UNIVERSIDAD JOSÉ CARLOS MARIÁTEGUI

ING. DE SISTEMAS E INFORMÁTICA

AUDITORIA INFORMATICA MUNICIPALIDAD PROVINCIAL MARISCAL

INTEGRANTES:

- ORLANDO JIMMY MAMANI POMA
- MICHELLA AROHUANCA A.
- WILLY MAMANI CUTIPA
- CARMEN QUIÑONEZ MAYTA
- MADELEINE MUÑOZ ORTEGA
- NELSSY POCOHUANCA TURPO


AUDITORIA
INFORMATICA
Auditoria a sistemas de Computo

CAPITULO I

AUDITORIA INFORMATICA

AUDITORIA INFORMATICA

1.1.ORIGEN DE LA AUDITORIA:

La presente Auditoria se realiza en cumplimiento del Plan Anual de Control 2003, aprobada mediante Resolución de Contraloría N° 235- 2002-CG del 15 de Diciembre del 2002.

1.2.OBJETIVOS Y ALCANCE

1.2.1. OBJETIVO GENERAL

Revisar y Evaluar los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

1.2.2. OBJETIVOS ESPECIFICOS

- Evaluar el diseño y prueba de los sistemas del área de Informática
- Determinar la veracidad de la información del área de Informática
- Evaluar los procedimientos de control de operación, analizar su estandarización y evaluar el cumplimiento de los mismos.
- Evaluar la forma como se administran los dispositivos de almacenamiento básico del área de Informática
- Evaluar el control que se tiene sobre el mantenimiento y las fallas de las Pcs.
- Verificar las disposiciones y reglamentos que coadyuven al mantenimiento del orden dentro del departamento de cómputo.

1.3.ANTECEDENTES

La convención Nacional el 29 de Diciembre de 1857 aprueba la ley que es promulgada por el libertador Ramón Castilla disponiendo q el Dpto. de Moquegua, conformando por 04 provincias: Tacna, Arica, Tarapacá y Moquegua, entre otros Dptos., procedan a constituir juntas electorales en las capitales de Dptos., provincias y distritos, para q se elijan las primeras Municipalidades establecidas por la constitución.

En la Capital de la Provincia de Moquegua, debían elegirse 11 Municipalidades, en el resto de la Provincia (Torata, Omate, Ubinas, Carumas, Puquina, Iloe Ichuña)el numero de Municipalidades variaban de 3 a 5 miembros.

Exactamente no se conoce la fecha cuando comenzaron las funciones municipalidades en Moquegua, trabajo de investigación histórica que es necesario abocarse para que bajo su conocimiento se de luces y perspectivas en el desenvolvimiento participatorio de la comunidad en el desarrollo de la municipalidad.

Anteriormente, el gobierno local de la provincia de Mariscal Nieto-Moquegua ocupaba una casona ubicada en la calle Moquegua N° 851, inmueble cuya construcción data de 1799 y que fue donada a la Municipalidad de Moquegua el 05 de Setiembre de 1945.

Actualmente la Municipalidad Provincial de Mariscal Nieto cuenta con una infraestructura moderna ubicada en la calle Ancash N°275

1.4.ENFOQUE A UTILIZAR

- La presente acción de control, se realiza de acuerdo con el organismo central y rector de los Sistemas Nacionales de Estadística e Informática, responsable de normar, supervisar y evaluar los métodos, procedimientos y técnicas estadísticas e informáticas utilizados por los órganos del Sistema INEI (Instituto Nacional de Estadística e Informática), Normas Internacionales de Auditoria (NIA); habiéndose aplicado procedimientos de Auditoria que se consideraron necesarios de acuerdo a las circunstancias.

- La presente Auditoria Informática se realizara en la Municipalidad Provincial de Mariscal Nieto, ubicada en el Distrito de Moquegua, Provincia Mariscal Nieto Departamento de Moquegua, siendo el área a examinarse la de Informática.

