre los usuarios y controlar el uso e instalación de software, tanto en equipos personales como en servidores, evitando al mismo tiempo actos de piratería.

6.6.2 POLITICAS

1. Las instalaciones del software se harán a través del personal de la División Desarrollo de Tecnologías de la Información y Comunicaciones, mediante solicitud dirigida a la Sección Asistencia Mantenimiento y Soporte Tecnológico y presentada por el representante de informática en la dependencia o Jefe inmediato superior.

2. Cuando la Sección Asistencia Mantenimiento y Soporte Tecnológico preste licencias a personal de la División Desarrollo de Tecnologías de la Información y Comunicaciones, se deberá llevar control en la bitácora y solicitar las autorizaciones respectivas.

3. Cualquier instalación de software, aun cuando sea el utilizado en el Instituto, pero que no cuente con su licencia respectiva, será un acto de piratería por parte del usuario, por lo cual será responsable de cualquier consecuencia administrativa o legal.

4. La instalación de software no aprobado por la División Desarrollo de Tecnologías de la Información y Comunicaciones será responsabilidad del usuario que incurra en la falta, por lo que la pérdida de información, virus en el sistema o la red, faltas a la Ley de Derechos de Autor y cualquier otra resultante, será atribuible exclusivamente a éste.

5. Será responsabilidad del usuario, el uso y administración de Software que han adquirido sin el conocimiento y aprobación de la División Desarrollo de Tecnologías de la Información y Comunicaciones.

6.7 USO DE LA RED Y DOMINIO INSTITUCIONAL

RESPONSABLES	DEPENDENCIAS DEL ISSS

6.7.1 OBJETIVO

Transportar material que soporte la función laboral de Instituto Salvadoreño del Seguro Social, a través de la red de Comunicaciones e información.

6.7.2 POLITICAS

1. El uso de la red institucional por individuos u organizaciones que no sean parte del personal del Instituto, deberá ser solicitado por el jefe de la dependencia interesada, el acceso será de forma restringida y con los controles de seguridad adecuados. El jefe solicitante deberá especificar el tiempo necesario para accesar a la red.

2. Las políticas de uso aceptable de la red incluyen el uso de la red de comunicación con el objetivo de apoyar actividades administrativas y de salud asociadas con las actividades laborales y de investigación de la Institución, así como para la comunicación con instituciones o empresas privadas y de gobierno relacionadas, siempre y cuando estén vinculadas con las tareas encomendadas institucionalmente. Se excluye la interacción social, exceptuando aquellos casos en los que por la naturaleza de su trabajo requieran este acceso. La responsabilidad del buen uso de este servicio y que su uso no interfiera con los objetivos del ISSS es responsabilidad de la jefatura que solicita y avala su configuración.

3. El uso de la red de comunicaciones del ISSS para actividades lucrativas no relacionadas con las actividades normales de la Institución no está permitido.

4. La Institución no permite la transferencia de claves o Números de Identificación Personal (PIN) o cualquier otra metodología de seguridad, entre cualesquiera individuos. Tal acción es considerada inaceptable y será sujeta a acción disciplinaria.

5. Al momento de la terminación de su contrato de empleo por cualquier razón que fuere, las cuentas y todos los datos encontrados en ella de un empleado, serán removidos de los servidores del Centro de Cómputo del ISSS, así como del software que las administra. Además, los Administradores de Red deben eliminar la información respectiva de todas las instalaciones de la Institución dónde les compete. Con este propósito todo retiro o cesación de relación laboral deberá ser notificado oportunamente a la División Desarrollo de Tecnologías de la Información y Comunicación y al Administrador de Red local por parte del Jefe inmediato superior del empleado en cuestión.

6. Las cuentas y los datos de usuarios podrán ser utilizados por personal autorizado para ello.

7. A ningún miembro de la Institución, le será permitido interceptar, leer, copiar o modificar datos electrónicos privados (ya sea en tránsito a través de la red o almacenados dentro de una computadora) sin el consentimiento escrito del propietario legítimo.

8. Las facilidades de redes de la Institución no pueden ser usadas por ningún individuo o grupos de personas para ninguna actividad de naturaleza ilegal o fraudulenta, incluyendo actividades ilegales como las definidas por las leyes locales, estatales e internacionales, así como las políticas, códigos y regulaciones de la industria.

9. Cualquier actividad que se sospeche ilegal o fraudulenta debe ser inmediatamente reportada a la autoridad competente, jefe de la División Desarrollo de Tecnologías de la Información y Comunicación o al Técnico de Mantenimiento y Soporte Tecnológico los centros de atención que lo posean), para que tome las acciones respectivas.

10. En casos que involucren alegada actividad fraudulenta, la Institución puede, a discreción del jefe de la División Desarrollo de Tecnologías de la Información y Comunicación, suspender los privilegios de acceso en espera de los procedimientos legales.

11. La ruptura de estas Políticas de Uso Aceptable y Acceso, que no involucren actividad fraudulenta o ilegal, serán referidas al jefe inmediato superior para su consideración.

12. La vigencia de la Clave de Acceso es de tiempo limitado, recordándole con un máximo de 15 días y un mínimo de 7 sobre su caducidad, dicha Clave de Acceso no podrá ser igual a cierta cantidad de Claves anteriores y debe cumplir con las características de longitud y complejidad (todos estos requisitos serán definidos por la División Desarrollo de Tecnologías de la Información y Comunicación). El recordatorio automático de forma anticipada del vencimiento de clave de acceso no aplica para SAFISSS.

13. El Usuario no deberá utilizar Claves de Acceso que estén asociadas a datos comunes del usuario, tales como la fecha de nacimiento, apelativos, nombres de familiares, etc.

14. Las carpetas compartidas deberán estar delimitadas para ser accesadas solo para el personal que hará uso de ellos, el cual será definido por la jefatura del área solicitante.

15. No se permite el uso de los recursos informáticos para los siguientes actividades:

    - Para la exhibición de material pornográfico en cualquier lugar de la Institución utilizando el equipo de cómputo y/o los servicios de comunicación institucionales.

    - Provocar deliberadamente el mal funcionamiento de computadoras, estaciones o terminales, periféricos de computadoras y periféricos de redes y/o sistemas.

    - Utilizar los servicios de comunicación para intimidar, insultar o acosar a otras personas e interferir con el trabajo.

    - Cualquier actividad ilegal, indecorosa o que dañe a terceros.

16. A los usuarios que quebranten estas políticas y reglamentos de uso y acceso, les será eliminado el acceso a las redes de comunicación y computadoras de la Institución. La violación de esta política de uso es considerada una violación de los reglamentos de la Institución.

6.8 NAVEGACIÓN EN LA WEB

RESPONSABLES:	DEPENDENCIAS DEL ISSS

6.8.1 INTRODUCCIÓN

Todo empleado que haga uso de Internet en todas las dependencias del ISSS, se regirá y aceptará cumplir con los términos y condiciones establecidas en las políticas institucionales, así como las leyes aplicables nacionales e internacionales.

La División Desarrollo de Tecnologías de la Información y Comunicación tiene como meta promover un uso adecuado de Internet y vigilar el cumplimiento del mismo.

Cualquier usuario que utilice Internet y viole esta política y cualquier norma de la Institución, estará sujeto a la suspensión del servicio y a cualquier otra acción disciplinaria que la administración determine.

6.8.2 OBJETIVOS

- Regular el servicio de Internet ofrecido por el Instituto según la definición de los términos, condiciones y responsabilidades que gobiernen el uso de este servicio a través de las computadoras y dispositivos móviles por parte de los usuarios de la Institución en todas sus dependencias.

- Proporcionar el servicio de Internet para el apoyo en la realización de las labores diarias e investigación, cualquier uso inadecuado de estos servicios que interfiera con la imagen de la Institución, autoridades y empleados será considerado una violación a esta política y estará sujeto a las sanciones correspondientes.

6.8.3 ALCANCE

Esta política aplica a todos los usuarios que utilizan la red institucional a través computadoras y dispositivos móviles para la realización de las labores diarias.

ASIGNACIÓN DE DERECHOS DE ACCESO (PRIVILEGIOS)

Los privilegios de uso de Internet estarán limitados por la necesidad de acceso que requiera el desarrollo de las labores diarias de cada usuario.

Las solicitudes de uso de Internet y los cambios de privilegios de acceso se deben presentar por escrito a la División Desarrollo de Tecnologías de la Información y Comunicación con la aprobación y justificación del jefe del área a la que pertenezca el usuario, siendo responsabilidad del jefe del área y del usuario al que se asignaron los privilegios la mala utilización del servicio de Internet.

Se podrán otorgar derechos de acceso a personas ajenas al ISSS, siempre y cuando la solicitud haya sido aprobada por el jefe del área o responsable de la dependencia en la cual trabajaran. Estos derechos tendrán una vigencia no mayor a 30 días, pero podrán ser extendidos, previa solicitud del jefe del área o responsable de dependencia respectivo.

La utilización del servicio de Internet por parte de los usuarios constituye una aceptación de las políticas de uso de Internet vigentes, la cual está disponible en el Portal Institucional.

6.8.5 POLÍTICAS

La Institución provee acceso a Internet a los empleados para asistirlos en el curso normal de sus funciones, al hacer uso de Internet el usuario acepta cumplir con lo siguiente:

1. Utilizar Internet apropiadamente de acuerdo a lo establecido en esta política.

2. Es responsabilidad del usuario verificar que la información que accede en la Internet es exacta, completa y actual.

3. Respetar las protecciones legales de los datos y software proporcionados por los derechos de autor y licencias respectivos.

4. Informar inmediatamente a la División Desarrollo de Tecnologías de la Información y Comunicación a través de los números telefónicos 2268-3166, 2268-3418 o correo electrónico seguridad.tic@isss.gob.sv, sobre cualquier situación inusual que suceda en el uso de este servicio.

5. La División Desarrollo de Tecnologías de la Información y Comunicación definirá las categorías a las que los usuarios tendrán permitido visitar basado en las mejores prácticas aplicadas por los filtros de contenido Web con el fin de aumentar la productividad de los empleados.

6. Es obligación de cada jefe de área o encargado de dependencia el reportar de manera inmediata a la División Desarrollo de Tecnologías de la Información y Comunicación a través de los números telefónicos 2268-3166, 2268-3426 o correo electrónico seguriad.tic@isss.gob.sv los cambios de personal que puedan afectar el uso del servicio de Internet, tales como: traslados, restauros, suspensiones, despidos, vacaciones, licencias, incapacidades, etc.

7. El uso de comunicación interactiva o Chats: Messenger, ICQ, AOL, Yahoo Messenger, Google Talk, entre otros, deberá ser justificado y autorizado por la jefatura respectiva previo al análisis y consideración por parte del área técnica competente.

8. Los usuarios deberán tomar las medidas de seguridad en la descarga de archivos gratuitos, en sitios Web desconocidos, redes sociales y cualquier tipo de chat; ya que son una potencial vía de propagación de virus y será responsabilidad del usuario cualquier consecuencia generada por esa acción.

9. No descargar, instalar y distribuir programas no relacionados con el desempeño de las labores diarias, específicamente aquellos ubicados en redes peer-to-peer, servicio de alojamiento personal en Internet, redes compartidas, canales de chat o cualquier otro medio disponible en Internet.

10. No utilizar programas para evadir las medidas de seguridad implementadas que regulan el buen uso de Internet.

11. No acceder a sitios que distribuyan programas de software que violentan los derechos de autor o derechos de copia según las leyes internacionales y nacionales. Esto incluye copiar o editar: información, imágenes, música o videos protegidos por los derechos de autor y derechos de copia.

12. No descargar contenido multimedia que contenga: material pornográfico, racista, político, que incite a la violencia, odio o cualquier actividad ilegal, a menos que sea parte de una actividad relacionada con el desempeño de las labores diarias.

13. Es responsabilidad del usuario la eliminación de los archivos temporales e historial de navegación en Internet.

14. No utilizar Internet para actividades que no están relacionadas con el desempeño de las funciones relacionadas con el cargo asignado y las labores diarias.

15. No utilizar Internet para visitar páginas con contenido pornográfico, sexual explícito o implícito, pedofilia, criminal, terrorista u ofensivo.

16. No utilizar Internet para actividades criminales según lo definido por las leyes de la Republica de El Salvador.

17. No utilizar Internet para la transmisión de información o material en violación a las leyes de la Republica de El Salvador.

18. No utilizar Internet para publicar o difundir información del Instituto que sea considerada de carácter confidencial.

19. Está prohibido el uso de cualquier dispositivo que permita conectarse a Internet diferente a los medios de conexión brindados por el Instituto (redes alámbricas e inalámbricas propiedad del ISSS) en todos los equipos propiedad del ISSS o propiedad del empleado y que estén directa o indirectamente conectados o que tengan interacción con la red institucional. Cualquier consecuencia derivada de esta falta, será responsabilidad del empleado y estará sujeta a las acciones disciplinarias contempladas en esta política..

20. No se permite el uso de aplicaciones y/o sistemas de búsqueda, obtención e intercambio de archivos; como por ejemplo: Kazaa, e-Mule, Napster, Imesh, entre otros; para la obtención de cualquier material: música, videos, aplicaciones y/o sistemas comerciales con derechos reservados cuyo uso y/o distribución represente una violación a las leyes de derecho de copia. La institución se reserva el derecho de rehusarse a defender a cualquier empleado ante cualquier asunto legal relacionado a infracciones a las leyes de copyright o piratería de software.

21. No se permite la descarga y utilización de ningún tipo de juego en línea (flash, shockwave, Java, etc.).

22. No se permite la descarga e instalación de barras de búsqueda, ya que estas generan tráfico excesivo en la red al enviar las preferencias de navegación del usuario a servidores externos para luego desplegar ventanas emergentes con propaganda, mejor conocido como spyware o adware.

23. No se permite compartir el usuario y contraseña con derechos de navegación a Internet con otros usuarios de manera que aquellos usuarios que no cuentan con derecho de navegación a Internet puedan hacerlo sin autorización.

6.8.6 DEBERES Y RESPONSABILIDADES

Todo usuario con acceso a Internet debe cumplir con esta política y regirse en todo momento por las leyes de la Republica de El Salvador, incluyendo pero no limitado a, los derechos de autor, las leyes que rigen las comunicaciones, además de los derechos de privacidad de otras personas.

Toda actividad ilegal o cualquier otra actividad que intercepte o interrumpa el uso de las computadoras o la red están prohibidas.

6.8.7 VIGILANCIA Y MONITOREO

A través de los equipos de monitoreo y análisis de tráfico instalados en la División Desarrollo de Tecnologías de la Información y Comunicación, se detectarán a los usuarios que hagan mal uso de los servicios de Internet.

- La División Desarrollo de Tecnologías de la Información y Comunicación utilizará programas de registro y seguimiento de sesiones de usuario para verificar el cumplimiento de estas normas.

- La División Desarrollo de Tecnologías de la Información y Comunicación del Instituto Salvadoreño del Seguro Social cooperará plenamente con las autoridades competentes en la investigación de cualquier presunto delito y/o violación de la seguridad de sistemas o redes; internos y/o externos causado por cualquier usuario.

6.8.8 ACCIONES DISCIPLINARIAS

Cualquier usuario que viole esta política puede estar sujeto a las acciones disciplinarias contempladas en el Reglamento Interno del ISSS.

El incumplimiento de esta política conlleva a la suspensión del servicio de Internet por un periodo no menor a 1 mes, en caso de reincidencia la suspensión del servicio de Internet será definitiva.

7. COMUNICACIONES

Se han elaborado las siguientes políticas, con el fin de establecer la plataforma y dar seguimiento a los diversos procesos de comunicación, para facilitar el intercambio de información entre las áreas que conforman el Instituto, además de hacer más eficientes algunos de los servicios que se prestan a los usuarios internos y externos de la información que se genera en el seno de la Institución.

7.1 SERVICIO DE CORREO ELECTRÓNICO INTERNO

RESPONSABLES:	SECCION ADMINISTRACIÓN DE SEGURIDAD Y BASE DE DATOS

7.1.2 INTRODUCCIÓN

Todo empleado que haga uso del correo electrónico Institucional en todas las dependencias del ISSS, se regirá y aceptará cumplir con los términos y condiciones establecidas en las políticas institucionales, así como las leyes aplicables nacionales e internacionales.

La División Desarrollo de Tecnologías de la Información y Comunicación tiene como meta promover un uso adecuado del correo electrónico y vigilar el cumplimiento de las políticas que lo rigen.

Cualquier usuario que utilice el correo electrónico Institucional y viole esta política y cualquier norma de la Institución, estará sujeto a la suspensión del servicio y a cualquier otra acción disciplinaria que la administración determine.

7.1.3 OBJETIVO

- Regular el servicio de correo electrónico ofrecido por la Institución, según la definición de los términos, condiciones y responsabilidades que gobiernen el uso de este servicio, a través de las computadoras y dispositivos móviles, por parte de los usuarios de la Institución en todas sus dependencias.

- Regular el servicio de correo electrónico como apoyo en la ejecución de las labores diarias, cualquier uso inadecuado de este servicio que interfiera con la imagen de la Institución, autoridades y empleados será considerado una violación a esta política y estará sujeto a las sanciones correspondientes.

7.1.4 ASIGNACIÓN DE CUENTA DE CORREO

Las solicitudes de asignación de cuentas de correo electrónico institucional deberán presentarse por escrito a la División Desarrollo de Tecnologías de la Información y Comunicación con la aprobación y justificación del jefe del área a la que pertenezca el usuario, siendo responsabilidad del jefe del área y del usuario al que se asignaron los privilegios la mala utilización del mismo.

Se podrán otorgar buzones de correo electrónico institucional a personas ajenas al ISSS, siempre y cuando, la solicitud haya sido aprobada por el Jefe del área o responsable de dependencia en el que trabajarán. La definición de la vigencia del buzón de correo electrónico provisto es responsabilidad del jefe del área o responsable de dependencia y deberá ser plasmado en el formato de solicitud vigente. La vigencia podrá ser extendida, previa solicitud del jefe del área o responsable de dependencia respectivo. Una vez expirada la vigencia el buzón y de no contarse con una solicitud de extensión de vigencia, este será desactivado.

El correo institucional es una herramienta de trabajo propiedad del Instituto Salvadoreño del Seguro Social y como tal se asigna a los empleados para su utilización exclusiva en el desempeño de sus labores diarias. Por lo tanto la cuenta de correo asignada no constituye una cuenta de correo personal (ej. Gmail, Hotmail, Yahoo, etc.), y la utilización de esta implica una aceptación de esta política, la cual está disponible en el Portal Institucional.

7.1.5 POLÍTICAS

1. Toda Cuenta de correo electrónico, deberá ser debidamente justificada y especificarse el motivo por el cual se necesita dicho servicio, detallando las funciones para las cuales se desea contar con el servicio de correo electrónico. Dicha solicitud, deberá ser autorizada por el jefe inmediato con el visto bueno de la jefatura inmediata superior, excepto Director General, Subdirecciones, Jefaturas de División y Unidad.

2. La jefatura interesada deberá enviar la solicitud (completamente llena) a la Sección Asistencia, Mantenimiento y Soporte Tecnológico, mediante el procedimiento establecido para tal efecto, se indica que es responsabilidad de cada jefatura solicitante del servicio, velar por el cumplimiento de las normas establecidas. Asimismo es responsabilidad de la misma, notificar a la División Desarrollo de Tecnologías de la Información y Comunicación los cambios o movimientos del personal que autoriza, ya sea estos: traslado a otra dependencia, despido, renuncia entre otros.

3. Los Formularios para Creación de Usuarios de Correo Electrónico deberán ser almacenados por la Sección Administración de Bases de datos y Sistemas Operativos.

4. Las cuentas de usuario se crearán utilizando el usuario de la red, si existiera algún inconveniente, podría variar la cuenta de usuario con la cuenta de correo.

5. Autorización del servicio: La División Desarrollo de Tecnologías de la Información y Comunicación, revisará y está en la libertad de verificar la información de la misma, y autorizará únicamente los servicios que a criterio de esta División ameriten su instalación, (en base a la justificación expuesta en la solicitud).

6. Los problemas de las cuentas, deberán ser reportadas a la brevedad a la División Desarrollo de Tecnologías de la Información y Comunicación para su pronta corrección.

7. Instalación de los Servicios: Personal de la Sección Asistencia Mantenimiento y Soporte Tecnológico o Técnicos de Mantenimiento y Soporte Tecnológico (en el que aplique), se presentará a las instalaciones de los usuarios solicitantes de los servicios y configurará los equipos, de acuerdo a lo autorizado por la División Desarrollo de

Tecnologías de la Información y Comunicación, debiendo además el usuario beneficiado con el servicio, firmar la Hoja de aceptación de políticas institucionales.

8. Los usuarios son completamente responsables de todas las actividades realizadas con los solicitantes y el buzón de correo electrónico asociado.

9. Es una falta grave, facilitar y ofrecer la cuenta de correo electrónico a personas no autorizadas, esta es personal e intransferible.

10. El correo electrónico es una herramienta para el intercambio de información entre personas, no es una herramienta de difusión de información.

11. Está prohibido enviar correo electrónico a personas que no desean recibirlo. Si la División Desarrollo de Tecnologías de la Información y Comunicación recibe quejas, denuncias o reclamos sobre estas prácticas, la cuenta será cancelada.

12. Están prohibidas las siguientes actividades:
    - Utilizar el correo electrónico para cualquier propósito comercial o financiero.
    - Participar en la propagación de "cadenas", esquemas piramidales, divulgación de temas políticos, religiosos o temas similares.
    - Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para la Institución o que no están relacionados con el desempeño de las labores diarias.
    - El envío o reenvío de mensajes con contenidos de carácter difamatorio, insultantes, racista o repulsivo.

13. Para la difusión masiva de correos, deberá existir una coordinación entre la Sección Administración de Bases de Datos y Sistemas Operativos, y la dependencia encargada de emitir los correos, a fin que la información la reciba los destinatarios correspondientes, a excepción de los casos debidos.

14. A los usuarios que accesan directamente a los buzones de correo institucional, deberán evitar que se afecte el espacio del servidor, se establece lo siguiente: Debido a que el espacio de los buzones de

correo institucional afecta directamente sobre el espacio del servidor, se establece lo siguiente:

- Todos los usuarios deben revisar frecuentemente su correo electrónico para leer sus mensajes, de modo que puedan ser eliminados o almacenados en la computadora asignada.

- Todo usuario debe vaciar la papelera de reciclaje de su buzón de correo electrónico.

15. Toda información o contenido que sea transmitido por las cuentas de correo electrónico institucional, cualquier punto de vista u opiniones presentadas son responsabilidad del autor y no necesariamente representan los del ISSS. El Instituto no aceptará responsabilidad alguna por el contenido del correo electrónico, ni por las consecuencias de las acciones tomadas en base a la información provista, a menos que esa información sea subsecuentemente confirmada por medio escrito, de lo contrario la responsabilidad absoluta recae únicamente sobre el empleado que lo envió.

16. Todos los correos pueden ser monitoreados.

17. Si por cualquier motivo sospecha que la seguridad de su cuenta de correo electrónico ha sido comprometida, deberá notificarlo en un lapso no mayor a 24 horas a la División Desarrollo de Tecnologías de la Información y Comunicación a través de: los teléfonos 2268-3166, 2268-3418.

18. Es obligación de cada jefe de área o encargado de dependencia, el reportar de manera inmediata a la División Desarrollo de Tecnologías de la Información y Comunicación, a través de los números telefónicos 2268-3166, 2268-3426 los cambios de personal que puedan afectar el uso del servicio de correo electrónico, tales como: traslados, retiros, suspensiones, despidos, vacaciones, licencias, incapacidades, etc.

19. Las cuentas de correo electrónico no son transferibles, es decir un buzón de correo electrónico desactivado o eliminado no puede ser asignado a otro usuario, la nueva cuenta debe ser solicitada como una cuenta nueva y la cuenta antigua será eliminada luego de realizarse el respectivo respaldo.