1.5.RELACION DE FUNCIONARIOS O PERSONAL A CARGO DEL AREA A EXAMINAR

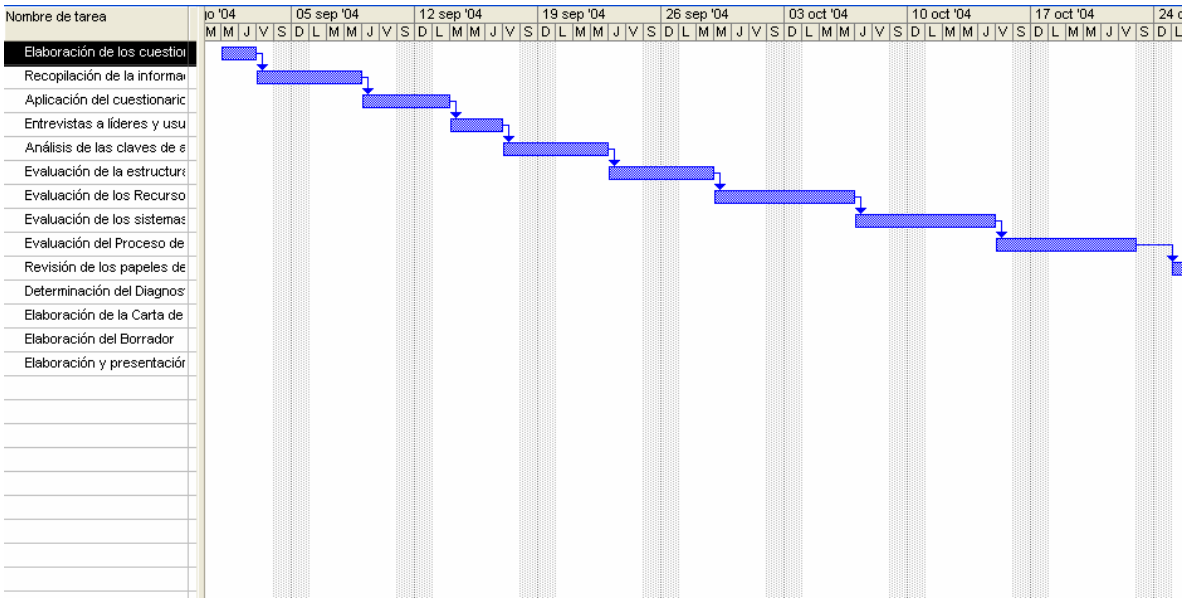
Apellidos Nombres	Cargo	Periodo de Gestión		Domicilio
		Del	Al	
Cervantes Games, Ivan	Jefe	01.01.03	30.12.03	Av. Balta N°232
Manchiria Zeballos, Victoria	Planillas	01.01.03	30.12.03	Calle Lima Nº 44
Velasquez Zapata, Sonia	Secretaria	01.01.03	30.12.03	Calle Moquegua N°145
Gamez Villa, Celia	Secretaria	01.01.03	30.12.03	Calle Lima N°1420

1.6.CRONOGRAMA DE TRABAJO

PROGRAMA DE AUDITORIA			
EMPRESA: Municipalidad Provincial Mariscal Nieto		FECHA:	HOJA N°
FASE	ACTIVIDAD	HORAS ESTIMADAS	ENCARGADOS
I	VISITA PRELIMINAR • Solicitud de Manuales y Documentaciones. • Elaboración de los cuestionarios. • Recopilación de la información organizacional: estructura orgánica, recursos humanos, presupuestos.	8 HS.	

II	DESARROLLO DE LA AUDITORIA • Aplicación del cuestionario al personal. • Entrevistas a líderes y usuarios mas relevantes de la dirección. • Análisis de las claves de acceso, control, seguridad, confiabilidad y respaldos. • Evaluación de la estructura orgánica: departamentos, puestos, funciones, autoridad y responsabilidades. • Evaluación de los Recursos Humanos y de la situación Presupuestal y Financiera: desempeño, capacitación, condiciones de trabajo, recursos en materiales y financieros mobiliario y equipos. • Evaluación de los sistemas: relevamiento de Hardware y Software, evaluación del diseño lógico y del desarrollo del sistema. • Evaluación del Proceso de Datos y de los Equipos de Cómputos: seguridad de los datos, control de operación, seguridad física y procedimientos de respaldo.	32 HS.	
III	REVISION Y PRE-INFORME • Revisión de los papeles de trabajo. • Determinación del Diagnostico e Implicancias. • Elaboración de la Carta de Gerencia. • Elaboración del Borrador.	16 HS.	
IV	INFORME • Elaboración y presentación del Informe.	4 HS.	

DIAGRAMA DE GANTT



1.7.DOCUMENTOS A SOLICITAR

- Políticas, estándares, normas y procedimientos.
- Plan de sistemas.
- Planes de seguridad y continuidad
- Contratos, pólizas de seguros.
- Organigrama y manual de funciones.
- Manuales de sistemas.
- Registros
- Entrevistas
- Archivos
- Requerimientos de Usuarios

1.8.EJECUCION DE LA REVISION ESTRATEGICA

1.8.1. CONOCIMIENTO INICIAL DE LA ENTIDAD

Anteriormente, el gobierno local de la provincia de Mariscal Nieto-Moquegua ocupaba una casona ubicada en la calle Moquegua N° 851, inmueble cuya

construcción data de 1799 y que fue donada a la Municipalidad de Moquegua el 05 de Setiembre de 1945.

Actualmente la Municipalidad Provincial de Mariscal Nieto cuenta con una infraestructura moderna ubicada en la calle Ancash N°275

1.8.2. AUTORIDADES DE LA MUNICIPALIDAD PROVINCIAL DE MARISCAL NIETO

NOMBRE	CARGO
Dr. Vicente Antonio Zeballos Salinas	Alcalde
Dr. Javier Flores Arocutipa	Vicerrector
Mag. Hilda Guevara Gomez	Decana de la Facultad de Ciencias de la Salud
Ing. Oscar Paredes Vargas	Decano de la Facultad de Ingeniería
Mag. Victor Cornejo Rodriguez	Decano de Cs.Jurídicas, Empresariales y Pedagógicas.

1.8.3. PRINCIPALES ACTIVIDADES:

- Acordar su régimen de Órgano Interior
- Aprobar su presupuesto
- Aprobar sus Bienes y Rentas
- Crear, modificar, suprimir o examinar sus contribuciones, atribuciones y derecho, conforme a Ley.
- Organizar, Reglamentar y Administrar sus servicios públicos locales.