20. Toda cuenta de correo electrónico, que no haya sido accesada por el usuario en un periodo mayor a 30 días, será desactivada a menos que

se cuente con una notificación por escrito o por correo electrónico que justifique lo contrario.

21. Las cuentas de correo electrónico pertenecen a la dependencia que las solicito, por tal motivo si el empleado propietario de la cuenta ya no pertenece a la dependencia, el jefe de esta puede disponer del buzón de correo electrónico para que este sea eliminado y substituido por uno nuevo para otro empleado, esta cuenta deberá ser solicitada como cuenta nueva y deberá ser acompañada por la solicitud de eliminación de la cuenta anterior.

7.2 FORMATO DE ARCHIVOS PARA INTERCAMBIO DE INFORMACIÓN

RESPONSABLES:	DEPENDENCIAS DEL ISSS

7.1.1 OBJETIVO

Contar con un método que permita normar y establecer los formatos y protocolos, así como las actividades necesarias para intercambiar información de forma eficiente y segura entre las entidades.

7.1.2 POLITICAS

1. Cuando la información que se pretenda intercambiar sean archivos tipo texto, el formato deberá ser en Microsoft Word o PDF, o en su defecto en código ASCII o TXT.

2. Si se trata de información contenida en hojas de cálculo, ésta deberá tener el formato de Excel ó CSV.

3. Cuando la información a intercambiar sean imágenes o gráficos, deberán ser enviados en archivos de formato TIF, GIF, PCX, JPG, o PNG o BMP, dependiendo de los programas con que cuenten las áreas involucradas. Debe evitarse el uso de BMP en la medida de lo posible, debido a que es el formato de mayor peso.

4. Si se trata de algún otro tipo de archivo no mencionado anteriormente, para su envío deberá contactar antes al área receptora, para poder establecer el formato común de dicho archivo.

5. En archivos que rebasen el tamaño de 6 Mb, se deberá utilizar un método de compresión bajo el formato .ZIP ó .RAR

6. Antes de proceder a la transferencia de información, la unidad emisora tiene la obligación de verificar que su información esté libre de virus o cualquier otro tipo de código malicioso, para así, preveer contagiar al receptor con algún virus informático.

8. ADQUISICIÓN DE BIENES INFORMÁTICOS

RESPONSABLES:	DEPENDENCIAS DEL ISSS

8.1 OBJETIVO

Contar con un método estándar para la adquisición de equipos para nuevos proyectos de renovación por obsolescencia o daño por parte de cada área.

8.2 POLÍTICAS

1. La adquisición de bienes informáticos se apegará a los procedimientos establecidos por la Ley de Adquisiciones y Contrataciones de la Administración Publica y a su Reglamento vigente, así como por el Presupuesto para el Ejercicio correspondiente.

2. Las tecnologías de información que se planeen adquirir, deberán ser congruentes con los servicios que se pretenden prestar y apegarse a las medidas de racionalidad, austeridad y disciplina presupuestal vigentes.

3. Es responsabilidad del usuario solicitar equipo informático durante el primer trimestre de cada año para ser considerado en el presupuesto del año siguiente.

4. La renovación del equipo informático se realizará de acuerdo a la vida útil del mismo, que en el caso de computadoras será de 5 años y para impresores de 3 años.

5. La División Desarrollo de Tecnologías de la Información y Comunicaciones, pondrá a disposición de los funcionarios del ISSS, las especificaciones técnicas de los equipos más frecuentes, por medio del sitio WEB del ISSS (www.isss.gob.sv/especificaciones)

6. Los procesos de adquisición de tecnologías de información se regirán por lo establecido en las bases de licitación.

9. ATENCIÓN DE REQUERIMIENTOS

RESPONSABLES:	USUARIO O SOLICITANTE, DEPENDENCIAS Y DIVISIÓN DESARROLLO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

9.1 OBJETIVO

Define las políticas de recepción y atención de requerimientos de servicio que se realizan a la División Desarrollo de Tecnologías de la Información y Comunicaciones.

9.2 POLÍTICAS

1. Será responsabilidad del usuario registrar los requerimientos y solicitudes de servicios a través de la Sección Asistencia, Mantenimiento y Soporte Tecnológico para que estos sean atendidos. Caso contrario la División Desarrollo de Tecnologías de la Información y Comunicaciones, no será responsable de su resolución o consecuencias.

2. Es responsabilidad de las jefaturas de la División Desarrollo de Tecnologías de la Información y Comunicaciones correspondiente, proporcionar los manuales de usuario, manuales técnicos, contraseñas, códigos fuentes, respaldos y licencias a la Sección Asistencia, Mantenimiento y Soporte Tecnológico para su resguardo.

3. Será responsabilidad de las jefaturas de cada área de la División Desarrollo de Tecnologías de la Información y Comunicaciones establecer guías de atención y/o procedimientos de solución de los requerimientos más frecuentes y asegurarse que estos sean proporcionados al jefe de Sección Asistencia, Mantenimiento y Soporte Tecnológico, para que este pueda brindar soluciones a las demandas de servicio más comunes.

4. El personal de la División Desarrollo de Tecnologías de la Información y Comunicaciones encargado de la resolución del requerimiento, será responsable de seguir el procedimiento y/o normativas establecidas para la atención del requerimiento.

5. Todas las solicitudes de servicio y requerimientos recibidos serán atendidas secuencialmente (en orden de llegada), a excepción de los requerimientos de carácter urgente designados por jefaturas inmediatas de la División

Desarrollo de Tecnologías de la Información y Comunicaciones o las prioridades establecidas por las autoridades superiores"

6. Es responsabilidad del Operador Help Desk comunicar la asignación de un nuevo requerimiento a la Jefatura de la Sección y/o Departamento de la División Desarrollo de Tecnologías de la Información y Comunicaciones encargada de su resolución.

7. Las Jefaturas de las diferentes áreas de la División Desarrollo de Tecnologías de la Información y Comunicaciones, serán las responsables de darle seguimiento a los requerimientos asignados a su área hasta su finalización.

8. El Personal asignado para la resolución del requerimiento, será responsable de notificar de forma inmediata la finalización del requerimiento a su Jefatura o a la Sección Asistencia, Mantenimiento y Soporte Tecnológico para actualizar en el sistema el estatus del requerimiento, previa autorización del jefe inmediato.
9. Es responsabilidad de las jefaturas de la División Desarrollo de Tecnologías de la Información y Comunicaciones correspondiente evaluar todas aquellas actividades de acuerdo a su prioridad de atención o complejidad y trasladar a la Sección Asistencia, Mantenimiento y Soporte Tecnológico las que corresponden a un primer nivel de atención.

10. Es responsabilidad de cada Dependencia de la División Desarrollo de Tecnologías de la Información y Comunicaciones, archivar física o electrónicamente, la evidencia de la resolución del requerimiento.

10. CREACIÓN DE USUARIOS PARA CORREO ELECTRÓNICO INSTITUCIONAL

RESPONSABLES:	USUARIO TÉCNICO DE MANTENIMIENTO Y SOPORTE TECNOLÓGICO OPERADOR DE HELP DESK

10.1 OBJETIVO

Describir políticas para la creación de cuenta de correo electrónico, así como los requisitos a cumplir por parte de los usuarios solicitantes.

10.2 POLÍTICAS

1. Se crearán usuarios de dominio y se dará acceso a los servicios únicamente cuando el usuario complemente el formulario Solicitud de Servicios de Red y este deberá estar autorizado por el jefe de la dependencia del empleado solicitante

2. Las solicitudes de Creación de Usuarios de Correo Electrónico deberán ser recibidas y registradas en el Sistema de Asistencia Informática.

3. Los Formularios para Creación de Usuarios de Correo Electrónico deberán ser almacenados por la Sección Administración de Bases de datos y Sistemas Operativos.

4. El número permitido de usuarios de correo electrónico estará definido por la capacidad de los Servidores de Correo Electrónico y la cantidad de licencias adquiridas para ello.

11. ADMINISTRACIÓN DE RECURSOS INFORMÁTICOS

RESPONSABLES:	PERSONAL DE LA DIVISIÓN DESARROLLO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

11.1 OBJETIVO

Definir las políticas para la Administración de licencias, manuales técnicos y de usuario, backups o medios de almacenamiento, contraseñas y códigos fuente.

11.2 POLÍTICAS

1. Es responsabilidad del encargado de Recursos Informáticos y Contratos, velar por el buen estado de los Recursos Informáticos resguardados en la Sección Asistencia, Mantenimiento y Soporte Tecnológico.

2. El encargado de Recursos Informáticos y Contratos deberá mantener los recursos informáticos en orden y clasificados según tipo.

3. Será responsabilidad del encargado de Recursos Informáticos y Contratos asegurarse que se cumpla el tiempo estipulado para el préstamo de los recursos informáticos y llevar actualizado el inventario.

4. El usuario será responsable de enviar las licencias de software para resguardo en la Sección Asistencia, Mantenimiento y Soporte Tecnológico cuando estas no sean adquiridas a través de la División Desarrollo de Tecnologías de la Información y Comunicaciones.

5. Es responsabilidad del encargado de Recursos Informáticos y Contratos entregar al usuario los Recursos Informáticos solicitados siempre que cumplan con los requisitos establecidos para su préstamo.

6. El préstamo de Recursos Informáticos deberá registrarse en la bitácora que se lleva en la Sección Asistencia Mantenimiento y Soporte Tecnológico, la cual será firmada por el usuario al momento de recibir lo solicitado.

7. El período de préstamo de un Recurso Informático dependerá de los rangos establecidos para cada tipo de recurso, no debiendo exceder de 3 días hábiles, en caso que se necesite más tiempo, el usuario deberá solicitar prorroga del periodo de préstamo y actualizar la bitácora. De lo contrario el encargado de Recursos Informáticos y Contratos, deberá gestionar su recuperación.

8. Se deberá dar cumplimiento a la depuración de los Recursos Informativos, de acuerdo al procedimiento establecido.

9. Cuando un usuario reporte la pérdida de un Recurso Informático o cuando éste sea devuelto incompleto o dañado, es responsabilidad del encargado de Recursos Informáticos y Contratos comunicarlo inmediatamente al jefe de la Sección Asistencia, Mantenimiento y Soporte Tecnológico para que este lo informe por escrito al jefe inmediato del usuario, solicitándole se proceda a investigar lo sucedido y se emita un informe que respalde la pérdida o el daño.

10. Es responsabilidad del encargado de Recursos Informáticos y Contratos verificar que se reciba toda la documentación necesaria que proporcione las especificaciones requeridas para realizar el registro en el Sistema del Recurso Informático y archivarlos en el lugar que corresponde.

11. Es responsabilidad del usuario que proporciona manuales y licencias de Software, proporcionar la respectiva documentación para que sea registrado en el Sistema.

12. Cuando sean resguardados los recursos informáticos, estos deberán ser identificados por el número de ingreso que le asigna el sistema.

12. EJECUCIÓN Y TRASLADO DE BACKUPS A LA BÓVEDA DE SEGURIDAD EXTERNA

RESPONSABLES:	ADMINISTRADOR DE SISTEMAS OPERATIVOS ENCARGADO DE RECURSOS INFORMÁTICOS Y CONTRATOS

12.1 OBJETIVO

Establecer las políticas para la ejecución de los backups de los Servidores de Datos y Aplicaciones seleccionados para ello y para el traslado de los backups ejecutados a la Bóveda de Seguridad Externa.

12.2 POLÍTICAS

1. Es responsabilidad del Administrador de Sistemas Operativos ejecutar diariamente los backups de los Servidores de Datos y Aplicaciones seleccionados.

2. Es responsabilidad del Administrador de Sistemas Operativos realizar el control de calidad de la información contenida en los backups ejecutados, utilizando los procedimientos establecidos para ello.

3. Cuando un backup no pueda ser ejecutado o finalizado satisfactoriamente, es responsabilidad del Administrador de Sistemas Operativos tratar de solventar el problema por propia cuenta o con ayuda del proveedor si se tuviere, en caso de no resolverlo, comunicarlo al jefe de la Sección Administración de Base de datos y Sistemas Operativos y a la Sección Asistencia Mantenimiento y Soporte Tecnológico para su control.

4. Los backups ejecutados deberán ser registrados por el operador que los realiza en la Bitácora de Backups Ejecutados. Este control puede ser llevado de forma automática por medio del Software Institucional que se usa para la ejecución de los respaldos.

5. Es responsabilidad del encargado de Recursos Informáticos y Contratos trasladar el juego de backups ejecutados a la Bóveda de Seguridad Externa, con la periodicidad establecida en el procedimiento Ejecución Y Resguardo de Backups.

6. Los juegos de backups deberán ser trasladados y entregados al encargado de la Bóveda de Seguridad en las respectivas Cajas de Seguridad.

7. La Sección Administración de Bases de Datos y Sistemas Operativos deberá realizar el reciclaje de los medios de almacenamiento que han sido utilizados para respaldos diarios, siempre que esto no afecte a otros respaldos cuya validez no haya caducado.

8. Los backups mensuales deberán mantenerse archivados durante el período solicitado por el área propietaria de la Información, y en concordancia con el reglamento emitido por la Corte de Cuentas de la República.

13. PROCESAMIENTO DE ÓRDENES DE TRABAJO PARA EJECUCIÓN DE PROCESO, PROGRAMA O IMPRESIÓN DE LISTADOS

RESPONSABLES:	SECCIÓN DE ADMINISTRACIÓN DE BASES DE DATOS Y SISTEMAS OPERATIVOS

13.1 OBJETIVO

Satisfacer en forma eficiente, eficaz y oportuna las demandas de los usuarios que solicitan ejecución de proceso, programa o impresión de listados de la División Desarrollo de Tecnologías de la Información y Comunicación, a través del cumplimiento de normas y estándares de procedimientos en la atención de los requerimientos y solicitudes recibidas.

13.2 POLÍTICAS

1. Toda ejecución de proceso, programa o impresión de listados, que se requiera realizar en la Sección de Administración de Bases de Datos y Sistemas Operativos, deberá gestionarlo el área solicitante mediante requerimiento a la Sección Asistencia, Mantenimiento y Soporte Tecnológico. Dicho requerimiento debe contener toda la información necesaria para realizar el trabajo, de manera clara, correcta, completa y específica, todos los parámetros e información necesaria para la ejecución de la misma, por lo que se deben anotar nombre de archivos, programas, jobs, longitud de registro, catálogo, datos a digitar, momento en el que se debe ejecutar, etc.

2. La Sección de Administración de Bases de Datos y Sistemas Operativos, ejecutará los requerimientos en el orden que le sean entregadas, pudiendo alterar dicho orden, las de prioridad con nivel alto. Si se determinaran otras prioridades, éstas serán indicadas por la jefatura de la Sección de Administración de Bases de Datos y Sistemas Operativos o de las jefaturas superiores de la División Desarrollo de Tecnologías de la Información y Comunicación.

3. Si un requerimiento no puede ser ejecutado por fallas en los programas, jobs o parámetros indicados, dicho requerimiento se regresará al solicitante indicando el problema generado, en estos casos para reejecutar el proceso se debe generar uno nuevo.

4. Cuando el requerimiento haya sido procesado, el Administrador de Sistemas Operativos que verifique la finalización del proceso, informará a la Sección Asistencia, Mantenimiento y Soporte Tecnológico, al Jefe inmediato superior y al usuario solicitante, especificando la fecha y hora de finalización del proceso.

14. IMPLEMENTACIÓN DE SISTEMAS DE INFORMACIÓN

RESPONSABLES:	SECCIÓN IMPLEMENTACIÓN DE SISTEMAS

14.1 OBJETIVO

Establecer las políticas para la implementación de Sistema de Información con el fin de garantizar el buen funcionamiento y operación de los mismos.

14.2 POLÍTICAS

1. La implementación de Sistemas de Información podrá realizarse por requerimiento de usuario, Plan de Trabajo de la División Desarrollo de Tecnologías de la Información y Comunicación o a Plan Estratégico Institucional.

2. La solicitud de requerimiento de implementación de un sistema de información por parte de un usuario, deberá ser autorizada por el jefe de la dependencia o Director del centro de atención, que requiere la Implementar un sistema y puede ser enviada a través de nota o correo electrónico.

3. La Jefatura de la dependencia a la cual se le implementará un sistema de información, deberá proporcionar a la Sección Implementación de Sistemas la información de los empleados a los cuales se les capacitará para la operación del sistema, cumpliendo con las normas de implementación (Capacitar un mínimo de 2 personas por aplicación).

4. La Sección Implementación de Sistemas no implementará un sistema de información, si la dependencia o proceso a automatizar, no reúnen las condiciones técnicas necesarias ya establecidas, según lo requieran los sistemas de información específicos, y especialmente si el equipo informático no cuenta con la protección de UPS.

5. El Analista Implementador de Sistemas, deberá entregar a la Jefatura de la dependencia a la cual se le implemente un sistema de información, la correspondiente acta de implementación, como constancia de las condiciones y recomendaciones para mantener eficiente el funcionamiento y operación del sistema de información.

6. La metodología para la migración de datos comprende los siguientes pasos:
   a. Extracción de datos del sistema de origen.
   b. Transformación de los datos en el formato adecuado.
   c. Carga de datos en el correspondiente módulo.
   d. Comprobación de los datos.
      - Reportar detalle de datos migrados correctamente.
      - Reportar detalle de los datos no migrados.
   e. Aplicar migración en ambiente productivo.

   Teniendo en las consideraciones siguientes:
   a. Utilizar un entorno de ensayo, el cual será el ambiente de pruebas funcionales (ambiente calidad).
   b. La estrategia a utilizar: ENTRADA DIRECTA.
   c. Tipo de datos migrado: DATOS MAESTROS/DATOS TRANSACCIONALES.

15. POLÍTICA PARA CLASIFICACIÓN DE LA INFORMACIÓN

RESPONSABLES:	DIVISIÓN DESARROLLO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

15.1 OBJETIVO

Establecer las políticas para la clasificación de la información en el Instituto.

15.2 POLÍTICAS

1. La información en el Instituto Salvadoreño del Seguro Social se clasificará de la siguiente manera:

   a) Información Pública.
   b) Información Confidencial.
      i) Información con confidencialidad máxima.
      ii) Información con confidencialidad media.
      iii) Información con confidencialidad mínima.
      iv) Información confidencial de terceros .

F. _____
Ing. José Pedro Rivera Moncada
Jefe División de Desarrollo de Tecnologías de Información y Comunicación

F. _____
Inga. Claudia Jennifer Molina
Jefa de Unidad de Desarrollo Institucional

Fecha de modificación 19/08/2015

2. Definición de grado de confidencialidad.

   Mínima: Información general que no puede ser conocida por terceros sin autorización del responsable de la información. Es del tipo de información que si es utilizada o modificada sin autorización impactaría en forma leve al ISSS.

   Media: Información financiera o técnica que no puede ser conocida por terceros sin autorización del responsable de la información. Es del tipo de información que si es utilizada o modificada sin autorización impactaría de forma importante al ISSS.

   Alta: Información financiera o técnica que no puede ser conocida por terceros sin autorización especial de la Dirección General del ISSS. Es del tipo de información que si es utilizada o modificada sin autorización impactaría de forma grave al ISSS.

16. SEGURIDAD LÓGICA

RESPONSABLES:	SECCIÓN ADMINISTRACIÓN DE BASE DE DATOS Y SISTEMAS OPERATIVOS

16.1 INTRODUCCIÓN

En este apartado, se establece la política de seguridad informática del Instituto Salvadoreño del Seguro Social, la cual pretende proteger la integridad de los datos y mitigar los riesgos y perdidas asociadas con las amenazas de seguridad dirigidas hacia los recursos informáticas.

Como muchas otras instituciones el Instituto Salvadoreño del Seguro Social, puede experimentar incidentes de seguridad con diferentes niveles, estos incidentes pueden ser desde una infección individual de virus hasta la pérdida de conectividad de red producto de diferentes tipos de ataques. La gestión proteger de estos incidentes es una responsabilidad de la División Desarrollo de Tecnologías de la Información y Comunicación.

16.2 OBJETIVOS

Los objetivos de la política de seguridad informática son:

- Establecer políticas de seguridad a nivel Institucional para proteger la integridad de los datos contenidos en los recursos informáticos del Instituto Salvadoreño del Seguro Social de daños, abusos y usos inapropiados.

- Establecer políticas que identifiquen y prevengan el abuso de la red y sistemas informáticos.

16.3 POLÍTICAS PARA CREACIÓN Y NOMBRAMIENTO DE CUENTA DE USUARIO

I. Declaración de la Política de Seguridad

La División Desarrollo de Tecnologías de la Información y Comunicación del Instituto Salvadoreño del Seguro Social, provee recursos de red a todas las dependencias para tener acceso a los sistemas informáticos en utilización. Se crearán políticas para establecer medidas para prevenir o al menos minimizar el número de incidentes de seguridad informática institucional.

II. Administración del Acceso de Usuarios

a) Cuentas de Usuario

1. Este conjunto de políticas es de exclusiva aplicación para el software que administra las cuentas de usuario de la red o dominio Institucional. No es aplicable a la seguridad particular de otro software adquirido a terceros, hechos dentro de la Institución o cualquier otra herramienta informática que se posea.

2. Las cuentas de usuario son requeridas para acceder a la red institucional, servidores y recursos compartidos. Toda cuenta de usuario deberá ser solicitada a través del formato denominado "solicitud de creación de usuario de red", ver Anexo No. 2.b. Estas deben ser canalizadas por el Jefe inmediato Superior del usuario al Técnico de Mantenimiento y Soporte Tecnológico del centro de atención o a la Sección Asistencia, Mantenimiento y Soporte Tecnológico para el caso de Torre Administrativa y dependencias que no posean Técnico de Mantenimiento y Soporte Tecnológico. Si el usuario es interino deberá especificarse el periodo de acceso.

3. Cada cuenta de usuario es creada para ser utilizada por una única persona, por tal razón está prohibido compartirlo. La persona para la cual la cuenta fue creada es responsable de la seguridad de la cuenta y de las acciones asociadas a su utilización.

4. Una cuenta puede ser inactivada si:

   - La utilización de esta viola cualquier porción de esta política.
   - El propietario de la cuenta ha realizado actividades que violan cualquier porción de esta política.
   - El propietario de la cuenta, ya no tiene una relación laboral con el Instituto Salvadoreño del Seguro Social.
   - Por conveniencia Institucional.
   - Evaluación técnica por parte de Informática.
   - Poco uso de esta o no uso de ella por un periodo superior a los 30 días calendario, sin justificación proporcionada a Informática por parte del jefe inmediato superior del usuario. La justificación debe ser

enviada por correo electrónico o nota escrita al jefe de la Sección Administración de Bases de Datos y Sistemas Operativos, con copia a la jefatura de la Sección Asistencia, Mantenimiento y Soporte Tecnológico.

5. La creación y activación de una cuenta de usuario, constituye un acuerdo que establece que el usuario ha comprendido esta política y se someterá a esta.

6. Toda cuenta de usuario de red será nombrada de la manera siguiente, tomando como base el nombre según DUI, exceptuando las que por la naturaleza del trabajo deban crearse con nombre genérico:
   Primer nombre. Primer apellido
   Ej. Nombre del solicitante a cuenta de red **Mario Antonio Salazar Bermúdez,** siguiendo el estándar el nombre de cuenta seria **mario.salazar**

   Sin embargo y teniendo en consideración que pudiera haber más personal con nombre coincidente, y que no pueda aplicarse este estándar, se tendrán las siguientes alternativas:

   Primer nombre inicial segundo nombre. Primer apellido; cuando ya exista una cuenta asignada bajo el estándar principal, es decir cuando ya exista una cuenta con el primer nombre. Primer apellido.
   Ej. **Mario Enrique Salazar Torres**; nombre de cuenta **marioe.salazar**

   Primer nombre inicial segundo nombre. Primer apellido inicial segundo apellido, cuando en casos muy especiales, se hace difícil la creación de la cuenta.
   Ej. Mario Enrique Salazar Bermudez; nombre de cuenta **marioe.salazarb.**

   Primer nombre. Primer apellido inicial segundo apellido; cuando ya exista una cuenta asignada bajo el estándar anterior, es decir cuando ya exista una cuenta con el primer nombre inicial segundo nombre. Primer apellido inicial segundo apellido.
   Ej. **Mario Enrique Salazar Torres**; nombre de cuenta **mario.salazart**

   Si el solicitante de la cuenta es mujer casada, el nombre de usuario se constituirá en base al nombre según DUI y considerando las leyes vigentes al respecto. Por lo cual, las mujeres casadas podrán optar por tener su nombre de usuario según los criterios anteriores o haciendo uso de su apellido de casada:
   Primer nombre. Apellido de casada.