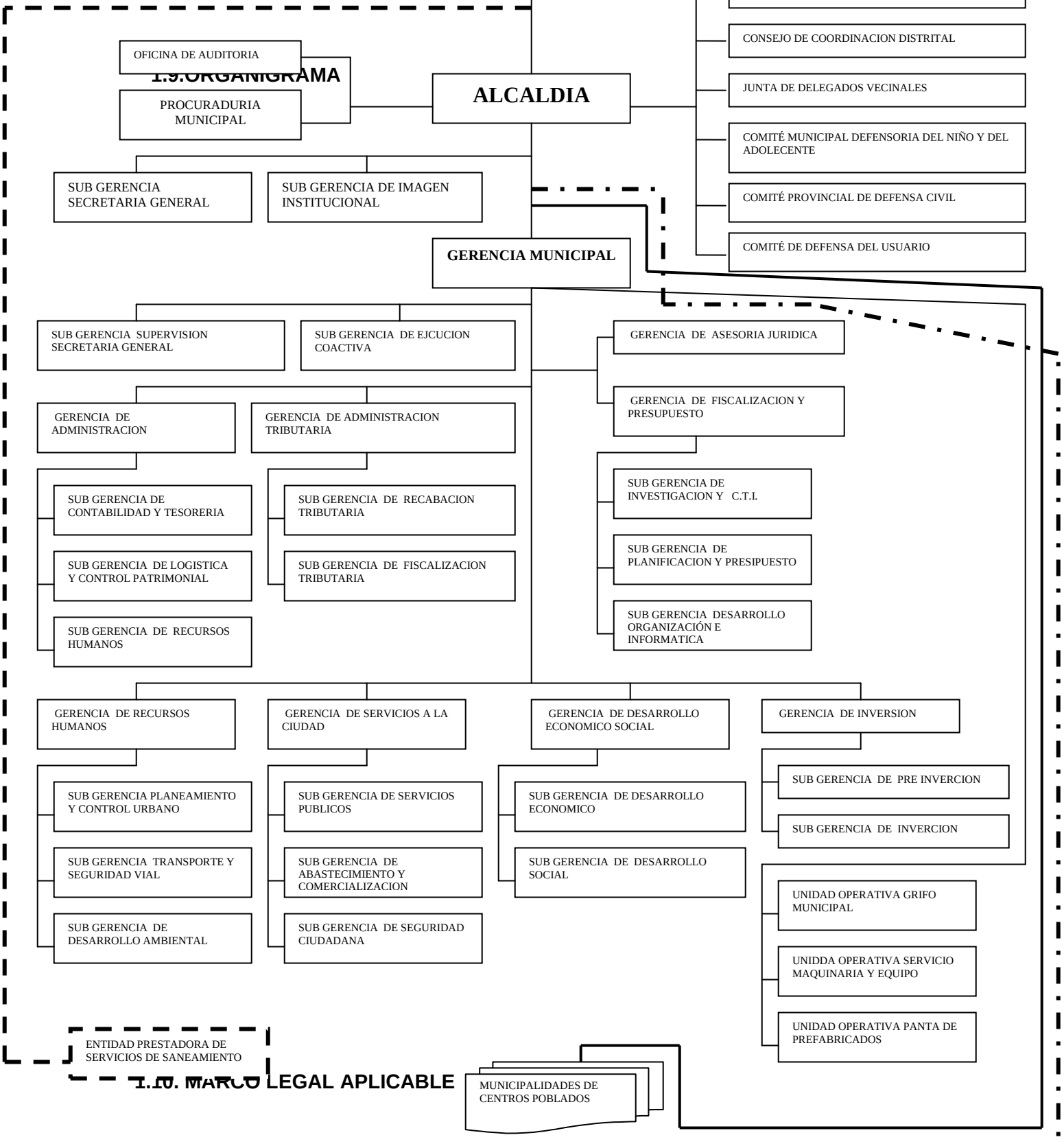
- Contratar con otras entidades públicas y no públicas, preferentemente locales, la atención de los servicios que no administraron directamente.
- Planificar el desarrollo de sus pueblos y ejecutar los planes correspondientes.

- Examinar el cumplimiento de sus propias Normas, a través de sus propios medios o con el auxiliar de las fuerzas policiales.
- Celebrar contratos con otros municipios para organizar servicios comunes.
- Promover y organizar la participación de los vecinos en el desarrollo comunal.

1.8.4. FUNCIONES GENERALES

- Planificar, ejecutar e impulsar, a través de los órganos correspondientes, el conjunto de acciones destinadas a proporcionar al ciudadano, el ambiente adecuado para las satisfacciones de sus necesidades viales de vivienda, salubridad, abastecimiento, educación, recreación, transporte y comunicación.
- Formular el plan de desarrollo distrital en concordancia con las necesidades y requerimientos de la población organizada y los planes de desarrollo nacional y regional.
- Conducir los programas de acondicionamiento territorial, vivienda y seguridad colectiva, conforme lo establece la ley orgánica de municipalidades, velando por su ejecución.

1.9.ORGANIGRAMA



1.10. MARCO LEGAL APLICABLE

La base normativa empleada está compuesta por las Normas Internacionales de Auditoría (NIA´s) 1001 “Sistemas de Microcomputadoras”, 1002 “Sistemas de Microcomputadoras en Línea”, 1003 “Sistemas de Bases de Datos”, 1008 “Evaluación de Riesgos y Control Interno” y el marco COBIT.

1.11. SISTEMAS Y CONTROLES IDENTIFICADOS

a) Control de Actividades y Operaciones.

- La Municipalidad Provincial de Mariscal Nieto a formulado el Reglamento de Organización y Funciones (ROF),
- Asimismo la entidad ha formulado el Manual de Organización y Funciones.

b) Controles de Confiabilidad y Validez de la Información.

- Las funciones y responsabilidades de cada funcionario y/o directivo están establecidas en el Reglamento General Interno, Reglamento de Organización y Funciones (ROF).

1.12. OFICINA DE PLANEACION Y PRESUPUESTO

1.12.1. AREA DE COMPUTO E INFORMATICA

MISION

El área de Computo e informática de la municipalidad Provincial de Mariscal Nieto– Moquegua, tiene por misión normar el adecuado uso y aprovechamiento de los recursos informáticos; la optimización de las actividades, servicios procesos y acceso inmediato a información para la toma de decisiones, mediante el desarrollo, implantación y supervisión del correcto funcionamiento de los sistemas

y comunicaciones, así como la adquisición y control de la plataforma física de computo.

VISION:

El Área de cómputo e informática, de la Municipalidad Provincial Mariscal Nieto, capaz de liderar el desarrollo informático, asegurando un marco transparente para el acceso a los ciudadanos a la información

1.12.2. SITUACION ACTUAL

Ubicación:

El área de cómputo e informática orgánicamente depende de la oficina de planificación y presupuesto, asumiendo la responsabilidad de dirigir los procesos técnicos de informática

Recursos Humanos:

Actualmente en el área de cómputo e informática labora una sola persona quien cumple las funciones de administración, capacitación, soporte y procesamiento de datos.

Recursos informáticos existentes:

Servidores (Windows 2000 Server)	1
Computadoras Personales	2
Impresoras	1

1.12.3. OBJETIVOS:

El área de Cómputo e informática tiene los siguientes objetivos Sectoriales:

- Apoyar a las Municipalidades Distritales de la Provincia de Mariscal Nieto.

- Estandarizar y Uniformizar información relevante referente a los gobiernos locales
- Brindar un mejor servicio a los usuarios de Moquegua, a través de una pagina Web

OBJETIVOS ESPECIFICOS (PRESUPUESTADOS):

- Equipamiento de la gestión Municipal.
- Optimizar las aplicaciones existentes a satisfacción de la municipalidad.
- Digitalización de Partidas de Nacimiento, Matrimonio y Defunción
- Brindar acceso a Internet
- Diseño y elaboración de páginas Web.
- Alojamiento y Mantenimiento de la Pagina Web.

1.12.4. ANALISIS FODA

- **Fortalezas**

  - Disponibilidad de recursos económicos.
  - Personal Directivo y técnico con amplia experiencia(recursos humanos)
  - Capacidad de Convocatoria(Difusión)

- **Oportunidades**

  - Búsqueda de reducción de costos, aprovechando la aparición de nuevas tecnologías.
  - Buen servicio y trato.
  - Tendencias Tecnológicas generan un amplio campo de acción
  - Predisposición y voluntad de los nuevos directivos para cambio Tecnológico

- **Debilidades**

  - Falta de planes y Programas Informáticos.
  - Poca identificación del personal con la institución
  - Inestabilidad laboral del personal
  - Escasa capacidad de retención y voluntad del personal
  - No existe programas de capacitación y actualización al personal
  - La oficina del Área de computo e informática muy reducido
  - Personal técnico Calificado insuficiente en el área de computo

- **Amenazas**

  - Rotación permanente del personal imposibilitando continuidad a los objetivos propuestos.
  - Estandarizar y Uniformizar información relevante referente a los gobiernos locales.

PLAN DE AUDITORIA

2.1.METODOLOGIA

La metodología de investigación a utilizar en el proyecto se presenta a continuación:
Para la evaluación del Área de Informática se llevarán a cabo las siguientes actividades:

- Solicitud de los estándares utilizados y programa de trabajo
- Aplicación del cuestionario al personal
- Análisis y evaluación del a información
- Elaboración del informe
- Para la evaluación de los sistemas tanto en operación como en desarrollo se llevarán a cabo las siguientes actividades:
    - Solicitud del análisis y diseño del os sistemas en desarrollo y en operación
    - Solicitud de la documentación de los sistemas en operación (manuales técnicos, de operación del usuario, diseño de archivos y programas)
    - Recopilación y análisis de los procedimientos administrativos de cada sistema (flujo de información, formatos, reportes y consultas)
    - Análisis de llaves, redundancia, control, seguridad, confidencial y respaldos
    - Análisis del avance de los proyectos en desarrollo, prioridades y personal asignado
    - Entrevista con los usuarios de los sistemas
    - Evaluación directa de la información obtenida contra las necesidades y requerimientos del usuario
    - Análisis objetivo de la estructuración y flujo de los programas
    - Análisis y evaluación de la información recopilada
    - Elaboración del informe
- Para la evaluación de los equipos se llevarán a cabo las siguientes actividades:
    - Solicitud de los estudios de viabilidad y características de los equipos actuales, proyectos sobre ampliación de equipo, su actualización

- Solicitud de contratos de compra y mantenimientos de equipo y sistemas
- Solicitud de contratos y convenios de respaldo
- Solicitud de contratos de Seguros
- Elaboración de un cuestionario sobre la utilización de equipos, memoria, archivos, unidades de entrada/salida, equipos periféricos y su seguridad
- Visita técnica de comprobación de seguridad física y lógica de la instalaciones de la Dirección de Informática
- Evaluación técnica del sistema electrónico y ambiental de los equipos y del local utilizado
- Evaluación de la información recopilada, obtención de gráficas, porcentaje de utilización de los equipos y su justificación

↳ Elaboración y presentación del informe final (conclusiones y recomendaciones)

2.2.JUSTIFICACION

- Aumento considerable e injustificado del presupuesto del PAD (Departamento de Procesamiento de Datos)
- Desconocimiento en el nivel directivo de la situación informática de la empresa
- Falta total o parcial de seguridades lógicas y fisicas que garanticen la integridad del personal, equipos e información.
- Descubrimiento de fraudes efectuados con el computador
- Falta de una planificación informática
- Organización que no funciona correctamente, falta de políticas, objetivos, normas, metodología, asignación de tareas y adecuada administración del Recurso Humano
- Descontento general de los usuarios por incumplimiento de plazos y mala calidad de los resultados
- Falta de documentación o documentación incompleta de sistemas que revela la dificultad de efectuar el mantenimiento de los sistemas en producción

2.3.MOTIVO O NECESIDAD DE UNA AUDITORIA INOFRMATICA:

2.3.1. Síntomas de descoordinación y desorganización:

- No coinciden los objetivos del área de Informática y de la propia Institución.
- Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente. Puede ocurrir con algún cambio masivo de personal, o en una reestructuración fallida de alguna área o en la modificación de alguna Norma importante

2.3.2. Síntomas de mala imagen e insatisfacción de los usuarios:

- No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de software en los terminales de usuario, resfrecamiento de paneles, variación de los ficheros que deben ponerse diariamente a su disposición, etc.
- No se reparan las averías de hardware ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.
- No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de Aplicaciones críticas y sensibles.

2.3.3. Síntomas de debilidades económico-financiero:

- Incremento desmesurado de costes.
- Necesidad de justificación de Inversiones Informáticas (la empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).
- Desviaciones Presupuestarias significativas.
- Costes y plazos de nuevos proyectos (deben auditarse simultáneamente a Desarrollo de Proyectos y al órgano que realizó la petición).

2.3.4. **Síntomas de Inseguridad:** Evaluación de nivel de riesgos

- Seguridad Lógica
- Seguridad Física

- Confidencialidad

- Los datos son propiedad inicialmente de la organización que los genera. Los datos de personal son especialmente confidenciales

CAPITULO

II

AUDITORIAS

AUDITORIA FISICA

1. Alcance de la Auditoria

- Organización y cualificación del personal de Seguridad.
- Remodelar el ambiente de trabajo.
- Planes y procedimientos.
- Sistemas técnicos de Seguridad y Protección.