Ej. Silvia Elena Sandoval de Martinez; nombre de cuenta **silvia.demartinez**

En el caso que la usuaria finalizará su matrimonio, y decidiera cambiar su nombre de usuario para obviar el apellido de casada, podrá hacerlo haciendo la solicitud respectiva con el Técnico de Mantenimiento y Soporte Tecnológico local o a la Sección Asistencia, Mantenimiento y Soporte Tecnológico según corresponda, anexando a dicha solicitud fotocopia del DUI actualizado, luego de finiquitado el divorcio. Esto implica que su usuario será eliminado y se creará una nueva cuenta considerando los criterios anteriormente detallados. Por lo cual, el requerimiento deberá tener dos componentes, uno para la creación del nuevo usuario y otro para la configuración de su equipo de cómputo con el nuevo usuario y la migración correspondientes de la información institucional desde la anterior cuenta. Aquellas usuarias con correo electrónico asignado deberán actualizar a sus contactos con la nueva dirección asignada a partir de esta modificación.

7. Las cuentas con nombre genérico serán utilizadas por trabajadores que por la naturaleza del cargo desempeñado lo amerite, tomando para ello los siguientes criterios:

   - El puesto de trabajo es utilizado por diferentes empleados a lo largo del tiempo, como por ejemplo en procesos de rotación de personal frecuente.
   - El puesto de trabajo prevalece sobre el empleado que lo ocupa. Por ejemplo el caso de Secretarias.
   - La División Desarrollo de Tecnologías de la Información y Comunicación o la jefatura superior del puesto de trabajo considera que la cuenta de usuario correspondiente debe ser genérica.
   - La División Desarrollo de Tecnologías de la Información y Comunicación puede obviar la creación de una cuenta de usuario genérica si así lo cree conveniente.

   El nombre de usuario de una Cuenta Genérica se construirá en base al nombre de puesto de trabajo que lo usará, de forma abreviada pero siendo lo más legible posible. Por ejemplo, para el caso de Secretaria de Dirección General podrá ser una opción "Secr. DirGral".

8. Las cuentas de usuario especiales utilizadas para propósitos específicos como monitoreos, interacción entre sistemas, plug-in, sistema de administración, así como cualquier otro software que sea necesario instalar y que este requiere usuario de Dominio serán creadas acorde a

las especificaciones propias de cada software o con las que la División Desarrollo de Tecnologías de la Información y Comunicación considere más convenientes técnica y administrativamente.

9. Los campos que de carácter obligatorio deben ser completados son:
   - Nombre completo (Nombre de pila y apellidos).
   - Nombre para mostrar.
   - Descripción (Puesto o Cargo).
   - Departamento.
   - Oficina (Ubicación).
   - Teléfono.
   - Número de empleado.

10. Es obligación de cada usuario mantener la información anteriormente detallada completa y actualizada. En caso de necesitar modificaciones, se debe hacer el respectivo requerimiento al Técnico de Mantenimiento y Soporte Tecnológico o a la Sección Asistencia, Mantenimiento y Soporte Tecnológico, para el caso de la Torre Administrativa o dependencias dónde no se cuenta con Técnico de Mantenimiento y Soporte Tecnológico. Una vez recibido el requerimiento y asignado, es responsabilidad del Técnico de Mantenimiento y Soporte Tecnológico o del Administrador de Sistemas Operativos respectivo hacer la actualización de la Información.

11. Es obligación de los jefes inmediatos informar a la Sección Administración de Bases de Datos y Sistemas Operativos acerca de cualquier cambio en los puestos de trabajo. En caso que el movimiento sea interno, se deberá justificar el uso de Cuenta de Usuario de Red, Correo Electrónico, Internet y cualquier otro servicio informático que el usuario tenía en su cargo laboral previo, para validar si estos se mantendrán o no en el nuevo cargo. En el caso que el movimiento sea fuera hacia otra área, se deshabilitarán los servicios informáticos asignados al usuario, para lo que será necesario hacer de nuevo el requerimiento de asignación de dichos servicios, por parte del nuevo jefe inmediato superior.

12. Toda cuenta de usuario deberá ser solicitada a través del formato establecido por la División Desarrollo de Tecnologías de la Información y Comunicación y canalizada a través de la Sección Asistencia, Mantenimiento y Soporte Tecnológico de la División antes mencionada.

13. Las cuentas de usuario y los servicios asociados a esta: correo electrónico y acceso a Internet, deberán ser utilizados exclusivamente como una herramienta de trabajo.

14. Cada cuenta de usuario es creada para ser utilizada por una única persona, por tal razón está prohibido compartirla. La persona para la cual la cuenta fue creada es responsable de la seguridad de la cuenta y de las acciones asociadas a su utilización.

15. Cualquier actividad ilegal, que afecte a terceros, que vaya en contra de los intereses institucionales o que no sea de aspecto laboral, realizada desde una cuenta de usuario, es responsabilidad del empleado propietario (asignado) de esta.

16. El acceso a la red por parte de usuarios que no son empleados del Instituto, pero que tienen alguna relación de negocios con él, y que para la ejecución de lo contratado así lo requieran, será permitido únicamente mediante la autorización de las autoridades superiores, por medio de una nota o correo electrónico de respaldo, y debiendo haber hecho el respectivo requerimiento a la Sección Asistencia, Mantenimiento y Soporte Tecnológico.

17. Todo usuario externo o tercero, estará facultado a utilizar única y exclusivamente el servicio que le fue asignado, y acatar las responsabilidades que devengan de la utilización del mismo.

18. No se proporcionará el servicio solicitado por un usuario, sin antes haberse completado todos los procedimientos de autorización necesarios para su ejecución.

19. Si el propietario de la cuenta detecta el uso no autorizado de su cuenta de usuario, deberá comunicarse inmediatamente a la Sección Asistencia, Mantenimiento y Soporte Tecnológico a los teléfonos 2268-3166 y 2268-3418 o a la dirección de correo electrónico asistencia.informatica@isss.gob.sv, reportando el uso no autorizado.

b) Cuentas de Usuario Inactivas o Eliminadas

1. Toda cuenta de usuario es desactivada antes de ser eliminada. El estado inactivo es el paso intermedio entre una cuenta de usuario activa y una cuenta de usuario eliminada. En el estado inactivo, se le niegan a la cuenta de usuario la utilización de todos los servicios: acceso, correo, Internet, recursos compartidos en la red, etc. Una

cuenta puede ser reactivada siempre y cuando no haya sido eliminada.

2. El jefe inmediato superior del usuario deberá informar por escrito al Técnico de Mantenimiento y Soporte Tecnológico del centro de atención o a la Sección Asistencia, Mantenimiento y Soporte Tecnológico según corresponda para proceder a la inactividad o eliminación de la cuenta.

3. Las cuentas de usuarios podrán ser desactivadas a criterio de las jefaturas de cada dependencia.

4. Las dependencias deberán notificar a la División Desarrollo de Tecnologías de la Información y Comunicación, las licencias o incapacidades de los empleados por periodos, mayores a 30 días para que se aplique el procedimiento respectivo a las cuentas de usuarios.

5. Una cuenta puede ser desactivada, cuando el propietario de esta, ya no tiene una relación laboral con el Instituto Salvadoreño del Seguro Social, esta situación deberá ser reportada a la División Desarrollo de Tecnologías de la Información y Comunicación por la jefatura inmediata de la dependencia involucrada, de forma escrita o por medio de correo electrónico.

6. Una cuenta puede ser reactivada siempre y cuando no haya sido eliminada y sea solicitada por la jefatura de dependencia, y haya disponibilidad tanto en capacidad del servidor como en licencias disponibles para ello.

c) Restricción de Servicios

1. En ocasiones la cuenta de usuario puede tener restricciones para la utilización de servicios. Puede haber muchas razones para que esto ocurra, desde el uso inapropiado de los recursos de red, hasta la solicitud explicita de restricción de servicios a la cuenta de usuario por parte del jefe inmediato.

d) Cuentas Compartidas

1. Cualquier actividad abusiva iniciada desde una cuenta de usuario es relacionada al propietario de esta, y el propietario es por lo tanto responsable de esta actividad. El comportamiento de cualquier usuario

con el que se comparta una cuenta de usuario, es de total responsabilidad del propietario de la cuenta. Si el abuso de los recursos de red es tal que la cuenta es restringida o inactivada, el responsable es el propietario de la cuenta. Por lo tanto, las cuentas de usuario no deben ser compartidas. Cada cuenta de usuario tiene una única persona autorizada para utilizarla.

e) Responsabilidades del Usuario

1. El usuario es responsable exclusivo de mantener a salvo su contraseña, así como del buen uso de esta.

2. Se debe evitar el guardar o escribir las contraseñas en cualquier papel o superficie o dejar constancia de ellas, o que esta información esté visible, fácilmente accesible o insegura.

3. El usuario deberá proteger su equipo de trabajo, evitando que personas ajenas a su cargo puedan acceder a la información almacenada en él, mediante una herramienta de bloqueo temporal (protector de pantalla), protegida por una contraseña, el cual deberá activarse en el preciso momento en que el usuario deba ausentarse.

4. Cualquier usuario que encuentre un hueco o falla de seguridad en los sistemas informáticos de la institución, está obligado a reportarlo a los administradores del sistema o Técnico de Mantenimiento y Soporte Tecnológico de su centro de atención, o a la Sección Asistencia, Mantenimiento y Soporte Tecnológico y a la Jefatura de la Sección de Administración de Bases de Datos y Sistemas Operativos, según corresponda.

f) Control de Acceso Entre Redes

1. El acceso a la red interna se permitirá siempre y cuando se cumpla con los requisitos de seguridad necesarios, y éste será permitido mediante un mecanismo de autenticación o previa configuración.

2. Cualquier alteración del tráfico entrante o saliente, a través de los dispositivos de acceso a la red será motivo de verificación.

3. La División Desarrollo de Tecnologías de la Información y Comunicación deberá emplear dispositivos, software o subcontratación de servicios para el bloqueo, enrutamiento, o el filtrado de tráfico, evitando el

acceso o flujo de información no autorizada hacia la red interna o desde la red interna hacia el exterior.

4. Los accesos a la red interna o local desde una red externa de la institución o extranet, se harán mediante un mecanismo de autenticación seguro, y el tráfico entre ambas redes será cifrado con una encriptación cuando aplique.

5. Se registrará todo acceso a los dispositivos de red mediante archivos de registro o Log, de los dispositivos que provean estos accesos.

g) Acceso al Sistema Operativo y Servidores

1. Se deberá renombrar las cuentas de administrador de los equipos, la cual deberá de divulgarse de manera confidencial al personal de la División Desarrollo de Tecnologías de la Información y Comunicación, que amerite tener conocimiento de ello.

2. Al terminar una sesión de trabajo en los servidores, se debe cerrar la sesión en el equipo.

3. El acceso a la configuración del sistema operativo de los servidores, es únicamente permitido al usuario Administrador de Sistemas Operativos, Administrador de Base Datos, Técnico de Seguridad, Jefe de Sección Administración de Bases de Datos y Sistemas Operativos, Jefe de Departamento Soluciones Integrales en Tecnologías de la Información y Comunicación o usuarios administradores de servicios que albergan los servidores y requieren este privilegio para el desarrollo de sus funciones. Este último caso está sujeto a previa aprobación de Jefe de Sección Administración de Bases de Datos y Sistemas Operativos.

h) Protección de los Datos

1. La seguridad de los datos alojados en servidores ubicados en el Centro de Computo de la División Desarrollo de Tecnologías de la Información y Comunicación es controlada por los Administradores de Sistemas Operativos. Toda solicitud de acceso a cualquiera de los datos alojados en dichos servidores, deberá ser autorizada por la Jefatura inmediata y canalizada a través de la Sección Asistencia, Mantenimiento y Soporte Tecnológico.

i) Manejo y Seguridad de Medios de Almacenamiento

1. Los medios de almacenamiento o copias de seguridad del sistema de archivos, o información de la Institución, serán etiquetados de acuerdo a la necesidad que se requiera, para facilitar su debida restauración.

2. Los medios de almacenamiento con información crítica o copias de respaldo, deberán ser manipulados única y exclusivamente por el personal encargado de hacer los respaldos y el personal encargado de salvaguardarla.

j) Abuso de los Recursos Informáticos

1. Es responsabilidad de la División Desarrollo de Tecnologías de la Información y Comunicación realizar todos los esfuerzos posibles para que estos recursos estén disponibles.

2. La penalización del abuso o mal uso de los recursos informáticos disponibles en la red pueden ser: Restricción temporal parcial o total a los recursos informáticos, restricción permanente parcial o total a los recursos informáticos.

3. Cualquiera que intente escribir, transferir, o con pleno conocimiento proliferar gusanos, virus informáticos de cualquier tamaño y forma o cualquier software malicioso, será sujeto de penalización y será restringido permanentemente de todos los recursos informáticos.

4. La utilización de la red informática para la transferencia de archivos que contengan: material pornográfico de cualquier tipo, información de cualquier tipo de los sistemas informáticos para ser negociado y/o obtener beneficio personal de cualquier tipo, atentar contra los intereses Institucionales, quebrantar las leyes o dañar a terceros, está prohibido y es sujeto de penalización y restricción permanente de todos los recursos informáticos.

k) Violación de Cuentas de Usuario y Contraseñas

1. Cualquier intento de obtener acceso o utilización de una cuenta de usuario de manera no autorizada, es considerado una violación. Tales intentos incluyen, pero no están limitados a: Obtención del acceso a la cuenta del usuario, mientras el propietario de la cuenta no se encuentra en su computadora, realización de esfuerzos para determinar la contraseña de la cuenta, mediante la observación de la digitación de esta o el desarrollo y/o instalación de aplicaciones que capturan la secuencia de teclas realizada por el usuario.

2. Cualquier intento de violar u obtener contraseñas, está prohibido.

3. Está prohibido el almacenamiento o transferencia encriptado o sin encriptar de la información pertinente a una contraseña.

4. Escribir, transferir, compilar, almacenar o ejecutar programas diseñados para descifrar contraseñas u obtener acceso no autorizado a cuentas de usuario, cuentas de sistemas o contraseñas, está prohibido, esto incluye programas o técnicas diseñadas para engañar u obligar a los usuarios para que estos divulguen sus contraseñas.

l) Acceso no Autorizado a los Datos de Otro Usuario

1. El acceso no autorizado a los datos o información contenida en la computadora o cualquier otro equipo, dispositivo informático o con capacidad de albergar información asignada al usuario o en servidores, está prohibido.

m) Degradación del Servicio de Red

1. La interferencia del servicio de red está prohibido. Por ejemplo: el apagado de cualquier dispositivo de comunicación, la desconexión del cable de red de cualquier equipo informático, la modificación o reconfiguración no autorizada del hardware o software de cualquier equipo informático, entre otros.

16.3 POLÍTICAS DE SEGURIDAD PARA ADMINISTRACIÓN DE CONTRASEÑAS DE USUARIO

Este conjunto de políticas es de exclusiva aplicación para el software que administra las cuentas de usuario de la red Institucional o dominio Institucional. No es aplicable a la seguridad particular de otro software adquirido a terceros, hechos dentro de la Institución o cualquier otra herramienta informática que se posea.

a) Selección de Contraseña de Cuenta de Usuario

1. Una de las partes más vulnerables de cualquier sistema informático es la contraseña de la cuenta de usuario. Cualquier sistema informático, no importa que tanta seguridad posea contra ataques de red, Troyanos, etc., este puede ser completamente explotado por intrusos que tengan acceso a este a través de una contraseña de usuario pobremente seleccionada. Es importante seleccionar una contraseña que no sea

fácilmente adivinada y más importante aún, no debe ser compartida con NADIE.

b) Selección de una Contraseña Adecuada

1. A continuación se detallan algunos lineamientos que pueden ayudar a los usuarios al momento de seleccionar una contraseña adecuada, estos lineamientos permiten asegurar que la contraseña sea lo más fuerte posible.

2. Una contraseña fuerte, por su definición en la Internet es una contraseña que es difícil de detectar o adivinar por humanos y programas informáticos, permitiéndole proteger de una manera efectiva los datos.

    - La contraseña seleccionada deberá tener por lo menos ocho caracteres e incluir cualquier combinación de: letras (mayúsculas y minúsculas), números y símbolos (@, #, $, %, etc.). Haciendo uso de la complejidad de las contraseñas en las redes.
    - No utilice su información personal: Nombres, apellidos, fechas de nacimiento, números de documentos, etc. como contraseña.
    - Evite la utilización de contraseñas secuenciales: 123456, abc123, xyz789, etc.
    - Utilice una contraseña que le sea fácil de recordar, utilice combinaciones de caracteres mencionados anteriormente. Y si lo considera necesario guarde una copia de esta en papel, en un lugar seguro y no accesible por otras personas.

c) Cambio de Contraseña

1. La División Desarrollo de Tecnologías de la Información y Comunicación ha establecido que las contraseñas de usuario tienen una validez de 30 días, transcurridos los cuales el usuario deberá cambiarla, tomando en cuenta las siguientes indicaciones:

    - La contraseña nueva no podrá ser igual a la contraseña que ha caducado.
    - La contraseña no podrá ser igual a cualquiera de las ultimas 12 contraseñas utilizadas.
    - Es responsabilidad del usuario cambiar la contraseña cuando el periodo de validez de esta ha terminado, así como cambiarla en el primer ingreso a la red, luego que ha solicitado a la Sección

Asistencia, Mantenimiento y Soporte Tecnológico o al Técnico de Mantenimiento y Soporte Tecnológico el reseteo de ella.

- Toda persona que haya olvidado su contraseña, deberá comunicarse con el Técnico de Mantenimiento y Soporte Tecnológico de su centro de atención o con la Sección Asistencia, Mantenimiento y Soporte Tecnológico en el caso de la Torre Administrativa y todas aquellas dependencias que no cuentan con Técnico de Mantenimiento y Soporte Tecnológico asignado.

2. Toda persona que haya olvidado su contraseña, deberá solicitar por medio de requerimiento, su reseteo de la clave a la Sección Asistencia, Mantenimiento y Soporte Tecnológico de la División Desarrollo de Tecnologías de la Información y Comunicación a los teléfonos 2268-3166 y 2268-3418 o por medio de correo electrónico.

3. Para los usuarios en los siguientes cargos : Dirección General, Sub Dirección General, Sub Dirección de Salud, Sub Dirección Administrativa y Asesores , la contraseña del usuario de dominio nunca deberá expirar debido a las obligaciones requeridas, según las funciones de cada cargo.

4. Para los usuarios Administradores, la contraseña no deberá expirar debido a las diferentes programaciones de eventos que son requeridos a nivel de sistema operativo en los servidores críticos.

d) Cambio de Requerimientos de Contraseñas

1. La División Desarrollo de Tecnologías de la Información y Comunicación puede cambiar el periodo de validez de contraseñas de usuario, la longitud mínima de la contraseña y la cantidad de contraseñas que no podrán repetirse según lo crea conveniente. Una vez tomada la decisión, se deberá informar a los usuarios por medio de correo electrónico con al menos una semana de anticipación antes de implementar el cambio. Los Técnico de Mantenimiento y Soporte Tecnológico y jefaturas a nivel nacional, deben informar de dicho cambio a todos los usuarios de red que no posean correo electrónico.

16.4 POLÍTICAS DE SEGURIDAD FÍSICA

a) Acceso Físico

1. Las puertas de acceso y paredes del área deben ser seguras, se debe limitar la entrada con cerraduras o algún otro sistema de seguridad para restringir los accesos a personal no autorizado al ingreso a las instalaciones, así como estas deben permanecer cerradas, y las llaves o controles de acceso, deberá tenerlas únicamente la Sección Administración de Bases de Datos y Sistemas Operativos.

2. Las instalaciones físicas del centro de cómputo serán áreas restringidas, únicamente podrán ingresar personas autorizadas, es decir personal que la División Desarrollo de Tecnologías de la Información y Comunicación defina, personal de mantenimiento de equipo que se presente a realizar labores de mantenimiento.

3. Se deberá llevar una bitácora de entrada/salida, de todas las personas que visiten el centro de cómputo. Quedan exentos de esta medida el Director General del ISSS, los Subdirectores del ISSS, Jefe de la División Desarrollo de Tecnologías de la Información y Comunicación, Jefe de la Sección Administración de Bases de Datos y Sistemas Operativos, el personal permanente, interino, por contrato, horas sociales o cualquier otra forma de relación laboral de la Sección Administración de Bases de Datos y Sistemas Operativos, personal de vigilancia, limpieza y mantenimiento destacados para el centro de cómputo, y el personal que la División Desarrollo de Tecnologías de la Información y Comunicación considere conveniente para los intereses del ISSS.

4. Solo el personal de la Sección Administración de Bases de Datos y Sistemas Operativos está autorizado para mover, cambiar o extraer equipo de cómputo del centro de atención a través de identificaciones y formatos de Entrada/Salida. La Sección Administración de Bases de Datos y Sistemas Operativos podrá autorizar a terceros realizar las actividades definidas en este apartado, si así lo considera conveniente para los intereses del ISSS.

b) Protección Física

1. El centro de cómputo debe recibir limpieza todos los días, que permita mantenerse libre de polvo, debe contar por lo menos con un extinguidor de incendio adecuado y cercano, contar con señalización

del área, disponer de suficiente espacio físico para área de trabajo, cuando se revise equipo para mantenimiento.

2. Se debe contar con las medidas de seguridad física mínimas recomendadas por los fabricantes de Hardware de las marcas de equipos que se encuentren en el centro de cómputo. Es decir, aire acondicionado, UPS, limpieza, etc.

3. Los equipos de cómputo y comunicación deberán estar protegidos con UPS, de preferencia en línea para contrarrestar los cambios de voltaje existentes por la red energética.

4. Todos los equipos de cómputo deberán conectarse a tomas corrientes polarizados.

5. Si luego de la revisión de un equipo reportado con problemas, se detectare que ya no tiene reparación, el personal de la División Desarrollo de Tecnologías de la Información y Comunicación o la empresa contratada para Mantenimiento Preventivo y Correctivo, deberá hacer nota técnica para proceder al descarte del equipo, haciendo uso del formato que esté vigente según la normativa de descartes, dejando copia de dicho documento.

16.5 SAFISSS

1. La creación de usuarios de SAFISSS deberá ser solicitada por medio de correo electrónico del jefe de Sección Asistencia, Mantenimiento y Soporte Tecnológico, detallando el nombre completo del recurso, número de empleado, justificación de la creación y centro de costo del área. La Sección Asistencia, Mantenimiento y Soporte Tecnológico notificará al jefe de Departamento Desarrollo de Sistemas de Información o al jefe de Sección Análisis, Diseño, Desarrollo y Mantenimiento de Sistemas para su evaluación y atención del requerimiento.

   Para los usuarios en los siguientes cargos: Dirección General, Sub Dirección General, Sub Dirección de Salud, Sub Dirección Administrativa y Asesores, no será requerido para la creación de usuarios en SAFISSS la documentación que ampare dicha creación debido al grado de sus puestos y ocupaciones.