2. Objetivos

- Revisión de las políticas y Normas sobre seguridad Física.
- Verificar la seguridad de personal, datos, hardware, software e instalaciones
- Seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático

PREGUNTAS	SI	NO	N/A
1. ¿Se han adoptado medidas de seguridad en el departamento de sistemas de información?		X	
2. ¿Existe una persona responsable de la seguridad?		X	
3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?		X	
4. ¿Existe personal de vigilancia en la institución?	X		
5. ¿Existe una clara definición de funciones entre los puestos clave?		X	
6. ¿Se investiga a los vigilantes cuando son contratados directamente?		X	
7. ¿Se controla el trabajo fuera de horario?		X	
8. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas?.	X		
9. ¿Existe vigilancia en el departamento de cómputo las 24 horas?		X	
10. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?		X	
11. ¿Se ha instruido a estas personas sobre que medidas tomar en caso de que alguien pretenda entrar sin autorización?		X	

12. ¿El centro de cómputo tiene salida al exterior?		**X**	
13. ¿Son controladas las visitas y demostraciones en el centro de cómputo?	**X**		
14. ¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática?	**X**		
15. ¿Se vigilan la moral y comportamiento del personal de la dirección de informática con el fin de mantener una buena imagen y evitar un posible fraude?		**X**	
16. ¿Se ha adiestrado el personal en el manejo de los extintores?		**X**	
17. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?		**X**	
18. ¿Si es que existen extintores automáticos son activador por detectores automáticos de fuego?		**X**	
19. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?		**X**	
20. ¿Saben que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego?	**X**		
21. ¿El personal ajeno a operación sabe que hacer en el caso de una emergencia (incendio)?		**X**	
22. ¿Existe salida de emergencia?		**X**	
23. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?			
24. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?	**X**		
25. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo?	**X**		
26. ¿Se limpia con frecuencia el polvo acumulado debajo del piso falso si existe?	**X**		
27. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?		**X**	
28. ¿Se tienen establecidos procedimientos de actualización a estas copias?		**X**	
29. ¿Existe departamento de auditoria interna en la institución?	**X**		
30. ¿Este departamento de auditoria interna conoce todos los aspectos de los sistemas?		**X**	
31. ¿Se cumplen?		**X**	
32. ¿Se auditan los sistemas en operación?		**X**	
33. Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?	**X**		
34. ¿Existe control estricto en las modificaciones?	**X**		
35. ¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?	**X**		
36. ¿Si se tienen terminales conectadas, ¿se ha establecido procedimientos de operación?		**X**	
37. ¿Se ha establecido que información puede ser acezada y por qué persona?		**X**	

Auditoria física:

- **Para hallar el SI**

37 ⟶ 100%
13 ⟶ X

X = 31.1

- **Para hallar el NO**

37 ⟶ 100%
24 ⟶ X

X = 64.86

LISTADO DE VERIFICACIÓN DE AUDITORIA FISICA

Gestión física de seguridad.

	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
Los objetivos de la instalación física De computo					✔
Las características físicas de son seguras de centro				✔	
Los componentes físicos de computo		✔			
La conexiones de los equipos de las comunicaciones e instalaciones físicas			✔		
La infraestructura es			✔		
El equipos es			✔		
La distribución de los quipos de computo es				✔	

Evaluación de análisis física de cómputo

	100%	80%	60%	40%	20%

	Excelente	Bueno	Regular	Mínimo	No cumple
Evaluación de la existencia y uso de normas, resolución base legal para el diseño del centro de computo.					✔
El cumplimiento de los objetivos fundamentales de la organización para instalar del centro de cómputo.					✔
La forma de repartir los recursos informáticos de la organización.					✔
La confiabilidad y seguridades el uso de la información institucional				✔	
La satisfacción de las necesidades de poder computacional de la organización.				✔	
La solución a identificación del centro de cómputo (apoyó).		✔			

Análisis de la delimitación la manera en que se cumplen:

	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
La delimitación espacial, por las dimensiones físicas.					✔
La delimitación tecnológica, por los requerimientos y conocimientos informáticos.				✔	

Análisis de la estabilidad y el aprovechamiento de los recursos a para instalar el centro de computo.