2. La jefatura del Departamento Desarrollo de Sistemas de Información o jefe de Sección Análisis, Diseño, Desarrollo y Mantenimiento de Sistemas,

establecerá la estructura conveniente para la definición de un usuario en el SAFISSS; para clientes internos la estructura del nombre de usuario es el número de empleado y para los clientes externos se define un nombre diferente. Así como la contraseña inicial para nuevo usuarios y reseteo de contraseñas.

3. La extensión de vigencia de usuarios temporales o suspensión permanente en el SAFISSS deberán ser gestionadas por medio de la Sección Asistencia, Mantenimiento y Soporte Tecnológico considerando la forma de comunicación definida en el numeral dos de este literal.
4. La contraseña no podrá ser igual a las ultimas 5 contraseñas utilizadas.

5. La longitud de la contraseña de usuario es de 8 caracteres.

6. Los roles creados en el sistema SAFISSS se construyen de acuerdo a las funciones que realiza el usuario en su puesto de trabajo.

7. Los roles asignados en el SAFISSS son autorizados por los jefes de las áreas propietarios de los módulos, por lo que pueden tener más de un rol asignado, según sea necesario para ejercer sus funciones.

17. CENTROS DE CÓMPUTO DE CENTROS DE ATENCIÓN

17.1 INTRODUCCIÓN

Las políticas de seguridad en centros de cómputo tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información, equipos de cómputo, sistemas de información, redes de Datos y personas que interactúan haciendo uso de los servicios asociados a ellos.
La División Desarrollo de Tecnologías de la Información y Comunicación a través del Coordinador de Mantenimiento y Soporte Tecnológico de Centros de Atención es quien dará a conocer estas políticas de seguridad a todo Técnico de Mantenimiento y Soporte Tecnológico de centros de cómputo del ISSS.

RESPONSABLES:	SECCIÓN COMUNICACIONES, SEGURIDAD Y REDES

17.2 POLÍTICAS DE SEGURIDAD FÍSICA

a) Acceso Físico

1. El buen funcionamiento de los recursos informáticos asignados para almacenamiento y resguardo, dependerá de las condiciones físicas adecuadas que se asignen. Para ello se deberá contar con una ventilación adecuada, instalaciones no magnetizadas y áreas libres de polvo.

2. El acceso físico es importante, todos los equipos deben de estar protegidos del acceso no autorizado.

3. Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario final no tenga acceso físico directo. Entendiendo por sistema de comunicaciones: el equipo activo y los medios de comunicación.

4. El acceso a las instalaciones físicas del centro de cómputo, serán áreas restringidas, únicamente podrán ingresar personas autorizadas, es decir personal de la División de Desarrollo de Tecnologías de la Información y Comunicaciones del ISSS, personal de mantenimiento de equipo que se presente a realizar labores de mantenimiento.

5. Se deberá llevar una bitácora de entrada/salida, de todas las personas que visiten el centro de cómputo (Ver Anexo No. 3).

6. Solo el Técnico de Mantenimiento y Soporte Tecnológico en las unidades médicas, centros hospitalarios y personal de mantenimiento de equipo de la División Desarrollo de Tecnologías de la Información y Comunicación está autorizado para mover, cambiar o extraer equipo de cómputo del centro de atención a través de identificaciones y formatos de Entrada/Salida (Ver Anexo 1).

7. El resguardo de los equipos de cómputo deberá quedar asignado a la persona que lo usa o administra, permitiendo conocer siempre la ubicación física de los equipos.

b) Protección Física

1. Las puertas de acceso, así como las paredes que del área deben ser seguras, se debe limitar la entrada con dispositivos, o instalar cerraduras de combinación para restringir los accesos a personal no autorizado al

ingreso a las instalaciones, así como estas deben permanecer cerradas, y las llaves deberá tenerlas únicamente el Técnico de Mantenimiento y Soporte Tecnológico.

2. El centro de cómputo debe recibir limpieza todos los días, que permita mantenerse libre de polvo, debe contar por lo menos con un extinguidor de incendio adecuado y cercano, que cuente con detectores de humo y en buen estado, que se les de mantenimiento, contar con señalización del área, disponer de suficiente espacio físico para área de trabajo cuando se revise equipo para mantenimiento.

3. Los equipos de cómputo y comunicación deberán estar protegidos con UPS de preferencia en línea para contrarrestar los cambios de voltaje existentes por la red energética.

4. Todos los equipos de cómputo deberán conectarse a tomas corrientes polarizados, y la red de energía eléctrica deberá ser independiente de la red eléctrica del centro de atención y tiene que estar protegida con conexiones a las plantas de emergencia.

5. Todos los centros de cómputo deben de contar con aire acondicionado independiente, según requerimiento del espacio físico.

6. Los gabinetes de red y Racks deberán permanecer con llave.

7. Todo equipo de cómputo debe ser resguardado por el jefe del área o sección al cual pertenece (Custodio del bien), si este se daña deberá ser retirado por Técnico de Mantenimiento y Soporte Tecnológico, Personal de informática o técnicos de la empresa que en ese momento estén proporcionando el soporte de mantenimiento informático, haciendo uso de formato según Anexo 1 para que quede constancia del movimiento del equipo y la razón por la que se retira.

8. Si luego de la revisión se detectare que ya no tiene reparación, el personal de informática, deberá hacer nota técnica para proceder al descarte del equipo, dicho proceso lo hará el custodio del bien, haciendo uso del formato que esté vigente, según la normativa de descartes, dejando copia de dicho documento al Técnico de Mantenimiento y Soporte Tecnológico.

9. Así mismo los repuestos que se reemplacen quedaran en poder del Técnico de Mantenimiento y Soporte Tecnológico, para que

posteriormente, éste haga el descarte de dichas partes, según formato de descarte de repuestos.

17.3 POLÍTICAS DE SEGURIDAD LÓGICA DE LA RED

El uso de analizadores de red es permitido única y exclusivamente para el Técnico de Mantenimiento y Soporte Tecnológico, Analista de Control de Calidad o personal del Departamento Soluciones Integrales en Tecnologías de la Información y Comunicación de la División Desarrollo de Tecnologías de la Información y Comunicación, para monitorear la funcionalidad de la red.

a) De uso aceptable de los usuarios

1. Los recursos de cómputo empleados por el usuario:
   - Deberán ser afines al trabajo desarrollado.
   - No deberán ser proporcionados a personas ajenas.
   - No deberán ser utilizados para fines personales.

2. Todo usuario debe respetar la intimidad, confidencialidad y derechos Individuales de los demás usuarios.

3. El correo electrónico no se deberá usar para envío masivo, materiales de uso no institucional o innecesarios (entiéndase por correo masivo todo aquel que sea ajeno a la institución, tales como cadenas, publicidad y propaganda comercial, política o social, etcétera).

4. Para reforzar la seguridad de la información de su cuenta, el usuario conforme su criterio, deberá hacer respaldos de su información, dependiendo de la importancia y frecuencia de modificación de la misma.

5. Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor.

6. Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de cómputo y red del ISSS, de acuerdo con las políticas que en este documento se mencionan.

7. Los usuarios deberán solicitar apoyo al Técnico de Mantenimiento y Soporte Tecnológico de su dependencia, ante cualquier duda en el manejo de los recursos de cómputo de la Institución.

b) De los Servidores

1. El Técnico de Mantenimiento y Soporte Tecnológico tiene la responsabilidad de verificar la instalación, configuración e implementación de seguridad, en el servidor conectado a la red.
2. La instalación y/o configuración de todo servidor conectado a la red, deberá ser solicitada a través de una solicitud de servicio al centro de operaciones de la red que proporcionará la División Desarrollo de Tecnologías de la Información y Comunicación.

3. El Técnico de Mantenimiento y Soporte Tecnológico debe normar el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios.

4. La información de los servidores deberá ser respaldada, de acuerdo a los estándares ya establecidos o con los siguientes criterios:
    a) Diariamente,
    b) Semanalmente.
    c) Mensualmente.

5. Los respaldos de documentos personales serán responsabilidad absoluta de los usuarios, no así, los respaldos de los sistemas, son responsabilidad exclusiva del Técnico de Mantenimiento y Soporte Tecnológico.

17.4 POLÍTICAS DE CONTROL Y ADMINISTRACIÓN DE LOS RECURSOS EN LOS CENTROS DE ATENCIÓN Y DE RESPALDOS DE INFORMACIÓN DE LOS SISTEMAS EN SERVIDOR

1. Todo cambio, problema, mantenimiento o suceso detectado en servidor de los centros de atención deberá ser registrado por el Técnico de Mantenimiento y Soporte Tecnológico en la "Bitácora del Servidor" (Ver Anexo 4), detallando las acciones realizadas para la solución del problema.

2. Se respaldarán las carpetas de los diferentes sistemas que estén **instalados localmente y activos** en el momento de la ejecución del respaldo, en el formato "Bitácora de Respaldo de Archivos" (Ver Anexo 5), según los criterios:

    a) Sistema de Laboratorio Clínico: carpetas DATOS, HISTÓRICO, ANUARIO y el contenedor de la Base de Datos.
    b) Sistema Emergencia DOS: carpeta BASES.

c) Sistema de Rayos X: carpetas DATOS y RADIO.
d) Sistema de Odontología: carpeta Odontología.
e) Sistema Registro de tumores: carpeta Bases de datos.
f) Sistema de Maestros: carpeta Bases.
g) Sistema de Área de cotizaciones: carpetas principales.

Se deberán incluir los datos de los sistemas locales de las clínicas comunales adscritas a cada centro de atención, atendido por un Técnico de Mantenimiento y Soporte Tecnológico, en cada material de respaldo enviado para su resguardo. En caso de falta de medios de almacenamiento, se deberán hacer los respaldos en el servidor FTP asignado para tal fin, en la División Desarrollo de Tecnologías de la Información y Comunicación.

3. El Técnico de Mantenimiento y Soporte Tecnológico deberá completar la "Hoja de Control de Respaldos" (Anexo 6), de forma diaria, semanal y mensual en el momento que realice el respaldo de la información contenida en los CD´s, los cuales deberán ser entregados a la Sección Asistencia, Mantenimiento y Soporte Tecnológico periódicamente para su resguardo.

4. El Técnico de Mantenimiento y Soporte Tecnológico anotará en la "Bitácora de Respaldo de Archivos" (Anexo 5), el periodo a respaldar, material utilizado para llevar a cabo el respaldo y el detalle de la información contenida.

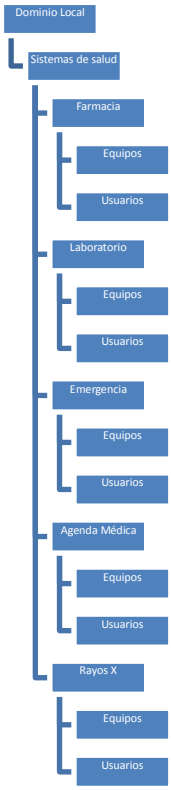
5. El Coordinador de Mantenimiento y Soporte Tecnológico de los Centros de Atención, deberá completar formulario "Control y Administración de Recursos" (ver anexo 7), en cada visita realizada a los diferentes centros de cómputo, donde se tenga asignado por lo menos un Técnico de Mantenimiento y Soporte Tecnológico.

17.5 DIRECTORIO ACTIVO Y CARPETAS DE APLICACIONES

1. La estructura de Directorios, y de Directorio Activo, será por medio de Contenedores, bajo el esquema siguiente:

   - **Directorio Activo**

     Como parte de la Organización Institucional de cada centro de atención se crearan Unidades Organizativas, y se nombraran según las aplicaciones que se instalaran, así como se muestra en el esquema.



2. Las Unidades Organizativas estarán divididas en sub unidades, las que corresponderá a los sistemas que se tengan instalados. Grupos, que serán nombrados según el área de desarrollo, estas pueden variar según necesidades de cada dependencia.

3. Los usuarios pertenecerán a grupos según área de trabajo donde aplique según sus funciones.

4. La cuenta Administrador tiene que estar renombrada, con conocimiento del Técnico de Mantenimiento y Soporte Tecnológico, de la cual hace uso para la realización de sus tareas en el sistema.

5. En los centros de cómputo de los diferentes centros de atención, se deberá completar el formulario "Bitácora de Creación de Usuarios" y "Bitácora de Creación de Grupos", en donde se llevará un control de los usuarios con acceso a la red Institucional. (Anexo 8 y Anexo 9 respectivamente)

- **Diagrama de Red de Datos.**

6. Cada Técnico de Mantenimiento y Soporte Tecnológico deberá realizar un diagrama de red de su centro de atención, elaborado en el software que proporcione la División Desarrollo de Tecnologías de la Información y Comunicación, dicho diagrama deberá cumplir con las siguientes especificaciones:

- Nombre de la localidad, la fecha de creación, fecha de modificación.

- Los diagramas lógicos, como físicos deberán contener tanto los dispositivos pasivos como los activos con sus respectivas ubicaciones, puertos utilizados, puertos vacíos etc.

- Deberán de mantenerse en medio electrónico e impreso.

- El mapa de cada dispositivo deberá contener: Nombre del Dispositivo, u otra información que identifique la ubicación física del dispositivo como tal.

- El equipo activo debe de ser representado con figuras de acuerdo a los estándares proporcionados por la División Desarrollo de Tecnologías de la Información y Comunicación, para diferenciarlo (SWITCH, HUB, ROUTER, Servidores etc.)

- En el diagrama deberá diferenciarse los medios utilizados como cobre, Fibra Óptica, satélite, y otros.

- **Inventario de Equipo Informático**

7. Cada Técnico de Mantenimiento y Soporte Tecnológico deberá mantener un inventario de equipo Informático, en el que pueda identificarse fácilmente movimientos de entrada salida, características de los equipos, descartes, etc.

8. El inventario deberá de actualizarse 2 veces al año, en los meses de mayo y noviembre, de los cuales se tiene que enviar informe al Coordinador de Mantenimiento y Soporte Tecnológico de los Centros de Atención y a la jefatura de la Sección Asistencia, Mantenimiento y Soporte Tecnológico, ambos de la División Desarrollo de Tecnologías de la Información y Comunicación.

9. El formato de inventario se estará utilizando el que se genere a través del sistema de inventario desarrollado para tal fin o el establecido en una hoja electrónica.

17.6 DIRECCIONAMIENTO IP, EN CENTROS DE ATENCIÓN

La asignación de direcciones IP en toda Red de Datos del ISSS, deberá regirse bajo el estándar siguiente:
Asignación de direcciones IP, de manera automatizada, mediante la utilización de DHCP (Dinamic Host Configuration Protocol), bajo los parámetros siguientes:
El rango de direcciones IP, será asignada por la División Desarrollo de Tecnologías de la Información y Comunicación.

Direcciones a excluir de rango IP:

- XXX.XXX.XXX.1 hasta XXX.XXX.XXX.4
  Switch que necesite asignación de IP.

- XXX.XXX.XXX.5
  Será asignada a router (Gateway).

- XXX.XXX.XXX.6 hasta XXX.XXX.XXX.9
  Serán asignadas a los Servidores antivirus, de actualizaciones.

- XXX.XXX.XXX.10 hasta XXX.XXX.XXX.11
  Serán asignadas a los Servidores de aplicaciones.

- XXX.XXX.XXX.12 hasta XXX.XXX.XXX.14
  Serán asignadas a las computadoras del Técnico de Mantenimiento y Soporte Tecnológico.
- XXX.XXX.XXX.15 hasta XXX.XXX.XXX.16
  Serán asignadas a las computadoras del sistema marcador biométrico.

- XXX.XXX.XXX.17 hasta XXX.XXX.XXX.20
  Disponibles para dispositivos que necesiten dirección IP (impresores Ups, etc.).

- XXX.XXX.XXX. 31 Hasta XXX.XXX.XXX.254
  Direcciones a distribuir en la red de datos, mediante DHCP.

- Este será el rango de direcciones a distribuir en la red de Datos, mediante DHCP.

- Aquellas direcciones que por requerimientos de aplicativos se necesiten sean fijas, serán asignadas por la entidad que lo solicite.
- En los centros de atención donde se encuentren redes informáticas pequeñas o que no se cuente con un servidor, se utilizarán distribución de IP estáticas.
- Los centros de atención donde la asignación de IP asignadas a las computadoras no sea suficiente, se deberá crear subredes a efectos de lograr cubrir todas las computadoras, según lineamientos proporcionados por la División Desarrollo de Tecnologías de la Información y Comunicación.

17.7 SEGURIDAD EN SISTEMA OPERATIVO DE RED

El sistema operativo de red, debe de configurarse de acuerdo la los parámetros siguientes.

PARÁMETROS RECOMENDADOS DE CONFIGURACIÓN DEL SISTEMA OPERATIVO DE RED.

Cuentas por Omisión	Valores Recomendados
Invitado (Guest)	Eliminada o Deshabilitada y renombrada
Administrador (Administrator)	Renombrada y con password cambiado

Políticas de Contraseñas	Valores Recomendados
Duración mínima de Contraseña (Minimun Password Age)	1 Día
Duración máxima de Contraseña (Máximum Password Age)	30 Días
Tamaño mínimo de Contraseña (Minimun Password Lenght)	Se recomienda para usuarios comunes Claves mayores a 8 caracteres y para usuarios privilegiados, como Administradores, claves mayores de 12 caracteres
Complejidad de Requerimientos (Complexity requirements)	Habilitado (Enabled)

Bloqueo de Cuentas	Valores Recomendados
Duración de Bloqueo de Cuentas (Account Lockout Duration)	15 minutos
Umbral de Cierre de la Cuenta (Account Lockout Threshold)	3 intentos inválidos de acceso
Tiempo de Reseteo del Contador de Bloqueo (Reset account lockout counter after)	15 minutos
Políticas de Auditoría	**Valores Recomendados**
Auditar Eventos de Acceso de Cuenta (Audit Account Logon Events)	Debe registrar los accesos exitosos y fallidos (success, failure)
Auditar Administración de Cuentas (Audit Account Management)	Debe registrar los accesos exitosos y fallidos (success, failure)
Auditar Eventos de Acceso (Audit Logon Events)	Debe registrar los accesos exitosos y fallidos (success, failure)
Auditar el Acceso a Objetos (Audit Object Access)	Debe registrarse los accesos fallidos (failure)
Auditar el Acceso de Servicio de Directorio (Audit Directory Service Access)	No auditar para Workstation y servidores miembros. Auditar los intentos fallidos para Controladores de Dominio (Domain Controllers)
Auditoria de Cambio de Politicas (Audit Policy Change)	Debe registrar los accesos exitosos y fallidos (success, failure)
Auditar el Uso de Privilegios (Audit Privilege Use)	Debe registrarse los accesos fallidos (failure)
Auditar el Seguimiento de Procesos (Audit Process Tracking)	Se recomienda tenerlo en la opción "No Auditing"
Auditar Eventos de Sistema (Audit System Events)	Debe registrar los accesos exitosos y fallidos (success, failure)

Políticas de Usuarios	Valores Recomendados
Cambiar Clave al siguiente Acceso	Seleccionarla cuando se crea un

Políticas de Usuarios	Valores Recomendados
(Change Password at next Logon)	nuevo usuario, cuando se activa uno ya existente o cuando se ha reestablecido su clave.
El Usuario no puede cambiar Clave (Usser cannot change Password)	Esta opción no tiene que estar seleccionada (Excepto para el usuario Guest)
La clave nunca expira (Password never expires)	Esta no tiene que estar seleccionada
Campos informativos del usuario deben estar llenos	Corroborar que dichos campos no estén vacíos

Asignaciones de Derechos de Usuarios	Valores Recomendados
Accesar está computadora desde la Red (Acces this computer from the network)	En los Domain Controllers deben incluirse solamente Administradores y usuario autenticados.
Agregar Estaciones de Trabajo a Dominios (Add Workstation to Domain)	No tiene que darse este derecho explícitamente. Los usuarios Administradores y Operadores de Grupos ya tienen esta habilidad
Respaldar Archivos y Directorios (Backup Files and Directories)	Esta facultad solo la deben tener los administradores y operadores de copia si existen
Quitar la Comprobación de Recorrido (Bypass Traverse Checking)	Esto solo lo deben tener los Administradores
Cambiar la hora del Sistema (Change the System time)	Solo Administradores y usuarios seleccionados por el mismo
Forzar apagado desde un sistema remoto (Force shutdown from a remote system)	Solo los Administradores lo deberían hacer
Cargar y retirar Manejadores de Dispositivos (Load and unload Device Drivers)	Solo los Administradores lo deberían hacer
Accesar localmente (Log on locally)	Solo los Administradores y los Operadores de copia deberían tener

Políticas de Usuarios	Valores Recomendados
	este privilegio
Administrar el Registro de Auditoria y Seguridad (Manage Auditing and Security Log)	Los administradores tienen este derecho por omisión y ellos pueden elegir a quien más se le permite.
Restaurar Archivos y Directorios (Restore Files and Directories)	Los administradores tienen este derecho y pueden asignarse a Operadores de copia si es necesario
Apagar el Sistema (Shut down the System)	Los administradores tienen este derecho y estos pueden decidir a quien más se le asigna.

Opciones de Seguridad	Valores Recomendados
Restricciones adicionales para Conexiones Anónimas (Additional Restrictions for Anonymous Connections)	Tiene que removerse los grupos "Everyone" y "Network". La opción que tiene que seleccionarse es: "No obtener acceso sin permisos anónimos explícitos" (No access without explicit anonymous permissions)
Permitir apagar el Sistema sin iniciar sesión (Allow system to be shut down without having to log on)	Por omisión en Windows Server viene **deshabilitado (disabled)** y se recomienda mantenerlo así.
Tiempo de Inactividad requerido antes de desconectar Sesión (Amount of idle time required before disconnecting session)	Se recomiendan 30 minutos
Deshabilitar el requisito de presionar Ctrl+Alt+Supr para iniciar sesión (Disable CTRL+ALT+DEL requirement for logon)	Se recomienda que esté **deshabilitada (disabled)**
No mostrar el nombre de último usuario en la pantalla de inicio de sesión	Se recomienda **habilitar (enabled)** esta opción

Opciones de Seguridad	Valores Recomendados
(Servers do not display last user name in logon screen)	
Pedir a usuario cambiar la contraseña antes de que caduque (Prompt user to change password before expiration)	Se recomiendan 14 días
Renombrar Cuenta de Administrador (Rename Administrator Account)	Evitar nombres obvios como "admin" o "root" y cambiar o eliminar la descripción original de la cuenta
Renombrar cuenta Invitado (Rename Guest Account)	Se recomienda eliminar o renombrar esta cuenta, cambiar password y mantenerla deshabilitada.
Restringir el acceso a CD-ROM a usuarios con sesión iniciada localmente (Restrict CD-ROM access to locally logged-on user only)	Se recomienda mantenerla deshabilitada
Restringir el acceso a unidad de disquete a usuarios con sesión iniciada localmente (Restrict floppy access to locally logged-on user only)	Se recomienda mantenerla deshabilitada

Registro de Sucesos	Valores Recomendados
Tamaño Máximo del Registro de Aplicación (Maximun application log size)	Los rangos permitidos están entre 64 KB to 4,194,240 KB., se recomienda dar un tamaño de 4,194,240 Kbytes
Tamaño Máximo del Registro de Seguridad (Maximun security log size)	
Tamaño Máximo del Registro de Sistema (Maximun system log size)	
Restringir Acceso del invitado al Registro de Aplicación	Tener habilitada (enabled) esta opción restringe que usuarios INVITADOS

Registro de Sucesos	Valores Recomendados
(Restrict Guest Access to Application Log)	puedan ver estos registros
Restringir Acceso del invitado al Registro de Seguridad (Restrict Guest Access to Security Log)	
Restringir Acceso del Invitado al Registro de Sistema (Restrict Guest Access to System)	
Conservar el Registro de Aplicaciones (Retain Application Log)	Esta opción no debe ser configurada, pues ningún evento debe ser reemplazado.
Conservar el Registro de Seguridad (Retain Security Log)	
Conservar el Registro de Sistema (Retain System Log)	
Método de Retención del Registro de Aplicación (Retention Method for Application Log)	Los registros no deben ser sobre escritos, se recomienda limpiarlos manualmente
Método de Retención del Registro de Seguridad (Retention Method for Security Log)	
Método de Retención del Registro de Sistema (Retention Method for System Log)	

17.8 CREACIÓN Y NOMBRAMIENTO DE CUENTA DE USUARIO

Se deben aplicar los mismos criterios listados en el numeral 15.2.

17.9 SEGURIDAD

Se deben aplicar los mismos criterios listados en el numeral 15.3.

a) Protección de los Datos

1. El Técnico de Mantenimiento y Soporte Tecnológico es responsable de asignar permisos a los archivos, carpetas, discos, impresores o cualquier otro recurso de la computadora asignada a otros usuarios.

2. Los derechos serán proporcionados según los requerimientos de las aplicaciones y sistemas instalados.

3. Por omisión todas las computadoras están configuradas de manera que todos los archivos, carpetas, discos, impresores o cualquier otro recurso son únicamente accesibles por el usuario que la utiliza.

b) **Uso de Software Bajo Licencia**

1. La División Desarrollo de Tecnologías de la Información y Comunicación proveerá acceso a una serie de software con licencia que podrá ser instalado en equipos institucionales siguientes: Servidores, Computadoras Personales, Laptops, Tablet PC y Smart Phones.

2. El software y documentación bajo licencia y derechos de copia, no podrá ser duplicado a menos que la licencia explícitamente establezca que puede ser copiado. Sólo la División Desarrollo de Tecnologías de la Información y Comunicación puede mantener copias de dicho software, para proteger los medios originales.

3. El copiar software a cualquier tipo de medio o a un equipo informático no autorizado, no solo constituye una violación a esta política sino también una violación a leyes y tratados internacionales.

4. Es responsabilidad de la División Desarrollo de Tecnologías de la Información y Comunicación proporcionar a los Técnico de Mantenimiento y Soporte Tecnológico software (Sistemas Operativos, ofimática y aplicativos) con licencia autorizada al ISSS, para que sea instalado en la dependencia que sea requerido. Esto se limita al software que según las necesidades y capacidades institucionales ha sido adquirido.

18. SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

UNIDAD RESPONSABLE:	DEPARTAMENTO DESARROLLO DE SISTEMAS DE INFORMACIÓN. DEPARTAMENTO SOLUCIONES INTEGRALES EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN.

18.1 OBJETIVO

Definir las políticas relativas a la seguridad mínima de acceso que deben tener los sistemas de información que se desarrollen en el Instituto.

18.2 POLÍTICAS

1. Todos los sistemas deberán iniciar sesión con el registro y validación, como mínimo, del nombre del usuario y su respectiva contraseña.

2. No se debe desplegar el listado de usuarios disponibles, para evitar que se pueda seleccionar cualquiera e intentar encontrar la contraseña. Tampoco se debe mostrar la contraseña que se está ingresando.

3. Los intentos fallidos para acceder al sistema al ingresar la contraseña incorrecta será de 3. Una vez agotados estos tres intentos se bloqueará el usuario y se cerrará la interfaz de acceso al sistema.

4. Cuando un usuario no exista o la clave sea incorrecta se debe colocar el mensaje del tipo "El usuario y la clave deben ser los correctos", evitando los mensajes que den la pauta para conocer información acerca de los usuarios.

5. Los sistemas deberán contar con opciones y controles para la administración de: usuarios y contraseñas; nombres completos de los usuarios; inactividad de usuarios; encriptación de contraseña; vencimiento, repetición y cambios de contraseñas; y perfiles o niveles de acceso.

6. El nombre de usuario del sistema debe contener 7 caracteres, para usuarios internos se deberá utilizar exclusivamente el número de empleado y para usuarios externos como entes contralores se aplicará la siguiente regla de acuerdo a la existencia de usuarios creados y clasificado como activo: Primera letra del primer nombre más primer apellido, o Primera letra del

segundo nombre más primer apellido, o Primera letra del primer nombre más segundo apellido, o Primera letra del segundo nombre mas segundo apellido.
Para el caso de la contraseña ésta debe contener 6 caracteres como mínimo y máximo 10, debiendo incluir de forma obligatoria la combinación de letras (mayúsculas y minúsculas) y número.

7. El periodo máximo de uso de una misma contraseña debe ser de 30 días.

8. Se debe establecer un ciclo de uso de contraseñas de 12 ocurrencias mínimo (no debe de repetirse las últimas 12 contraseñas), a excepción de SAFISSS.

9. Los perfiles o niveles de acceso de los usuarios de los sistemas deberán asignarse de acuerdo a las funciones y autorizaciones; y estos deben ser definidos por el responsable jerárquico que se determine en cada dependencia, no por el personal de Informática.

10. Podrán existir usuarios y perfiles o niveles de acceso para personal de la División Desarrollo de Tecnologías de la Información y Comunicación que brinda soporte a los sistemas.

11. Los sistemas deben incluir la administración de una bitácora de eventos.

12. Un sistema no debe permitir más de una sesión activa por usuario.

13. En caso de requerir la autorización de usuarios que consultarán los sistemas que funcionan para 1 ó más centros o dependencias, se podrá crear usuarios de consulta que deben ser autorizados por el responsable de la información y no deben establecerse con fines de actualización (ingreso, eliminación y modificación).

14. Todas las cuentas con permiso de ingreso, eliminación o modificación de información deben ser de carácter personal y sus contraseñas deben seguir los parámetros establecidos en las políticas de este manual.

15. Las cuentas consideradas de Administración (con derechos de creación/mantenimiento de usuarios) deben limitarse a 2 cuentas por sistema por centro de atención o dependencia. En caso de requerir más de lo establecido, deben ser autorizadas por la máxima autoridad del centro, dependencia o las autoridades centrales.

16. Para las cuentas de usuarios de los sistemas administrados por la División Desarrollo de Tecnologías de la Información y Comunicación, se utilizará el número de empleado.

19. ESTÁNDARES PARA EL DISEÑO Y DESARROLLO DE BASES DE DATOS ORACLE

19.1 INTRODUCCIÓN

Este documento describe los estándares a ser usados en el diseño y desarrollo de bases de datos en el Instituto Salvadoreño del Seguro Social.

Las aplicaciones del Instituto Salvadoreño del Seguro Social deberán utilizar como base de datos ORACLE o SQL Server, y los estándares para este RDBMS (Sistema Relacional de Gestión de Base de Datos, por sus siglas en inglés) son cubiertos en este documento.

19.2 RESPONSABILIDADES

La administración diaria (incluyendo backups) serán realizados por el equipo de administración de bases de datos.

Los desarrolladores de aplicaciones son responsables de producir el esquema de la base de datos, scripts de creación, código, diseño del esquema, otros objetos de la base de datos y documentación del código.

19.3 ARQUITECTURA Y DISEÑO

Usuarios

ORACLE.
Esquemas y usuarios.
En Oracle, la autenticación del sistema operativo NO DEBERÁ ser utilizada para los usuarios de las aplicaciones.

19.4 TABLAS

Nombres de Tablas

- Se utilizará únicamente caracteres alfanuméricos y el guión bajo (_) para los nombres de las tablas.
- Los nombres de las tablas no deberán iniciar con números o símbolos especiales (#,$,%,&,ñ, Ñ u otros).
- Los nombres de las tablas deben estar compuestos por 30 caracteres o menos.

Oracle

- Los nombres de las tablas en Oracle no son sensibles a la capitalización o a la plataforma, y por consistencia deberán ser definidos en mayúsculas.

Nombres de campos

- Se utilizará únicamente caracteres alfanuméricos y el guión bajo (_) para los nombres de los campos.
- Los nombres de los campos no deberán iniciar con un digito.
- Los nombres de los campos no deberán iniciar con números o símbolos especiales (#,$,%,&,ñ, Ñ u otros).
- Los nombres de los campos deben estar compuestos por 30 caracteres o menos.
- No se deberán utilizar palabras reservadas de SQL como nombres de campos.

19.5 ÍNDICES

Índices/constraints y desempeño

- Identificar las llaves primarias, únicas y foráneas (para reforzar la integridad de data importante o crítica) como parte inicial del proceso de diseño.

- Para evitar las consultas lentas y la degradación del desempeño en la base de datos, las consultas más comúnmente ejecutadas deberán ser analizadas con un "Explain Plan".

- Los índices deberán ser utilizado donde convenga, y se deberá utilizar un "Explain Plan" para justificarlos.

19.6 TABLESPACES

Almacenamiento blob/clob

- Si se está utilizando una cantidad considerable de almacenamiento BLOB/CLOB, o el volumen de acceso a campos BLOB/CLOB es bastante grande, se deberá solicitar un tablespace independiente para el almacenamiento de estos objetos BLOB/CLOB.

Creación de Índices

- Deberá ser requerido o definido en los scripts de creación de esquema que los índices sean creados en un tablespace diferente al de las tablas de la aplicación.

Interfaces

- Todas las APIs (Interface de programas de aplicación, por sus siglas en ingles) de la base de datos deberán contener manejo de errores y notificación de éxito y/o fracaso de las sentencias.
- Cuando se accese a la base de datos utilizando código JAVA se recomienda utilizar JDBC.
- Cuando se accese a la base de datos desde lenguajes diferentes a PL/SQL se deberá utilizar OCCI para Oracle.
- ODBC podrá ser utilizado para conectarse a las bases de datos de Oracle solamente si no existe otra alternativa.
- Se deberá utilizar listas de conexiones donde sea posible y/o apropiado para reducir el costo de inicialización y destrucción de conexiones desde los clientes o código de capa intermedia hacia los servidores de base de datos.

Almacenamiento

- La asignación de tablespaces para todos los objetos de los esquemas de Oracle DEBERA ser especificado en todos los scripts de creación de esquemas. Esto permite que las tablas, índices y opcionalmente los objetos grandes sean almacenados separadamente, mejorando potencialmente el desempeño de las aplicaciones y de todo el sistema.

Encriptamiento

- El encriptamiento DEBERA ser utilizado para el almacenamiento de palabras clave. de preferencia TripleDes.

Replicación

- Cualquier requerimiento de replicación deberá ser discutido con el equipo de administración de base de datos.

19.7 DESARROLLO

Carga de Datos

- Cualquier proceso de carga de datos DEBERA crear un registro resumen y de errores (en el evento de algún error) y un archivo de registros malos para aquellos registros que no fuesen cargados durante el proceso.
- Se deberá considerar un método de recuperación para aquellos procesos de carga que fallan en un punto intermedio de su ejecución ya sea a través de puntos de COMMIT o de alguna otra técnica de revisión.

19.8 ESTÁNDARES DE CODIFICACIÓN

Generales

- El código generado en la base de datos deberá estar siempre orientado a ser: claro, conciso, consistente y comentariado.

Seguridad

- Los usuarios de la base de datos deberán ser otorgados con los privilegios suficientes para permitirles realizar las tareas que necesitan.
- La conexión desde aplicaciones WEB, deberá realizarse siempre que sea posible a través del mismo usuario. Esto reduce las posibilidades de dejar un hueco en la seguridad y permite que las técnicas de listas de conexión estén más disponibles para el mejoramiento del desempeño.
- Las palabras claves que no utilicen cifrado no deberán ser mostradas en la codificación del lado del cliente.
- Las palabras clave que no utilicen cifrado no deberán ser almacenadas en servidores con acceso público.

Fechas

- Al convertir fechas del tipo de datos interno a formato cadena, el formato "YYYYMMDD HH24:MI:SS" deberá ser utilizado si se requiere ordenar las cadenas resultantes como valores "cronológicos".

Manejo de Errores

- La estrategia para el manejo de errores deberá estar claramente definida para todas las APIs de las bases de datos.

Encabezados

- Todos los scripts y módulos deberán contener un encabezado y un pie que incluyan la descripción de la función principal de dicho script o modulo, el nombre de este, la fecha de última actualización, el autor y ultimo modificador y la versión.
- Todos los procedimientos y funciones deberán contener un encabezado y pie que incluyan una descripción del objetivo de este, parámetros, excepciones emitidas y posibles código de retorno.

Manejo de Cursores

- Todos los recursos de cursores deberán ser liberados después de utilizados.

Manejo de conexiones

- Cuando no se esté utilizando listas de conexiones, todas las conexiones deberán de cerrarse una vez usadas. Cuando se esté utilizando listas de conexiones estas deberán ser liberadas al pool después de su uso.
- Todos los recursos asociados con una conexión utilizada deberán ser explícitamente liberados antes de que la conexión sea cerrada o liberada al pool de conexiones.
- Los recursos deberán ser correctamente liberados cuando ocurra un error o condición de excepción.

Abstracción de la Capa (nivel) de la Base de Datos

- Los detalles de la conexión (servidor, base de datos y servicio) se deben almacenar en archivos de configuración y no deberán estar en el código. Esto permite que el código de conexión a la base de datos sea distribuido a entornos de prueba sin la necesidad de modificación y/o recompilación.

- El código de las aplicaciones deberá hacer uso de un código común de acceso a las bases de datos (capa de abstracción de la base de datos). Esto permite que el código de las aplicaciones sea aislado de cambios inherentes a la información de la conexión a la base de datos y de las correcciones que fuesen hechas, por ejemplo: introducción y/o implementación de listas de conexiones, balanceo de carga, etc.

Paquetes y Procedimientos Almacenados

- Por razones de rendimiento, modularidad y protección de la información, todos los procedimientos almacenados de Oracle deberán ser siempre empacados (Consultar la documentación de PL/SQL para más información).

Mantenimiento

- Todos los cambios de gran envergadura realizados a los esquemas DEBERÁN ser realizados a través de un script. Para todos los cambios necesarios deberá realizarse una guía detallando de forma clara todos los pasos a seguir.

- El área que solicita los cambios es la responsable de definir el script y/o la guía a utilizar.
- El script y/o la guía deberán ser probados en un ambiente de desarrollo o de calidad antes de ser ejecutados en el ambiente de producción.

19.9 DOCUMENTACIÓN

Entregables

- La Sección Análisis, Diseño, Desarrollo y Mantenimiento de Sistemas DEBERÁ entregar un diagrama del diseño físico del esquema al equipo de administración de base de datos para toda base de datos, incluyendo el script de creación del esquema y código en formato digital (No archivo de imagen o documento escaneado).

- Se DEBERÁ proveer de evidencia de pruebas de rendimiento de SQL al entregar el código de aplicación de la base de datos. Los planes de ejecución generados pueden ser incluidos con la documentación de la base de datos.

Comentarios de Tablas y Campos

- Toda tabla deberá contener un comentario o descripción de su propósito y deberá incluirse en el script de creación y en el documento de diseño.

- Todo campo de cada tabla deberá también tener un comentario de campo en el documento de diseño, explicando su propósito, valor por defecto, etc.

19.10 INFRAESTRUCTURA Y CONFIGURACIÓN

Archivado

- Se debe llevar a consideración durante la etapa de diseño la estrategia de archivado.
- Generalmente, a menos que sea requerido específicamente, la data de la base de datos deberá ser archivada y almacenada por un periodo no mayor a 6 o 12 meses desde el momento en el tiempo en que expira su vida activa (o la fecha de archivación).

Respaldo

- En bases de datos en operación se deberá realizar respaldos completos semanalmente y respaldos incrementales diariamente. Cualquier otro requerimiento especifico de respaldo o recuperación

deberá ser discutido con el equipo de administración de la base de datos.
- Deberá llevarse la documentación respectiva de los respaldos realizados.

19.11 DOWNTIME PROGRAMADO

Downtime regular

- No debe existir downtime regular en bases de datos de Oracle en operación, Se deberán realizar respaldos en "caliente".

Downtime planeado

- Se debe notificar a los usuarios con una anticipación de por lo menos 48 horas antes del inicio de cualquier tarea de mantenimiento que requiera que las bases de datos se encuentre fuera de línea. En situaciones normales los usuarios deberán ser informados vía correo electrónico.

19.12 NOMENCLATURA

Puntos de Montaje o Directorios

- Para instalaciones de RAC y/ ASM se deberá hacer uso de las mejores prácticas recomendadas por Oracle o por el proveedor local.

- Para instalaciones sin uso de ASM se deberán crear cuatro directorios/Puntos de montaje, uno para software y tres para los archivos de la base de datos.

- Los directorios/Puntos de montaje deberán ser nombrados usando la siguiente sintaxis: /pm/q/dm.

    - Donde p es una constante de tipo carácter.
    - Donde m es un identificador único de longitud fija (un numero de dos dígitos) utilizado para distinguir cada punto de montaje/directorio.
    - Donde q es un string que denota que data de un tipo de base de datos está almacenado aquí.
    - Donde dm es el valor del parámetro de inicialización DB_NAME (Sinónimo del SID de la instancia).
- El primer directorio/punto de montaje estará reservado para el Software aplicativo de la base de datos.

- El segundo directorio/punto de montaje almacenará los archivos de datos de la instancia.
- El Tercer directorio/punto de montaje almacenara los archivos de registro de REDO de la instancia.
- El cuarto directorio/punto de montaje podrá ser utilizado para tareas administrativas de Restauración, Respaldo, aplicación de scripts.

Ejemplos:
/u02/oradata/test y /u03/oradata/test
(Unix)
\Disk02\OraData\Test y \Disk03\OraData\Test
(Windows)

Tablespaces

- Los nombres de los tablespaces estarán limitados a un máximo de 30 caracteres.
- Cada Sistema o aplicativo contenido en una instancia de base de datos deberán contener por lo menos 2 tablespaces, uno para datos y uno para índices.
- Los nombres de los tablespaces deberán incluir el nombre del esquema contenido en ellos seguido del prefijo _TBL o _IND para indicar si es un tablespace de datos o de índices. Ejemplos: AGENDAMEDICA_TBL, AGENDAMEDICA_IND.
- Los nombres de los archivos de los tablespaces deberán tener un máximo de 20 caracteres más una extensión de 3 dígitos.
    - Los nombres de los archivos deberán ser nombrados utilizando la siguiente sintaxis: tdn.dbf.
    - Donde t: es el nombre del tablespace.
    - Donde d: es el tipo de objetos contenidos en el tablespace, se usara D para datos y X para índices.
    - Donde n: es un número de tres dígitos.

    Ejemplos: AGENDAMEDICA podría tener un archivo de datos llamado AGENDAMEDICAD001.dbf para data y AGENDAMEDICAX001.dbf para índices.

Tablas

- Los nombres de las tablas deberán ser en plural.
- Los nombres no deberán contener espacios, deberá ser dividido utilizando el guión bajo (_), y estar limitado a un máximo de 25 caracteres.
- Si la tabla contiene varias palabras, únicamente la última deberá ser en plural, ejemplos:

- APLICACIONES
- APLICACIÓN_FUNCIONES
- APLICACIÓN_FUNCION_ROLES

– Tablas de referencias cruzadas deberán tener como sufijo _XREF

Triggers

– El nombre de cada trigger deberá seguir la siguiente sintaxis: <nombre_tabla>_<A/D><R/S>_<I/U/D>_TRG
  - Donde <A/D>: significa Antes o Después
  - Donde <R/S>: significa registro o sentencia
  - Donde <I/U/D>: significa Insert, Update o Delete
  - Donde TRG: identifica al objeto como un trigger

Ejemplo: CATALOGO_CUENTAS_ARD_TRG

Campos

– Los nombres de los campos no deberán tener prefijos
– El nombre del campo deberá ser en singular.
– Si el campo es una llave primaria deberá ir seguido por el sufijo _ID
– Si el campo está definido como una implementación de un súper-tipo el nombre deberá ir seguido por el sufijo _TYPE

Vistas

– Para separar las partes del nombre se deberá usar el guión bajo (_)
– El nombre de la vista deberá incluir los nombres de las tablas que se están utilizando.

Secuenciadores

– El nombre deberá ir precedido por una descripción corta del uso del secuenciador.
– Para separar las partes del nombre se deberá utilizar el guión bajo (_).
– El nombre del secuenciador deberá ir seguido por el sufijo _SEQ.
– Si se necesitan múltiples secuenciadores para una misma tabla el sufijo _SEQ deberá llevar un número de dos dígitos que lo identificara, ejemplo: _SEQ01.

Llaves Primarias

– Deberá contener el alias de la tabla.
– Deberá ir seguido por el sufijo _PK.

Llaves Únicas

- Deberá contener el alias de la tabla.
- Deberá ir seguido por el sufijo _UK

Llaves Foráneas

- Deberá contener los alias de las tablas involucradas.
- Deberá ir seguido por el sufijo _FK.

Check Constraints

- Deberá contener los alias de las tablas involucradas.
- Deberá ir seguido por el sufijo _CHK
- Si se necesitan multiple checks para una misma tabla el sufijo _CHK deberá. llevar un número de dos dígitos que lo identificara, ejemplo: _CHK01.

Índices

- Deberá contener el alias de la tabla.
- Deberá tener el sufijo _IDX
- Si el índice es sobre una llave primaria, foránea o única, el sufijo será _PK_IDX, _FK_IDX, _UK_IDX según corresponda.

Funciones, Paquetes, Procedimientos y Cursores

- El nombre no deberá ser mayor a los 30 caracteres.
- Deberá contener como prefijo el nombre corto de la aplicación.
- Como sufijo deberá tener: _PKG para paquetes, _FNT para funciones, _PRC para procedimientos, _CSR para cursores.
- El componente central será un nombre de formato libre que lo identifica o describe.

19.13 INFORMACIÓN ALMACENADA

Información en Campos de Texto Libre

- La información almacenada en campos de texto libre es total responsabilidad del usuario que la introdujo, ya sea por efectos de migración, introducción directa en la Base de datos o uso de un sistema.

Información en Campos Codificados

- La integridad de la información en campos que almacenan códigos o de integridad referencial es responsabilidad del Analista Programador, a menos que la información sea introducida directamente en la Base de Datos sin intervención de un sistema, en cuyo caso ello será responsabilidad del usuario que solicita esta acción, o del que la hace en caso que este tenga la potestad necesaria para ello y no tenga un requerimiento que lo ampare.

20. ESTÁNDAR DESARROLLO CON VISUAL STUDIO.NET

20.1 INTRODUCCIÓN

Este apartado tiene por objetivo ser una guía de los estándares a ser usados en el diseño y desarrollo de sistemas utilizando Visual Studio.Net.

20.2 CONTROLES COMÚNMENTE UTILIZADOS

Para identificar los controles a utilizar en los formularios se colocará el prefijo de acuerdo a la tabla de prefijos para controles comúnmente utilizados abajo detallada y a continuación del prefijo un nombre descriptivo de la función que realiza el control:

Tabla de Prefijos para controles comúnmente utilizados			
Control	**Descripción**	**Prefijo**	**Ejemplo**
Button	Botón de Comando	btn	btnAceptar
CheckBox	Casilla de verificación	chk	chkSoloLectura
DataRepeater	Repetidor de datos	drp	drpUbicacion
DBGrid	Cuadrícula de datos	dgd	dgdTitulos
DirListBox	Cuadro de lista de directorios	dir	dirSource
DriveListBox	Cuadro de lista de unidades	drv	drvDestino
DropDownList	cuadro de lista desplegable	ddl	ddlDepartamentos
DTPiker	Selector de fecha	dtp	dtpEditado
FileListBox	Cuadro de lista de archivos	fil	filOrigen
Área de Identificación	Marco	fra	fraIdioma

F. _____
Ing. José Pedro Rivera Moncada
Jefe División de Desarrollo de Tecnologías de Información y Comunicación

F. _____
Inga. Claudia Jennifer Molina
Jefa de Unidad de Desarrollo Institucional

Fecha de modificación 19/08/2015

Tabla de Prefijos para controles comúnmente utilizados			
Control	**Descripción**	**Prefijo**	**Ejemplo**
Grid	Cuadrícula	grd	grdPrecios
GridView	Cuadrícula enlazada a datos	grd	grdResultados
HScrollBar	Barra de desplazamiento horizontal	hsb	hsbVolumen
Image	Imagen	img	imgIcono
ImageButton	Botón con Imagen incorporada	btn	btnCancelar
ImageList	Lista de imágenes	ils	ilsTodosIconos
Label	Etiqueta	lbl	lblMensajeAyuda
Line	Línea	lin	linVerticial
ListBox	Cuadro de lista	lst	lstCodigos
listView	Lista de Datos	lst	lstTipoTrabajo
ListView	Visor de lista	lvw	lvwEncabezados
MaskTextBox	Cuadro de texto con mascara	msk	mskPedidos
Menu	Menú	mnu	mnuAbrirArchivo
MonthCalendar	Calendario	Cal	calFecha
MS FlexGrid	Cuadrícula MS Flex	msg	msgClientes
MSChart	MS Chart	chr	chrVentasPorRegion
MSComm	Comunicaciones	com	comFax
OLE	Contenedor OLE	ole	oleHojaCalculo
Panel	Panel	pnl	pnlGrupo
PictureBox	Cuadro de imagen	pic	picVGA
PictureClip	Picture Clip	clp	clpBarraHerramientas
RadioButtonList	Opciones de Botón de Radio	rbl	rblGenero
SatusBar	Barra de estado	sta	staFechaHora
Shape	Forma	shp	shpCirculo
Slider	Control deslizante	sld	sldEscala
SSTab	MS Tab	mst	mstPrimero
TabStrip	Fichas	tab	tabOpciones
TextBox	Cuadro de texto	txt	txtApellido
Timer	Cronómetro	tmr	tmrAlarma

Tabla de Prefijos para controles comúnmente utilizados			
Control	Descripción	Prefijo	Ejemplo
ToolBar	Barra de herramientas	tlb	tlbAcciones
Tooltip	Mensaje al usuario	Tip	tipNombre
TreeView	Visor de árbol	tre	treOrganizacion
UpdateProgress	Barra de progreso	upd	updCargarArchivo
UpDown	UpDown	upd	updDireccion
VScrollBar	Barra de desplazamiento vertical	vsb	vsbIndice
	cuando el tipo es desconocido	ctr	ctrActual

20.3 FORMULARIO DE INGRESO AL SISTEMA

1. Imagen particular de acuerdo al sistema.
2. Ubicación imagen: lado izquierdo.
3. Área de Identificación en lado derecho conteniendo: nombre de la Institución y nombre de la aplicación (si ésta no está incorporada en la imagen), centro de atención, usuario y contraseña.
4. Botones ("Aceptar", "Cancelar") ubicación: lado derecho, abajo del Área de Identificación.
5. Parte inferior centrado: derechos de autor, y datos relacionados con el contacto de soporte de sistemas informáticos.
   - ✓ El formulario de ingreso al sistema contendrá el logo del sistema en el que aparecerá el nombre de la aplicación.
   - ✓ Para aplicaciones de escritorio la interfaz de ingreso al sistema deberá contener 2 botones, uno para aceptar la acción y el otro para cancelar, este último cierra la pantalla.
   - ✓ Para aplicaciones web la interfaz de ingreso al sistema deberá contener un solo botón "conectar" con el cual el usuario una vez correcto todos los datos ingresa al sistema, y para cancelar la acción deberá digitar alt+f4 esto se indicará en la etiqueta de derechos de autor que se encontrará al pie de la interfaz.

Ing. José Pedro Rivera Moncada
Jefe División de Desarrollo de Tecnologías de Información y Comunicación

F.

Inga. Claudia Jennifer Molina
Jefa de Unidad de Desarrollo Institucional

20.4 MENÚ

1. Los nombres de las opciones de menú deben iniciar con mayúsculas. Cuando el nombre está compuesto por más de dos palabras, las preposiciones van en minúsculas.

2. La opción de primer nivel para administración de las tablas auxiliares deberá llamarse "Mantenimientos".

3. La opción de primer nivel para gestión de reportes deberá llamarse "Reportes".

4. La opción de primer nivel que se refiere a la seguridad del sistema y a las configuraciones en cuanto a centro de atención, etc. deberá llamarse "Configuración".

5. Para aplicaciones de Escritorio: Todas las opciones del menú deberán tener la capacidad de ser accedidas con la tecla alt+[letra].

6. Para aplicaciones de Escritorio: La última opción de primer nivel deberá llamarse "Salir" y contendrá las sub-opciones "Salir del Sistema" y "Cambio de Usuario".

7. Para aplicaciones de Web: La última opción de primer nivel deberá llamarse "Salir" y contendrá las sub-opciones "Salir del Sistema" y "Cerrar Sesión", al seleccionar la Opción "Cerrar Sesión" deberá mostrar la interfaz de Ingreso al Sistema.

8. La penúltima opción de primer nivel deberá llamarse "Ayuda" y contendrá las sub-opciones "Ayuda" y "Acerca de [nombre de la aplicación]"

9. Para aplicaciones de Escritorio: El menú deberá estar contenido dentro de un Formulario Convencional (no MDI)

21. ESTÁNDAR NATURAL ADABAS

Este estándar se aplicara mientras este en uso la plataforma NATURAL ADABAS.

21.1 ESTÁNDARES PARA LA PROGRAMACIÓN EN NATURAL PARA WINDOWS.

21.1.1 NOMBRES DE LIBRERÍAS

Nomenclatura: AAAAXXX.
Dónde:

"AAAA" es el prefijo que indica el contenido de la librería, de la siguiente manera:

- DESA: librería de programas en desarrollo, objetos fuentes.
- PROD: librería de programas en producción, los cuales son objetos compilados.

"XXX" es el sufijo que indica las iniciales del nombre del sistema.

Ejemplos:

- DESAPFD
- FUENPFD
- PRODPFD

21.1.2 NOMBRES DE PROGRAMAS

Nomenclatura: XXXT9999.
Dónde:

"XXX" es el sufijo que indica las iniciales del nombre del sistema.

"T" es el tipo de objeto Natural. Estos son:

- P: programa.
- M: mapa.
- S: subprograma.
- C: copycode.

"9999" correlativo que indica módulo o submenú, y dentro de éstos el correlativo de programa. En caso de subprogramas y copycodes especiales se indica un nombre mnemotécnico.

Ejemplos:

- PFDP1110
- PFDM1110
- PFDP6121
- PFDC1351

21.1.3 NOMBRES DE VARIABLES

Los nombres de variables se inician con el símbolo hash (#), y a continuación por múltiples palabras juntas, iniciando cada palabra con

letra mayúscula, y la idea es describir el contenido de la variable con tal nombre.

Ejemplos:

- #CorrAfil
- #NumAfil
- #TipDoc
- #NumDoc

21.1.4 NOMBRES DE ARCHIVOS

Nomenclatura: XXX-AAAAAAAA
Dónde:

"XXX" es el sufijo que indica las iniciales del nombre del sistema.

"AAAAAAAA" es el nombre descriptivo del archivo usando múltiples palabras juntas, iniciando cada palabra con letra mayúscula.

Ejemplos:

- PFD-Planilla
- PFD-Detalle
- PFD-Fechas

21.1.5 NOMBRES DE CAMPOS

Nomenclatura: XXX99-AAAAAAAA

Dónde:

"XXX" es el sufijo que indica las iniciales del nombre del sistema.

"99" es el número del archivo dentro de la base (FNR).

"AAAAAAAA" es el nombre descriptivo del campo, usando múltiples palabras juntas, iniciando cada palabra con letra mayúscula.

Ejemplos:

- PFD22-NumPat
- PFD22-Periodo
- PFD22-Detalle

21.1.6 IDENTIFICACIÓN DEL PROGRAMA

Se indica en las primeras línea del programa, identificando los siguientes ítems:

- Nombre del sistema.
- Nombre del programa.
- Nombre del submenú o módulo principal que lo invoca.
- Fecha de creación.
- Descripción resumida del programa.
- Autor y año.

21.1.7 ENTRADAS Y SALIDAS DE PROGRAMA

Se indican en las primeras línea de un mapa o reporte los siguientes ítems:

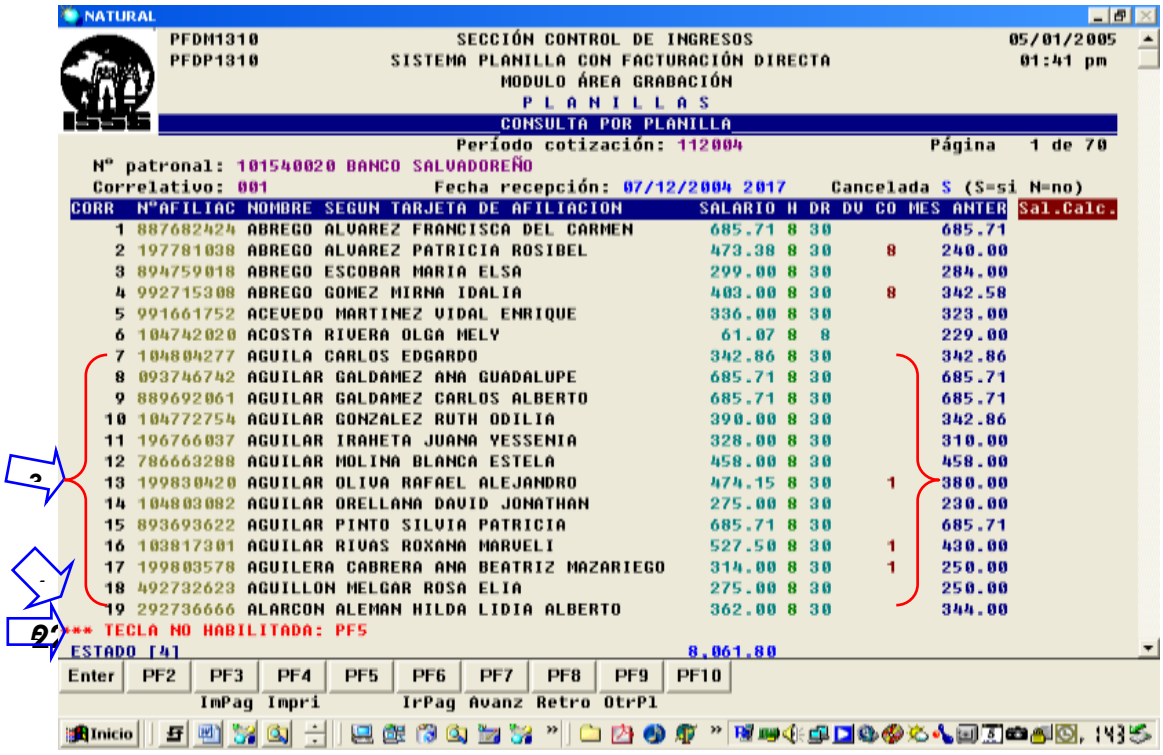
1. Identificación del programa: nombre de programa, mapa, área usuaria, nombre del sistema, nombre de módulo/submenú principal que invoca al programa, fecha y hora del sistema.

2. Identificación de datos principales: entrada o salidas generales de un documento o proceso que se ingresan o consultan, respectivamente.

3. Detalle de datos relacionado: información relacionada con los generales descritos en el item 2.

4. Mensajes de error o alertas.

5. Teclas de función para operar el programa: en forma abreviada, se denomina el evento que desarrolla cada tecla. El nombre completo y la descripción de éstos debe estar contenido en el manual del usuario.



Este estándar se aplicará mientras esté en uso las plataformas VISUAL BASIC y VISUAL FOXPRO.

22.1 INTRODUCCIÓN

Este documento se ha elaborado con el propósito de normar las actividades que involucran el proceso de desarrollo de sistemas: análisis, diseño, creación de prototipos, elaboración de la aplicación (programar) e implementación.

Se incluye aquellas actividades que ameriten ser normadas y puedan basarse en estándares.

Este Manual tiene como objetivo servir de guía a los Analistas de sistemas y programadores.

22.2 NOMBRE DE VARIABLES Y RUTINAS

Los nombres de las variables y funciones deben seguir la siguiente estructura:

<prefijo><cuerpo><calificador><sufijo>

<prefijo>: Describe el alcance y el tipo de la variable.
<Cuerpo>: Describe la variable.

<Calificador>: Denota el derivado de la variable.
<Sufijo>: El tipo de carácter.

22.3 DEFINICIÓN DE <prefijo>

Alcance
Prefijo Descripción
g Global
l Local para un módulo o formulario
s Variable estática
v Variable pasada por valor (local para una rutina)

r Variable pasada por referencia (local para una rutina)

Prefijos de tipos de variables

Tipo de Dato	Prefijo
Decimal	dcl
Double	dbl
Float	Flt
Integer	Int
Number	num
Smallint	Sint
Char	chr
Varchar2	Vcr
long	Lng
Raw	Raw
long raw	lraw
Date	dtm
timestamp	Tst
interval year	Iyr
interval day	Idy
rowid	Rid
Tipo de Dato	**Prefijo**
urowid	urid
boolean	bln
nchar	nchr
nvarchar2	cvcr
bfile	bfl
blod	bld
clod	clf
nclod	ncld

22.4 DEFINICIÓN DE <cuerpo>

El cuerpo de las variables y nombre de rutinas:
El cuerpo de las variables o nombre de rutinas debe usarse combinados entre mayúsculas y minúsculas; y puede ser tan larga como sea necesaria para describir el propósito de la misma. En adición los nombres de las funciones deben comenzar con un verbo, tal como InicializarNombreArreglo o CerrarDialogo.
Para usos frecuentes o términos largos, abreviaturas estándares son recomendadas para ayudar a mantener una longitud razonable. En general los nombres de las variables mayores que 32 caracteres pueden ser dificultosas para leer.
Se debe tomar en cuenta las siguientes consideraciones:

- El nombre de las variables y rutinas deberá iniciar con una letra capital.
- Elija nombre que indiquen la intención de la variable o rutina.
- Evite usar simples caracteres para nombres de variables excepto para variables temporales, los nombres comunes para variables temporales son c,d,e para campos de carácter e i,j,k,m y n para enteros.

Caracteres numéricos y especiales: Números, guiones y signos especiales no pueden usarse para nombres de variables o rutinas como letra inicial.

22.5 DEFINICIÓN DE <calificador>

Calificador en Nombres de Variables y Rutinas:
Relacionar variables y rutinas son a menudo usadas para administrar y manipular objetos comunes. En estos casos, se usan calificadores estándares para etiquetar las variables y rutinas derivadas. Aunque poner el calificador después del cuerpo del nombre puede verse como un poco complicado (como por ejemplo: TomarNombrePrimero, TomarNombreUltimo en vez de TomarPrimerNombre, TomarUltimoNombre), esta práctica puede ayudar a ordenar los nombres de variables o rutinas que están relacionadas, permitiendo que la lógica y la estructura de la aplicación sea fácil de entender. La siguiente tabla define los calificadores comunes y su significado.

Calificador	Descripción
Primer	Primer elemento de un conjunto.
Ultimo	Ultimo elemento de un conjunto.
Siguiente	Siguiente elemento de un conjunto.

Previo	Elemento anterior de un conjunto.
Actual	Elemento actual de un conjunto.
Minimo	Valor mínimo de un conjunto.
Maximo	Valor máximo de un conjunto.
Salvar	Usado para guardar variables que pueden cambiar posteriormente.

22.6 DEFINICIÓN DE <sufijo>

Sufijo en Nombres de Variables y Rutinas
Algunas convenciones de nombres también permiten agregar un sufijo al final del nombre, como por ejemplo gintVendedorMejor_ES, representando que la variable es utilizada para el mejor vendedor de El Salvador (ES). Un sufijo provee un nivel más aceptable de detalle del calificador. Siendo este manejo de sufijos opcional para el nombrado de variables o rutinas.
Se debe tomar en cuenta que el sufijo esta siempre antecedido por en guión bajo (_) antes del mismo.

22.7 NOMBRAMIENTO DE CONSTANTES

El cuerpo del nombre de una constante debe usarse en Mayúsculas con guión bajo entre las palabras, estas deben de representar el uso de dicha variable. Por ejemplo:

lintCALCULAR_USUARIOS_MAXIMO	Calcular el número máximo de usuarios, variable tipo entero (local para rutina o procedimiento).
gstrNUEVA_LINEA	Nueva línea de caracteres tipo "string" (global para la aplicación).

22.8 CONVENCIONES PARA NOMBRAR MENÚS

Las aplicaciones frecuentemente usan abundantes controles de menús. Los prefijos para los controles de menús podrían ir más allá de la etiqueta inicial "mnu" y agregarle un prefijo adicional por cada nivel de anidación, con el nombre del menú al final de la cadena.

Por ejemplo, se tiene el menú archivo con tres opciones internas (nuevo, abrir, guardar), cada opción se definiría de la siguiente forma:

- mnuArchivoNuevo
- mnuArchivoAbrir
- mnuArchivoGuardar

Cuando se usa esta convención, todos los miembros de un grupo de menú en particular son identificables fácilmente.

22.9 CONVENCIONES DE NOMBRES PARA OTROS CONTROLES

Para nuevos controles no listados anteriormente, se deben nombrar prefijos de tres caracteres únicos. Para objetos derivados de otros controles, se puede extender el prefijo para que no exista confusión con otros prefijos de controles existentes y que están en uso. Una abreviatura en minúsculas podría ser agregada al prefijo, por ejemplo: una instancia de un control creado para "Visual Basic Professional 3D Área de Identificación" podría usar como prefijo "fra3d" para evitar confusión con el control "Área de Identificación" existente.
Para controles usados en las aplicaciones que son de "Terceros" se usará el prefijo asignado para el control y una inicial que represente al vendedor del software, además en la sección de comentarios se debe de especificar el nombre completo del control y el nombre del vendedor del software.

Ejemplo:

Prefijo	**Tipo de control**	**Vendedor**
cmdm	Command Button	MicroHelp

22.10 COMENTARIOS DEL CÓDIGO

Todos los procedimientos y funciones deben comenzar con un breve comentario que describa las características funcionales de la rutina. Esta documentación no debe describir los detalles de implementación porque a menudo estos pueden cambiar con el tiempo, resultando en comentarios innecesarios, o peor, en comentarios erróneos.
Los paramentos pasados a una rutina deberían describirse cuando sus funciones no son obvias y cuando la rutina prevé que los parámetros pueden están en un rango específico. Funciones que retornen valores y variables globales que son cambiadas en la rutina (especialmente a través de parámetros de referencia) deben ser descritas al inicio de cada rutina o función.
Bloque de comentarios en el encabezado de las rutinas deberían ser como el siguiente ejemplo:

Seccion	Comment Description
Propósito	Que hace la rutina (no como).
Entradas	Cada parámetro no ambiguo en líneas separadas con su respectivo comentario.
Suponer	Listado de cada variable externa no ambigua, archivos de control, archivos abiertos, etc.
Retornos	Explicación de cada valor de retorno para la función.
Efectos	Lista por cada variable externa afectada, archivo de control, archivos y cualquier otro efectos (si sucediera).

Cada declaración de variable debe incluírsele una línea de comentario que describa el uso de la variable recién declarada.
Variables, controles y rutinas deben ser nombradas con suficiente claridad para que en la línea de comentarios sea necesaria solamente para complejas o no intuitivas.

22.11 FORMATEANDO EL CÓDIGO

La identificación de bloques anidados debe ser de cuatro espacios. Más de cuatro espacios son innecesarios y puede causar que código se oculte o sea accidentalmente truncado. Menos de dos espacios no es suficiente para mostrar en forma clara código anidado.
El comentario de la función general de una rutina debe ser indentado un espacio. El código de nivel más alto que sigue a la visión general debe ser indentado una tabulación (tab), con cada bloque se debe indentar una tabulación (tab) adicional.

Por ejemplo:
Se utiliza código de Visual Basic para ilustrar.

```
'*********************************************************************
'Propósito:     Localizar la primera ocurrencia de un usuario
                especifico  en el arreglo strListaUsuarios.
'Entradas:      strUserList():  La lista de usuarios en la cual se realizará la
búsqueda        strTarget User:   El nombre del usuario a buscar 'Retorno:    El
índice de la primera ocurrencia del usuarios a buscar (strTargetUser) en el
arreglo strListaUsuarios, si no se encuentra el usuario se retorna -1.
'*********************************************************************

'VB3Line: Enter the following lines as one line
Function iFindUser (strListaUsuarios() As String, strTargetUser as String)    As
Integer
  Dim i As Integer          ' Contador secuencial
  Dim bFound As Integer     ' bandera de objetivo encontrado
```

```
    iFindUser = -1
    i = 0
    While i <= Ubound(rasUserList) and Not bFound
      If rasUserList(i) = rsTargetUser Then
        bFound = True
        iFindUser = i
      End If
    Wend
  End Function
```

22.12 VISUAL FOX PRO

Prefijo	Objeto	Ejemplo
chk	check box	chkReadOnly
cbo	ComboBox	cboEnglish
cmd	CommandButton	cmdCancel
cmg	CommandGroup	cmgChoices
cnt	Container	cntMoverList
ctl	Control	ctlFileList
<user-defined>	Custom	user-defined
edt	EditBox	edtTextArea
frm	Form	frmFileOpen
frs	FormSet	frsDataEntry
grd	Grid	grdPrices
grc	Column	grcCurrentPrice
grh	Header	grhTotalInventory
img	Image	imgIcon
lbl	Label	lblHelpMessage
lin	Line	linVertical
lst	list box	lstPolicyCodes
olb	OLEBoundControl	olbObject1
ole	OLE	oleObject1
opt	OptionButton	optFrench
opg	OptionGroup	opgType
pag	Page	pagDataUpdate
pgf	PageFrame	pgfLeft
sep	Separator	sepToolSection1
shp	Shape	shpCircle
spn	Spinner	spnValues
txt	text box	txtGetText
tmr	Timer	tmrAlarm
tbr	ToolBar	tbrEditReport

22.13 NOMBRAR OBJETOS

Los nombres de los objetos deben seguir la siguiente estructura:
<prefijo><cuerpo>
<prefijo>: Describe el tipo de objeto
<Cuerpo>: Describe el objeto

22.14 PREFIJOS PARA OBJETOS ESTÁNDARES

- **VISUAL BASIC**

La siguiente tabla define los prefijos de los nombre de los objetos.

Prefijo	Tipo de Objeto	Ejemplo
ani	Animation button	aniMailBox
bed	Pen Bedit	bedFirstName
cbo	Combo box and drop down list box	cboEnglish
chk	Checkbox	chkReadOnly
clp	Picture clip	clpToolbar
cmd (3d)	Command button (3D)	cmdOk (cmd3dOk)
com	Communications	comFax
ctr	Control (when specific type unknown)	ctrCurrent
dat	Data control	datBiblio

Prefijo	Tipo de Objecto	Ejemplo
dir	Directory list box	dirSource
dlg	Common dialog control	dlgFileOpen
drv	Drive list box	drvTarget
fil	File list box	filSource
frm	Form	frmEntry
fra (3d)	Área de Identificación (3d)	fraStyle (fra3dStyle)
gau	Gauge	gauStatus
gpb	Group push button	gpbChannel
gra	Graph	graRevenue
grd	Grid	grdPrices
hed	Pen Hedit	hedSignature
hsb	Horizontal scroll bar	hsbVolume
img	Image	imgIcon
ink	en Ink	inkMap
key	Keyboard key status	keyCaps

lbl	Label	lblHelpMessage
lin	Line	linVertical
lst	List box	lstPolicyCodes
mdi	MDI child form	mdiNote
mpm	MAPI message	mpmSentMessage
mps	MAPI session	mpsSession
mci	MCI	mciVideo
mnu	Menu	mnuFileOpen
opt (3d)	Option Button (3d)	optRed (opt3dRed)
ole	OLE control	oleWorksheet
out	Outline control	outOrgChart
pic	Picture	picVGA
pnl3d	3d Panel	pnl3d
rpt	Report control	rptQtr1Earnings
shp	Shape controls	shpCircle
spn	Spin control	spnPages
txt	Text Box	txtLastName
tmr	Timer	tmrAlarm
vsb	Vertical scroll bar	vsbRate

23. ESTÁNDARES UTILIZADOS PARA LA ENTREGA DE SOFTWARE

El propósito de este documento es establecer los estándares a utilizarse en la entrega de software desarrollado.

A continuación se detallan los elementos a considerar cuando se realice la entrega de software:

23.1 DEFINICIÓN DE VERSIÓN Y REVISIÓN

Una **versión** se da cuando exista cualquiera de los siguientes casos:

a. Sustitución de formulario.
b. Opción nueva en menú.
c. Modificación de estructuras.
d. Modificación o adición de índices.
e. Adición de estructuras.

Una **revisión** se da cuando exista cualquiera de los siguientes casos:

a. Corrección de observaciones como resultado de revisión de Soporte al Usuario, ya sea por error de programación, funcionamiento, etc.
b. Detección de observaciones por parte de la sección salud posterior a la entrega del software a Soporte al Usuario.
c. Agregado o cambio de funcionalidad a un formulario siempre y cuando no implique cambio en estructuras de la Base de Datos.

F. Ing. José Pedro Rivera Moncada
Jefe División de Desarrollo de Tecnologías de Información y Comunicación

F. Inga. Claudia Jennifer Molina
Jefa de Unidad de Desarrollo Institucional

Fecha de modificación 19/08/2015

d. Agregado o cambio de componentes a un formulario siempre y cuando no implique cambio en estructuras de la Base de Datos.
e. Corrección de observaciones efectuadas por usuario final y que no afecte la Base de Datos.

Cuando en una entrega existan casos que pertenezcan a una versión y una revisión, predominará la versión.

La identificación del software a entregar para efectos de Versión será la siguiente:

- ✓ Se utilizará un número correlativo de 4 posiciones: dos para los enteros y dos para los decimales separados por un punto. Los enteros cambiarán únicamente cuando se dé el literal "e. Adición de estructuras" del listado de casos que identifican un cambio de versión y los decimales lo harán para los literales del "a." al "d.". Ambos números los enteros y decimales cambiarán correlativamente del 01 al 99, y cuando haya cambio de entero el decimal se reinicializará a cero.

La identificación del software a entregar para efectos de Revisión será la siguiente:

- ✓ Cada vez que exista cambio de Versión en su parte entera o decimal, la revisión se reinicia a Cero.
- ✓ La numeración utilizada cuando exista cambio de revisión será correlativamente del 00 al 99

Los datos de la Versión y Revisión deberán ser incorporados en el formulario "Acerca de..." del software a entregar utilizando el siguiente formato:

Versión: 5.01
Revisión: 00

23.2 NOMENCLATURA DEL NOMBRE DEL ARCHIVO CON CAMBIOS AL SISTEMA

El nombre del archivo del informe de cambios realizados a un sistema será nombrado de la siguiente manera:

Cambios en *nombre-sistema* a la *fecha* V *número* R *número*, en donde:

nombre-sistema: Nombre del Sistema que se entrega.
Fecha: Fecha en formato ddmmaa (999999)*.
V *número*: Número de versión que se entrega.
R *número*: Número de revisión que se entrega.

F. Ing. José Pedro Rivera Moncada
Jefe División de Desarrollo de Tecnologías de Información y Comunicación

F. Inga. Claudia Jennifer Molina
Jefa de Unidad de Desarrollo Institucional

Fecha de modificación 19/08/2015

Ejemplo: **"Cambios en Farmacia General al 011104 V5.01 R01"**

- Este archivo incluirá los cambios, correcciones o adiciones a formularios, funcionalidades, estructuras de la base de datos y todo aquello realizado durante la versión o revisión del sistema.

* Fecha en la cual se hace entrega de la versión/revisión.

23.3 CONTENIDO DEL ARCHIVO CON CAMBIOS AL SISTEMA

El contenido del archivo con el informe de cambios realizados a un sistema será el siguiente:

a. Encabezado con el título "INFORME DE CAMBIOS EN *nombre-sistema* AL *fecha* VERSIÓN *número* – REVISIÓN *número*".

INFORME DE CAMBIOS EN FARMACIA GENERAL AL 30112004
VERSION 5.00 - REVISION 00

Fig. 1. Muestra del encabezado de título.

b. Los cambios o adiciones se deberán definir en orden en que aparecen en el menú del sistema.
c. Los apartados a definir en cada cambio o adición serán:

✓ Cambios en formulario.
- Utilizar la palabra "Ninguna" cuándo no exista cambio en el formulario.
- Utilizar la frase "Nueva. Ver Figura x" cuando el formulario sea nuevo.
- Utilizar la palabra "Modificada" o "Eliminada" según sea el caso.
- Utilizar la palabra "Sustituida" cuando sea el caso.

✓ Funcionalidad.
- Qué hace el formulario y/o cómo funciona, cuando sea nuevo.
- Qué funcionalidad nueva se la ha incorporado, si es modificada.

✓ Cambios en Estructuras.
- Utilizar la palabra "Ninguna" cuando no se haya efectuado cambio o adición de estructuras.

F. _____
Ing. José Pedro Rivera Mancerda
Jefe División de Desarrollo de Tecnologías de Información y Comunicación

F. _____
Inga. Claudia Jenniffer Molina
Jefa de Unidad de Desarrollo Institucional

Fecha de modificación 19/08/2015

- Si se modificaron o se adicionaron estructuras seguir las indicaciones del literal "e" del presente numeral.

i. Si dentro de los cambios o adiciones surgen nuevos formularios, las gráficas de éstas se deberán anexar al documento y desde la definición de cambios o adiciones se deberá hacer referencia a ellas correlativamente utilizando la frase "Ver Figura x", donde la "x" se sustituye por el número correlativo de la figura.

j. Si existen cambios en estructuras ya existentes, los cambios se reflejarán en el apartado "Cambios en Estructuras".

k. Si la(s) estructura(s) son nuevas en la base de datos, se deberá anexar la descripción de la estructura junto con la de los índices, haciendo referencia a ellas desde el apartado "Cambios en Estructuras" y siguiendo el formato mostrado en la Fig. 2.

Nombre de la tabla: XXX.DBF
Descripción:

Índices

No.	Tag	Expresión
1	tag1	campo1
2	tag2	campo2
3	tag3	campo1+campo2

No.	Nombre Campo	Tipo	Tamaño	Descripción
1				
2				

Fig. 2. Muestra del contenido de descripción de estructuras nuevas.

El anexo de estructuras será en orden alfabético.

l. Si existe algún tipo de recomendaciones o actividades adicionales que se deben considerar durante la actualización de la versión o revisión, éstas se deberán listar al final de la descripción de cambios o adiciones antes de los anexos, utilizando el título "CONSIDERACIONES ADICIONALES".

m. Los anexos de muestras de gráficas de formularios y estructuras de bases de datos irán al final del documento.

n. Formato del documento:
   - ✓ Encabezado alineado a la izquierda de cada página indicando Nombre del sistema Versión y Revisión, por ejemplo "Farmacia General Versión 9.00 Revisión 00". Este encabezado irá en todas las páginas a excepción de la primera. Ver Fig. 3
   - ✓ Numeración de las páginas en la esquina inferior derecha. Todas las páginas irán numeradas.

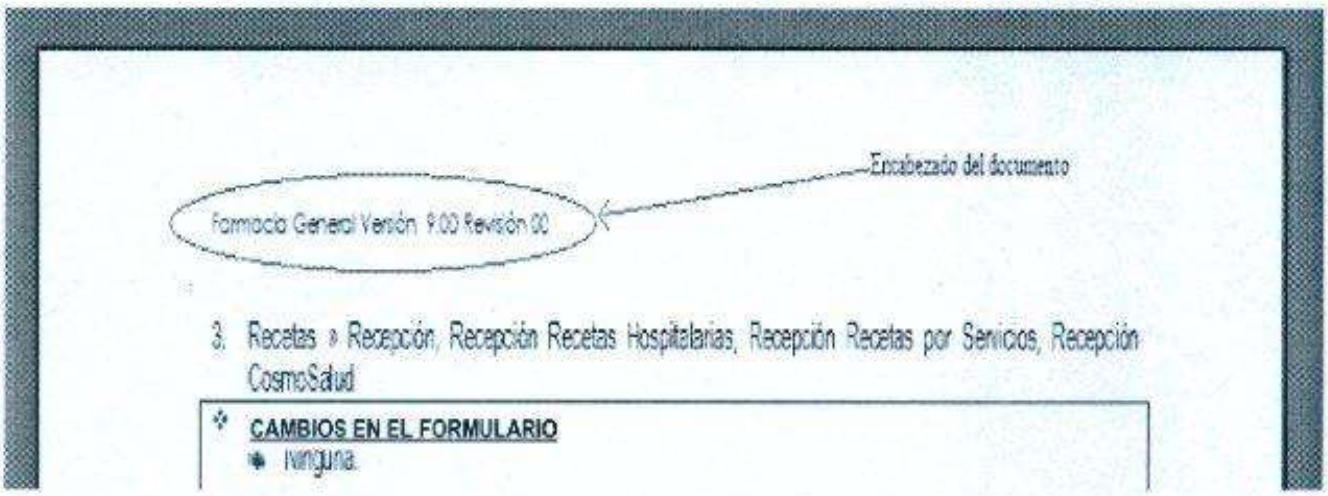


Fig. 3 Muestra del encabezado a utilizar

23.4 UBICACIÓN DEL ARCHIVO DE CAMBIOS DENTRO DE LA ESTRUCTURA DE DIRECTORIOS

El archivo será copiado en el directorio "DOCUMENTACIÓN" del directorio raiz de la aplicación. Si éste directorio no se encuentra será necesario crearlo.

23.5 ROTULACIÓN DEL CD DE ENTREGA

La rotulación del CD de entrega deberá contener la siguiente información:

- Nombre del Sistema.
- Versión.
- Revisión.
- Fecha.

F. Ing. José Pedro Rivera Moncada
Jefe División de Desarrollo de Tecnologías de Información y Comunicación

F. Inga. Claudia Jennifer Molina
Jefa de Unidad de Desarrollo Institucional

Fecha de modificación 19/08/2015

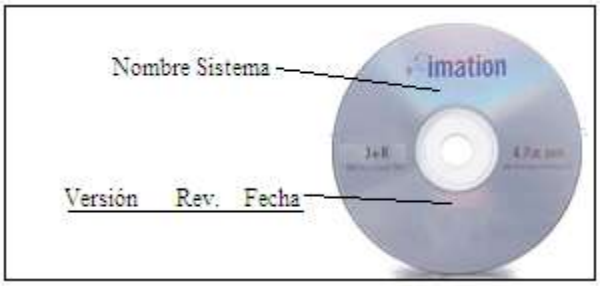


Fig. 3 Muestra del rotulado del CD

24. ESTÁNDARES DEL CONTENIDO DE MANUAL DE USUARIO Y MANUAL TECNICO

24.1OBJETIVO

Establecer el estándar del contenido para la administración de los manuales de usuario y técnicos de los Sistemas de información, los cuales facilitarán la operación de los mismos a los usuarios.

24.2 MANUAL USUARIO

1. Presentación del Sistema.
   a) Información General.
   b) Objetivos.
   c) Contexto de Operación.
      i) Teclas de Funciones.
      ii) Menús.
      iii) Mensajes (Alertas y Prohibiciones).

2. Generalidades del Sistema.

3. Acceso al Sistema.
   d) Acceso al Sistema.
   e) Inicio del Sistema.
   f) Niveles y/o Perfiles de Usuario.

4. Representación gráfica de la estructura del sistema (Diagrama Jerárquico del Sistema).

5. Procedimientos de operación de los componentes del sistema:

   g) Función de cada opción o componente.
   h) Ciclo operativo o cronológico de sistema.
6. Identificación adecuada de las etiquetas de los archivos de salida.

7. Procedimientos de seguridad y control en casos de emergencia.
8. Especificaciones de uso y diseño de entrada de datos (Formatos y formularios de captura).
9. Especificaciones de uso y diseño de salida de datos (Reportes y pantallas de consulta).
10. Procedimientos para notificar errores.
11. Glosario.
12. Anexos.

24.3 MANUAL USUARIO SISTEMA SAP

Los manuales de usuario del sistema SAP o BPP están formados por la siguiente estructura:

1. Objetivo.
2. Ruta de acceso.
3. Descripción del uso de la transacción construido por módulos que consta de:
   i) Parte descriptiva.
   ii) Parte gráfica.

24.4 MANUAL TÉCNICO

1. Introducción.
2. Ambiente de Desarrollo y Operación.
   Se describe el software en que se ha desarrollado la aplicación, la funcionalidad interna de la aplicación (si es en 3 capas, si usa web services, manejo de la seguridad a nivel de código de programación, manejo de la bitácora), así como también los requerimientos mínimos de hardware y software necesario para que la aplicación funcione.
3. Usuarios de la Aplicación.
   3.1 Usuarios Directos.
   3.2 Usuarios Externos.
4. Diagrama Jerárquico.
5. Descripción de objetos.

F. _____ Ing. José Pedro Rivera Mopeada Jefe División de Desarrollo de Tecnologías de Información y Comunicación	F. _____ Inga. Claudia Jenhifer Molina Jefa de Unidad de Desarrollo Institucional	Fecha de modificación 19/08/2015

Se detallan, si aplica: una breve descripción de la funcionalidad del reporte, ventanas asociadas, formularios, detalle de los objetos, eventos/procedimientos/funciones, tablas y paquetes (procedimientos almacenados) utilizados.

6. Tablas vrs. Opciones del Sistema.

7. Modelos de Datos.
   Muestra el diagrama del modelo físico de la base de datos.

8. Diccionario de Datos.
   Como primera tabla, se debe colocar un listado con los nombres y la descripción de todas las tablas de la aplicación. Incorporar en cada tabla el detalle de sus respectivos índices, con los campos que los constituyen (los campos pueden ir en paréntesis junto al nombre del índice). En cada detalle de las tablas, si las tablas pertenecen a otro esquema, colocar en la descripción el nombre del esquema al que pertenecen, esto puede ser entre paréntesis al final de la descripción. Al final incorporar una lista de los procedimientos almacenados utilizados por el sistema con la descripción y el nombre de su respectivo esquema.

   NOTA: en el caso del sistema SAFISSS se adoptará la estructura del Manual Técnico del proveedor del sistema informático.

25. ESTÁNDARES DE DESARROLLO SAP- ABAP

INTRODUCCIÓN

Es necesario definir estándares para el proceso de desarrollo de aplicaciones complementarias al sistema SAP.

Estándar Default

SAP tiene un estándar para los desarrollo de aplicaciones complementarias a la licencia adquirida, dicho estándar es la letra **"Z"**, la cual debe utilizarse como inicial a la identificación de las aplicaciones que se desarrollan, ya que cuando se realizan actualizaciones a la licencia todo lo que este identificado inicialmente con "Z" no lo toca la actualización.

Ejemplo.

Z……..

IDENTIFICACIÓN DE OBJETOS

A continuación se describe, por tipo de objeto de repositorio SAP, el método a utilizar para asignar los nombres de los mismos. Los criterios utilizados son principalmente: tipo de objeto y módulo SAP del ISSS.

DICCIONARIO DE DATOS

Tabla

Nombre **ZXXTT_Nombre**:

Z	Valor Fijo
XX	Módulo SAP del ISSS *
TT	Valor Fijo (**T**abla **T**ransparente)
Nombre	Descripción **

Estructura (diccionario de datos)

Nombre **ZXXE_Nombre**:

Z	Valor Fijo
XX	Módulo SAP del ISSS *
E	Valor Fijo (Estructura)
Nombre	Descripción **

Elemento de Datos

Nombre **ZXXED_Nombre**:

Z	Valor Fijo
XX	Módulo SAP del ISSS *
ED	Valor Fijo (**E**lementos de **D**atos)
Nombre	Descripción **

Dominio

Nombre **ZXXDO_Nombre**:

Z	Valor Fijo
XX	Módulo SAP del ISSS *
DO	Valor Fijo (**DO**minio)
Nombre	Descripción **

Objeto de Bloqueo

Nombre **EZ_Nombre**:

E	Valor Fijo (SAP estándar)
Z	Valor Fijo
Nombre	Nombre de tabla de Referencia

Vista

Nombre **ZXXV_Nombre**:

Z	Valor Fijo
XX	Módulo SAP del ISSS *
V	Valor Fijo (**V**ista)
Nombre	Descripción **

Data Type Group

Nombre **ZDT*Corr***:

Z	Valor Fijo
DT	Valor Fijo (**D**ata **T**ype)
Corr	Correlativo de 2 posiciones

Search Help

Nombre **ZXXSH_Nombre**:

Z	Valor Fijo
XX	Módulo SAP del ISSS *
SH	Valor Fijo (**S**earch **H**elp)
Nombre	Descripción **

SET/GET Parameter

Nombre **PA_Nombre**:

PA Valor Fijo (**Pa**rameter)

Nombre Descripción **

OBJETOS DE PROGRAMAS

Programa

Nombre: **ZXX_YY_*Nombre***:

Z Valor fijo

XX Módulo SAP del ISSS *

YY Tipo de Programa ****

Nombre Descripción **

Module Pool

Nombre: **SAPMZXX_*Nombre***:

SAP Valor Fijo (standard SAP)

M Valor Fijo (**M**odule Pool)

Z Valor Fijo

XX Módulo SAP del ISSS *

Nombre Descripción **

Module pool Include

Nombre: **MZIXX_*Nombre*_NN**:

M Valor Fijo (**M**odule Pool)

Z Valor Fijo

I Valor fijo

XX Módulo SAP del ISSS *

Nombre Descripción con referencia al Module Pool principal **

NN Correlativo

Transacción

Nombre: **ZXXT_Nombre**:

Z Valor Fijo

XX Módulo SAP del ISSS *

T Valor Fijo (**T**ransacción)

Nombre Descripción **

Clase de Mensaje

Nombre: **ZXX**:

Z Valor Fijo

XX Módulo SAP del ISSS *

Módulo de Función

Nombre **ZXXFU_Nombre**:

Z Valor Fijo

XX Módulo SAP del ISSS *

FU Valor Fijo (**FU**nción)

Nombre Descripción **

Grupo de Funciones

Nombre **ZXXGF_Nombre**:

Z Valor Fijo

XX Módulo SAP del ISSS *

GF Valor Fijo (**G**rupo de **F**unciones)

Nombre Descripción **

Sapscript

Nombre **ZXXS_Nombre**:

Z Valor Fijo

XX Módulo SAP del ISSS *

S Valor Fijo (**S**apscript)

Nombre Descripción **

SmartForms

Nombre **ZXXSF_Nombre**:

Z Valor Fijo

XX Módulo SAP del ISSS *

S Valor Fijo (**S**apscript)

Nombre Descripción **

Select Option Parameter

Nombre **SO_Nombre**:

SO Valor Fijo (**S**elect **O**ption)

Nombre Descripción **

Internal Table

Nombre **IT_Nombre**:

IT Valor Fijo (**T**abla **I**nterna)

Nombre Descripción **

Etructura (en tiempo en ejecución)

Nombre **E_Nombre**:

E Valor Fijo (**E**structura)

Nombre Descripción **

Variable, Constant and Range

Nombre **PP_Nombre**:

PP Prefijo de tipo de variable ***

Nombre Descripción **

OTROS OBJETOS

Batch input Session

Nombre **ZXX_Nombre**:

Z Valor Fijo

XX Módulo SAP del ISSS *

Nombre Descripción **

Ordenes de Transporte

Nombre **BC_XX: *Nombre***:

BC	Valor Fijo
XX	Módulo SAP del ISSS *
Nombre	Descripción **

Imágenes

Nombre Z**XX_IMG_<TIPO> *Nombre***: (Ej: ZDM_IMG_FIRM_LORENTC)

Z	Valor Fijo
XX	Módulo SAP del ISSS *
IMG	**Valor Fijo (IMG=IMAGE)**
Tipo Imagen	**FIRM-Firma, FOTO-Fotografia, FACH-Fachada, LOCA-Local**
Nombre	Descripción **

NORMAS Y PREFIJOS

Módulos SAP del ISSS (*):

Prefijo	Modulo de SAP
FI	GL, AR, TR, AM, AP, CFM
CO	CO, CO-PC, CO-OM
MM	MM, MM-IM
SD	SD
DE	Desarrollos globales

Descripción (**):

Para la asignación del nombre de los objetos se tomaran las 4 primeras letras de cada palabra que compone la descripción de lo que se va a desarrollar. En caso de que sean descripciones formadas por varias palabras, por cada palabra se debe utilizar guión mayor ('_') para separarlas.

Prefijo de tipo de variable (***):

Prefijo	Tipo de Variable	Descripción
NU	N - Numeric	Alfanumérica (solo números)
CH	C - Character	Alfanumérica
PK	P - Packet	Montos
IN	I – Integer	Números Enteros
FL	F – Floating	Números con 1 entero y mucho decimals

Prefijo	Tipo de Variable	Descripción
HX	X – Hexagésimal	Hexagésimal
DT	D – Date	Fecha
TM	T – Time	Hora
ST	STRING – String	Cadena de Caracteres de tamaño variable
CN	Cualquier Tipo	Constantes

Prefijo de tipo de Programa (****):

Prefijo	Tipo de Variable
IF	Interfaz
RE	Reporte
CN	Conversión
CI	Carga Inicial
PR	Programas
IN	Include

PAQUETES

Todo objeto de repositorio debe asignarse a un paquete al ser creado. Se crearon los siguientes paquetes:

Paquete	Descripción
ZFI	Desarrollos para FI
ZCO	Desarrollos para CO
ZMM	Desarrollos para MM
ZSD	Desarrollos para SD
ZDE	Desarrollos globales (clases o includes globales)

Todos los desarrollos que se realicen para pruebas o temporales, deben ser asignados como Objeto Local, es decir, al paquete estándar "$TMP". Con esto, no se tendrá que asignar el desarrollo a una orden de transporte.

ESTÁNDARES DE CÓDIGO

INDENTACIÓN DE BLOQUES A 2 ESPACIOS

Utilizar 2 espacios para indentar cualquier bloque de código. No utilizar tabuladores ya que estos pueden ser interpretados distinto según el editor (Ej.: Notepad), el uso de espacios asegura indentación correcta.

```
DO 5 TIMES.
  IF v_tipo = 'E'.
    v_nombre = r_cliente.
    IF v_nivel = 'M'.
      v_descripcion = 'Mayorista'.
    ELSE.
      v_descripcion = 'Minorista'.
    ENDIF.
  ELSE.
    v_nombre = r_cliente-nombre.
  ENDIF.
ENDDO.
```

MAYÚSCULAS PARA PALABRAS RESERVADAS

Para las palabras reservadas de OPEN SQL se utilizarán mayúsculas para facilitar la diferenciación de los elementos definidos por el usuario.

```
  SELECT SUM(total_venta)INTO v_total_venta
                         FROM zt_fiap_deta_vent
                         WHERE cliente = r_cliente-cliente.
```

MINÚSCULAS PARA ELEMENTOS DEFINIDOS POR USUARIO

Todos los elementos definidos por el programador como variables, constantes, tablas internas, estructuras, etc. deben utilizar el estándar en minúsculas. En caso de que sean nombres formados por varias palabras, por cada palabra se debe utilizar guión mayor ('_') para separarlas.

```
zt_fiap_deta_vent-nombre_entidad
v_entidad_comercial
c_tasa_interes
cu_clientes
```

ANCHO MÁXIMO DE LÍNEA A 70 CARACTERES

Limitar el número de caracteres por línea a 70 para mantener visible el código escrito. Cuando un comando se componga de varias líneas ajustar el texto de la siguiente línea a la altura de indentación del bloque de información al que pertenece. Se presentan varios ejemplos que tratan de ilustrar esto.

```
CONTATENATE primer_apellido
            segundo_apellido
            primer_nombre
            segundo_nombre INTO nombre_completo.
```

COMENTARIOS

Se debe mantener una documentación consistente en el código escrito para facilitar su entendimiento por otras personas. Debe incluir como mínimo la lógica del procedimiento que ejecuta el código.

Encabezado

Se debe escribir un encabezado que indique el estado, nombre, propósito e historial de modificaciones del procedimiento. Este debe utilizar los delimitadores "**" como se muestra en el ejemplo:

```
************************************************************************
* INFORMACION GENERAL
*  Nombre del Programa : <Nombre del Programa>
*  Título              : <Título del Programa en los Atributos>
*  Autor               : <Autor>
*  Fecha de Creación   : <Fecha de Creación>
*  Tipo                : <Reporte, conversión, Interfase, etc.>
*  Copia de            : <Programa Original del cual fue copiado >
*  Módulo              : <Módulo Funcional de SAP>
*  Llamado por         : <Transacción, o Programa>
*  Descripción         : <Breve descripción del Desarrollo>
*
************************************************************************
*  Modificaciones:
*  <Fecha> - <Autor>
*  <Modificación Descripción>
************************************************************************
REPORT  ZDE_RP_MODELO.
```

Entre Líneas

En este caso se debe de comentar cada vez que se inicia un bloque de procesamiento para explicar que es el propósito de esa sección de código. Si se quiere una línea de comentario completa, se utiliza "*" en la primera columna; si se quiere un breve comentario en la misma línea donde se encuentra una instrucción, se utiliza comillas dobles (") antes del comentario.

```
*  Revision del credito pendiente del cliente
  IF v_credito_pendiente = 0.    " Si no tiene Pendientes
    v_credito_pendiente=v_credito_pendiente + r_cuenta_cobrar-credito.
  END IF.
```

Modificaciones

Durante el desarrollo de una aplicación, se deben realizar modificaciones de código debido a correcciones u actualizaciones en la lógica del funcionamiento.

Lo que se debe hacer en estos casos, es que en cada modificación, dejar constancia de quien lo hace y desde donde hasta donde se realizó la modificación.

```
 * Modif. – 12.03.2005 – USER1 ----------------------------------------
----INI.
( Código )
 * Modif. – 12.03.2005 – USER1 ----------------------------------------
----FIN.
```

Esto ayuda a seguir modificando con facilidad y seguir los cambios que se han producido en el sentido de un historial debido a que se documenta la fecha y el desarrollador que realizo el cambio. Esto es importante ya que si el cambio diera algún tipo de problema, es sencillo regresar al estado anterior.

Si se va a reemplazar líneas o variables, dejarlas comentadas para tener como referencia la funcionalidad anterior a la modificación y el nuevo código hacerlo al costado o debajo de lo viejo.

Eventos, declaraciones y Subrutinas

Los eventos, declaraciones y subrutinas, deben ser documentadas de la siguiente forma:

```
************************************************************************
* INFORMACION GENERAL
*  Nombre del Programa : <Nombre del Programa>
*  Título              : <Título del Programa en los Atributos>
*  Autor               : <Autor>
*  Fecha de Creación   : <Fecha de Creación>
*  Tipo                : <Reporte, conversión, Interfase, etc.>
*  Copia de            : <Programa Original del cual fue copiado >
*  Módulo              : <Módulo Funcional de SAP>
*  Llamado por         : <Transacción, o Programa>
```

```
*  Descripción         : <Breve descripción del Desarrollo>
*
************************************************************************
*  Modificaciones:
*  <Fecha> - <Autor>
*  <Modificación Descripción>
************************************************************************
REPORT  ZDE RP MODELO.

************************************************************************
* TABLES                                                               *
************************************************************************
" Declaraciones de Tablas de Diccionario y Estructuras

************************************************************************
* TYPES                                                                *
************************************************************************
"Tipos de variables, estructuras y tablas internas
TYPES: BEGIN OF TYPE DATA,
       DATA1(5),
       DATA2(2) TYPE N.
       END OF TYPE_DATA.

************************************************************************
* DATA                                                                 *
************************************************************************
"Declaración de Variables globales, constantes, tablas internas
DATA: VAR1, VAR2.
************************************************************************
* PARAMETERS                                                           *
************************************************************************
"Parámetros y Select-options

************************************************************************
* INITIALIZATION                                                       *
************************************************************************
"Inicializaciones

************************************************************************
* AT SELECTION-SCREEN                                                  *
************************************************************************
"Validaciones sobre los parámetros

************************************************************************
* MAIN PROGRAM                                                         *
************************************************************************
START-OF-SELECTION.
PERFORM SUB RUTINE USING VAR1
                 CHANGING VAR2.
END-OF-SELECTION.
************************************************************************
* AT LINE-SELECTION                                                    *
************************************************************************
"Para Reportes Interactivos
************************************************************************
* AT USER-COMMAND                                                      *
************************************************************************
"Para Botones
************************************************************************
* TOP-OF-PAGE                                                          *
************************************************************************
"Encabezado de Reportes
************************************************************************
* BOTTOM-OF-PAGE                                                       *
************************************************************************
```

```
"Pié de Página de Reportes
*---------------------------------------------------------------------*
* FORMS                                                               *
*---------------------------------------------------------------------*
"Subrutinas
*&---------------------------------------------------------------------*
*&      Form  SUB_RUTINE
*&---------------------------------------------------------------------*
*       Subrutine Description
*----------------------------------------------------------------------*
*       -->P_VAR1  Parameter Description
*       <--P_VAR2  Parameter Description
*----------------------------------------------------------------------*
FORM SUB RUTINE USING    P VAR1
                 CHANGING P VAR2.

ENDFORM.                    " SUB_RUTINE                              .
*---------------------------------------------------------------------*
```

Existe ya creado en SAP, el programa ZDE_RP_MODELO, que puede utilizarse como modelo para los desarrollos.

ESTÁNDARES EN REPORTES

No es solo como se verá un reporte lo que define el estándar. Se deben tomar en cuenta los factores de uso para el usuario como el desarrollo del mismo para poder crear un estándar beneficioso tanto a usuario como a desarrollador.

Consideraciones de Hardware

Se debe tomar en cuenta que realmente ninguna herramienta puede dar un resultado 100% WYSIWYG, así que los estándares tratan de dar una guía que logre semejanzas entre los formatos impresos.
Para iniciar se presentan ciertas sugerencias al momento de desarrollar los reportes:

- Utilizar el mínimo de fuentes de letras posibles. Las que se deben usar son:
  Courier New.
  Times New Roman.
  Lnprint.

La selección de ella dependerá de la impresora que se desee utilizar para la forma.

- Evitar el uso de colores en los reportes para prevenir problemas de impresión por el tipo de impresora o driver.
- No utilizar tipos de letra itálica (es más difícil de leer).
- No utilizar espacios en blanco muy extensos entre registros (consumen espacio en las páginas).

- Si un reporte será utilizado en impresión caracter o gráfica no generar dos reportes sino que el reporte pueda adaptarse a cada tipo de impresión.

Todas las formas pueden realizarse ya sea en SmartForms o SAPScript. El primero es una versión gráfica que facilita la programación, la segunda se refiere a la versión texto que se encuentra disponible de la versión 1 a la 4.x.

Para realizar las formas en SmartForms es necesario tomar en cuenta que estas pantallas se basaran en ventanas, las cuales contienen objetos que pueden ser:

- Máscaras de Edición
- Tablas
- Textos Dinámicos
- Comandos
- Líneas de Programa
- Carpetas
- Función Gráfica
- Direcciones
- Líneas IF

Encabezado

Cada una de las formas tiene un encabezado, un título en el cual se deben utilizar los objetos:

- Textos Dinámicos

Cambian de acuerdo a los requerimientos específicos de la forma.

- Includes

Se deben utilizar cuando la información que se requiere desplegar ya se encuentra en esta base de datos. Pues son nombres almacenados comúnmente utilizados por los programadores.

Cuerpo del Reporte

En este caso depende del tipo de reporte que se elabore, solo se dan algunos estándares para poder mantener el mismo Look & Feel en los reportes del sistema.

Se debe realizar con la ayuda de Tablas las cuales tienen su respectiva cabecera y detalle. En el detalle se utilizan por lo general textos dinámicos. En ambos, cuando se tienen varios campos, se deben utilizar las Máscaras de Edición, que tienen la función de una tabla invisible que permite alinear el texto de manera que en la impresión pueda ajustarse a los formatos predefinidos.

Si se desea realizar algún cambio a una forma debe de tomarse el código de acuerdo a sus respectivos estándares mencionados en este documento. Además deben utilizarse las opciones como por ejemplo las condiciones.

Otras Recomendaciones

Existe otro tipo de reporte que es muy común en la generación de informes, principalmente de tipo gerencial, estos reportes son los reportes de tipo ALV.

Estos reportes también son muy usados principalmente en donde se manejan cifras de dinero. La gran ventaja que representan sobre SAPScript y SmartForms es que permiten manipular en pantalla la organización de la información, es posible agregar o quitar columnas, totalizar, filtrar, exportar a diversos formatos como por ejemplo: XML, HTML, EXCEL, WORD en donde es posible agregarles funcionalidad o hacer ajustes de formato, para su impresión.

Recomendamos usar el tipo de salida ALV en la elaboración de reportes gerenciales y de resultados.

ANEXOS

ANEXO 1

INSTITUTO SALVADOREÑO DEL SEGURO SOCIAL
UNIDAD DE INFORMATICA
DEPARTAMENTO DE TECNOLOGÍA
SECCIÓN MANTENIMIENTO Y CONTROL DE EQUIPOS

ENTRADA Y SALIDA DE EQUIPO | **Fecha:**

MANTENIMIENTO: ____ RETIRO: ____ DEMOSTRACION: ___ TRASLADO:____

Se autoriza al (los) Sr.(es): | **De:**

Representante de la Empresa: | **A:**

PARA EFECTUAR EL MOVIMIENTO DE EQUIPO QUE SE DETALLA A CONTINUACIÓN:

DESCRIPCIÓN DEL EQUIPO	MARCA	TIPO	NÚMERO DE SERIE	NÚMERO DE INVENTARIO	PROPIEDAD DEL ISSS	
					SI	NO

OBSERVACIONES:

_____	_____	_____
JEFATURA Ó COORDINADOR QUE AUTORIZA	**PERSONA QUE TRASLADA EL EQUIPO**	**VIGILANTE DEL I.S.S.S.**

Anexo 2.a

INSTITUTO SALVADOREÑO DEL SEGURO SOCIAL
DIVISION DE INFORMATICA
SOLICITUD DE SERVICIOS DE RED

DATOS DEL USUARIO DE RED			
Fecha de solicitud :			
Nombres		No. de Empleado:	
Apellidos		Centro de Costo:	

DATOS DEL CENTRO DE TRABAJO			
Lugar del Centro de Trabajo			
Unidad o División			
Departamento			
Sección			
Cargo			
No. Inventario del equipo	- - - -		
Número de Teléfono		Extensión	
Firma Empleado			

Nombre de Jefe Inmediato			
Especificar servicio solicitado	☐ ACCESO A RED ☐ CORREO ☐ INTERNET ☐ ACCESO A CHAT* Cuenta de Usuario de Chat: _____	*Chat al que solicita acceso: ☐ Live MSN ☐ GoogleTalk ☐ YahooMSN ☐ Otro: _____	Vo. Bo. Jefe Inmediato
Justificación de servicio solicitado			

ESPACIO RESERVADO PARA DIVISION DE INFORMÁTICA				
Cuenta de Usuario de Red:				
Cuenta de Buzón de correo:				
Servicios Habilitados:	Responsable	Fecha de Creación	Hora de Creación:	Firma de Responsable
☐ ACCESO A RED				
☐ CORREO				
☐ INTERNET				
☐ ACCESO A CHAT				

ESPACIO RESERVADO PARA MANTENIMIENTO Y CONTROL DE EQUIPOS			
Responsable de Configuración:	Fecha de Configuración	Hora de Configuración	Firma de Responsable
Servicios Configurados:			

El uso de la red y recursos de información del ISSS, están disponibles para fortalecer el flujo de información interna, la investigación en materia administrativa, educativa y apoyar a las diferentes tareas encomendadas para mejoramiento de nuestras labores... el uso inapropiado de la red será sancionado con la eliminación del acceso a estos recursos y puede conllevar a la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables.

Anexo 2.b

INSTITUTO SALVADOREÑO DEL SEGURO SOCIAL
ADMINISTRACION DE RED
SOLICITUD DE CREACIÓN DE USUARIO DE RED

DATOS DEL USUARIO DE RED			
Fecha de solicitud :			
Nombres		No. De Empleado:	
Apellidos			

DATOS DEL CENTRO DE TRABAJO			
Lugar del Centro de Trabajo			
Departamento, Servicio o Dependencia			
Sección			
Cargo			
No. Inventario del equipo	- - - - - - - - - -		
Número de Teléfono		Extensión	
Firma Empleado			
Nombre de Jefe Inmediato			
Especificar Sistema a ser Utilizado	Agenda Médi ☐ Farmacia ☐ Laboratorio ☐ Emergencia ☐ Biometrico ☐ Rayos X ☐		
		Vo. Bo. Jefe Inmediato	
Justificación de servicio solicitado			

ESPACIO RESERVADO ADMINISTRACION DE RED		
Cuenta del Usuario	Fecha de Creación	Hora de Creación:
Sistemas o Servicios Habilitados		
	Administrador de Red	Firma :

La cuenta de usuario asignada es exclusivo del empleado solicitante y es responsabilidad de el mismo cambiar periódicamente su contraseña antes de que esta caduque; esta cuenta de usuario es intransferible; el uso inapropiado de la red y de los recursos informáticos, será sancionado con la eliminación del acceso a estos recursos y puede conllevar a la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables

Anexo 3

BITACORA DE ENTRADA Y SALIDA DE VISITANTES A CENTRO DE COMPUTO					
Fecha	Hora de Entrada	Hora de Salida	Nombre de Visitante	Asunto	Firma

Anexo 4

INSTITUTO SALVADOREÑO DEL SEGURO SOCIAL

CENTRO DE ATENCION

BITÁCORA DEL SERVIDOR

Administrador de red: _____

Nombre de servidor:

FECHA	HORA	DESCRIPCIÓN DEL PROBLEMA	SOLUCIÓN	OBSERVACIONES

Anexo 5

INSTITUTO SALVADOREÑO DEL SEGURO SOCIAL

"BITACORA DE RESPALDO DE ARCHIVOS"

Centro de atención: _____

Fecha: Respaldo [ ] Diario [ ] Semanal [ ] Mensual

Respaldo realizado por : _____

Hora de inicio: _____ Hora de Finalización: _____

Material

Cinta [ ] Software utilizado: _____

CD [ ]

DVD [ ]

Total de unidades utilizadas: _____

Volumen del Respaldo

Total de Archivos: _____

Total de MB: _____

Detalle de respaldo:

_____

_____

_____

_____

_____

_____

Observaciones o problemas :

_____

_____

_____

_____

_____

Anexo 6

INSTITUTO SALVADOREÑO DEL SEGURO SOCIAL

HOJA DE CONTROL DE RESPALDOS

Establecimiento: _____

Semana / Mes	Semana 1					Semana 2					Semana 3					Semana 4				
	L	M	M	J	V	L	M	M	J	V	L	M	M	J	V	L	M	M	J	V
Enero																				
Febrero																				
Marzo																				
Abril																				
Mayo																				
Junio																				
Julio																				
Agosto																				
Septiembre																				
Octubre																				
Noviembre																				
Diciembre																				

En cada celda se deberá indicar el tipo de respaldo realizado por la columna y el mes indicado por fila.

D= Respaldo Diario

S= Respaldo Semanal, Último día hábil de la semana

M= Respaldo mensual, Último día hábil, este día se deberán hacer dos copias

Pág. ____ de ____

Anexo 7

INSTITUTO SALVADOREÑO DEL SEGURO SOCIAL
DIVISIÓN DE INFORMÁTICA
SECCIÓN COMUNICACIÓ Y REDES INFORMÁTICAS

CONTROL Y ADMINISTRACIÓN DE LOS RECURSOS

A- REVISION DE COMPUTADORAS PERSONALES

1) Equipo esta conectado al servidor de red: SI ☐ NO ☐

Si la respuesta es negativa, completar:
Uso específico: _____

"Políticas y Estándares de Informática", sección 5.1) Administración de Computadoras y Equipo Informático, política 1: "Todas las computadoras personales deberán estar conectadas a algún servidor de red, excepción hecha de aquellas que por razones de uso específico, incompatibilidad, seguridad, distancia, falta de recursos, etc. no puedan ser conectadas".

Que recursos necesita para estar en red: _____

2) El recurso informático está protegido con las condiciones eléctricas mínimas:

Conectada a UPS: SI ☐ NO ☐

Conectada a Regulador de voltaje: SI ☐ NO ☐

"Políticas y Estándares de Informática", sección 5.1) Administración de Computadoras y Equipo Informático, política 2: "Bajo ninguna circunstancia los equipos deberán estar conectados a tomas de corriente comunes, a excepción de aquellas áreas en donde no existan suficientes tomas de acuerdo a la demanda de equipos conectados y en donde no se cuenten con recursos suficientes para realizar las conexiones necesarias. En estos casos deberán estar conectadas a un UPS el cual nunca deberá estar cerca de la computadora.".

3) El software instalado en el equipo software es institucional: SI ☐ NO ☐

Software no autorizado encontrado	Desinstalado
	☐
	☐
	☐
	☐
	☐
	☐
	☐
	☐

"Políticas y Estándares de Informática", sección 5.6) Licencias y Software de los Equipos, política 1: Las instalaciones del software se harán a través del personal de la División de Informática, mediante solicitud dirigida a la Sección Asistencia Informática y presentada por el representante de informática en la dependencia o Jefe inmediato superior.

Cont. Anexo 7

Aplicativos institucionales instalados:

Aplicativos desinstalados en la depuración trimestralmente:

Deberá

Borrar todos los archivos temporales e historiales, en la opción Herramientas, de Opciones de Internet, de su navegador.

Cuantos aplicativos tienen licencia: _____

Las carpetas compartidas tiene contraseñas: SI ☐ NO ☐

"Políticas y Estándares de Informática", sección 5.7) Uso de la Red Y Dominio Institucional, política 14: Las carpetas compartidas deberán estar delimitadas para ser accesadas solo para el personal que hará uso de ellos, el cual será definido por la jefatura del área solicitante.

4) Revisión de Logs críticos:

Aplicación:

Seguridad

Sistema:

5) Identificación y eliminación de usuarios locales con derechos de administrador:

6) Fecha de compra del equipo: _____

Cont. Anexo 7

B - SEGURIDAD EN LOS CENTROS DE CÓMPUTO

1)¿El acceso a las instalaciones físicas del Centro de Computo es un área restringida?

SI ☐ NO ☐

Si la respuesta es NO, ¿por que? _____

_____

_____

_____

1. "Políticas y Estándares de Informática", sección 16.1) Políticas de seguridad física, política 4: El acceso a las instalaciones físicas del Centro de Computo, serán áreas restringidas, únicamente podrán ingresar personas autorizadas, es decir personal de informática del ISSS, personal de mantenimiento de equipo que se presente a realizar labores de mantenimiento.

2) ¿Los sistemas de comunicaciones están debidamente protegidos con la infraestructura apropiada?

SI ☐ NO ☐

Si la respuesta es NO,¿ por que? _____

_____

_____

_____

"Políticas y Estándares de Informática", sección 16.1) Políticas de seguridad física, apartado a, política 3: Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario final no tenga acceso físico directo. Entendiendo por sistema de comunicaciones: el equipo activo y los medios de comunicación

3) ¿Los Equipos de Cómputo y Comunicación están protegidos con UPS de preferencia en línea para contrarrestar los cambios de voltaje existentes por la red energética?

SI ☐ NO ☐

"Políticas y Estándares de Informática", sección 16.1) Políticas de seguridad física, política, apartado b, política 3 : Los Equipos de Cómputo y Comunicación deberán estar protegidos con UPS de preferencia en línea para contrarrestar los cambios de voltaje existentes por la red energética.

4) El Centro de cómputo cuenta con Aire Acondicionado independiente?

SI ☐ NO ☐

"Políticas y Estándares de Informática", sección 16.1) Políticas de seguridad física, apartado b, política 5: Todos los centros de cómputo deben de contar con Aire Acondicionado independiente según requerimiento del espacio físico.

5) Los gabinetes de red y Racks permanecen con llave?

SI ☐ NO ☐

"Políticas y Estándares de Informática", sección 16.1) Políticas de seguridad física, apartado b, política 6: Los gabinetes de red y Racks deberán permanecer con llave.

Cont. Anexo 7

C - PROCEDIMIENTOS PARA CENTROS DE ATENCION

1)¿Esta habilitado el servicio de DHCP? SI ☐ NO ☐

Específico el rango de IP´s excluidas

_____
_____
_____
_____
_____
_____
_____
_____
_____

"Políticas y Estándares de Informática", sección 16.5) Direccionamiento IP en centros de atención: Asignación de direcciones IP, de manera automatizada, mediante la utilización de DHCP (Dinamic Host Configuration Protocol)

2) La asignación del nombre de cuenta es realizada de acuerdo a la política y estándares de informática:

SI ☐ NO ☐

"Políticas y Estándares de Informática", sección 16.4) Directorio Activo y Carpetas de Aplicaciones, política 1: La estructura de Directorios, y de Directorio Activo, será por medio de Contenedores.

3) ¿La estructura del Directorio Activo está diseñada por medio de Contenedores?

SI ☐ NO ☐

"Políticas y Estándares de Informática", sección 16.4) Directorio Activo y Carpetas de Aplicaciones, apartdo Directorio activo: Como parte de la Organización Institucional de cada centro de atención se crearan unidades Organizativas, y se nombraran según las aplicaciones que se instalaran.

4) El diagrama de red se encuentra actualizado: SI ☐ NO ☐

Si su respuesta es negativa, especifique fecha de actualización: _____

"Políticas y Estándares de Informática", sección 16.4) Directorio Activo y Carpetas de Aplicaciones, apartado Diagrama de red de datos, política 6: Cada Administrador de red deberá realizar un diagrama de red de su centro de atención, elaborado en el software que proporcione la división de informática.

5) El inventario de equipo informático esta actualizado: SI ☐ NO ☐

Si su respuesta es negativa, especifique fecha de actualización: _____

"Políticas y Estándares de Informática", sección 16.4) Directorio Activo y Carpetas de Aplicaciones, apartado Diagrama de red de datos, política 7: Cada administrador de red deberá mantener un inventario de equipo informático, en el que pueda identificarse fácilmente movimientos de entrada salida, características de los equipos, descartes, etc.

Anexo 8

INSTITUTO SALVADOREÑO DEL SEGURO SOCIAL
DIVISIÓN DE INFORMÁTICA
Centro de Atención
Bitácora de creación de usuarios.

Fecha de creación: _____

Usuario solicitante — No. Empleado:
Primer nombre: — Segundo nombre:
Primer apellido: — Segundo apellido:
Apellido de casada

Centro de Costo _____ Teléfono: _____
Dependencia _____
Puesto _____
Ubicación _____

Tipo de cuenta — Personal [X] — Genérica [X]

Nombre de usuarios que acceden con cuenta genérica:
1-
2-
3-
4-
5-

Nombre de cuenta: _____

Correo Electrónico: — ISSS [X] — Local [X]

Miembro de Grupos _____

Administrador de red: _____

Anexo 9

INSTITUTO SALVADOREÑO DEL SEGURO SOCIAL
DIVISIÓN DE INFORMÁTICA
Centro de Atención
Bitácora de creación de grupos.

Fecha de creación: _____

Nombre de grupo:

Nombre de sistemas:

Derechos a carpetas

Descripción:

Miembros del grupo (Nombre de cuenta)

Administrador de red: _____