	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Análisis de la transparencia del trabajo para los usuarios.			✔		
La ubicación del centro de computo					
Los requerimientos de seguridad del centro de computo				✔	

Evaluación del diseño según el ámbito

	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Análisis del ambiente de trabajo				✔	
Evaluar el funcionamiento de los equipos			✔		
El local para el trabajo es				✔	
Los equipos cuentan con ventilación		✔			

La iluminación		✔			

Análisis de la seguridad física

	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
La seguridad de los equipos.			✔		
El estado centro de computo esta en			✔		
Los accesos de salida son			✔		

INFORME DE AUDITORIA

1. **Identificación del informe**

   Auditoria física.

2. **Identificación del Cliente**

   El área de Informática

3. **Identificación de la Entidad Auditada**

   Municipalidad Provincial de Moquegua.

4. **Objetivos**

   - Verificar la estructura de distribución de los equipos.
   - Revisar la correcta utilización de los equipos
   - Verificar la condición del centro de cómputo.

5. **Hallazgos Potenciales**

   - Falta de presupuesto y personal.
   - Falta de un local mas amplio
   - No existe un calendario de mantenimiento
   - Falta de ventilación.
   - .faltan salida al exterior
   - Existe salidas de emergencia.

6. **Alcance de la auditoria**

   Nuestra auditoria, comprende el presente periodo 2004 y se ha realizado especialmente al Departamento de centro de cómputo de acuerdo a las normas y demás disposiciones aplicable al efecto.

7. Conclusiones:

- Como resultado de la Auditoria podemos manifestar que hemos cumplido con evaluar cada uno de los objetivos contenidos en el programa de auditoria.

- El Departamento de centro de cómputo presenta deficiencias sobre todo en el debido cumplimiento de Normas de seguridad.

8. Recomendaciones

- Reubicación del local
- Implantación de equipos de ultima generación
- Implantar equipos de ventilación
- Implantar salidas de emergencia.
- Elaborar un calendario de mantenimiento de rutina periódico .
- Capacitar al personal.

9. Fecha Del Informe

	PLANEAMIENTO	EJECUCION	INFORME
FECHAS	01–10–04 al 15–10-04	16-10–04 al 20–11-04	23–11–04 al 28–11-04

10. Identificación Y Firma Del Auditor

APELLIDOS Y NOMBRES	CARGO
MAMANI CUTIPA WILY	AUDITOR SUPERIOR

AUDITORIA DE LA OFIMATICA

1. Alcance de la Auditoria.-

- Planes y procedimientos
- Políticas de Mantenimiento
- Inventarios Ofimaticos
- Capacitación del Personal

2. Objetivos de la Auditoria.-

Realizar un informe de Auditoria con el objeto de verificar la existencia de controles preventivos, detectivos y correctivos, así como el cumplimiento de los mismos por los usuarios.

PREGUNTAS	SI	NO	N/A
1. ¿Existe un informe técnico en el que se justifique la adquisición del equipo, software y servicios de computación, incluyendo un estudio costo-beneficio?		✔	
2. ¿Existe un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación?		✔	
3. ¿Han elaborado un instructivo con procedimientos a seguir para la selección y adquisición de equipos, programas y servicios computacionales?	✔		
4. ¿se cuenta con software de oficina?	✔		
5. ¿Se han efectuado las acciones necesarias para una mayor participación de proveedores?	✔		

6. ¿Se ha asegurado un respaldo de mantenimiento y asistencia técnica?	✔		
7. ¿El acceso al centro de cómputo cuenta con las seguridades necesarias para reservar el ingreso al personal autorizado?		✔	
8. ¿Se han implantado claves o password para garantizar operación de consola y equipo central (mainframe), a personal autorizado?	✔		
9. ¿Se han formulado políticas respecto a seguridad, privacidad y protección de las facilidades de procesamiento ante eventos como: incendio, vandalismo, robo y uso indebido, intentos de violación?	✔		
10. ¿Se mantiene un registro permanente (bitácora) de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos?		✔	
11. ¿Los operadores del equipo central están entrenados para recuperar o restaurar información en caso de destrucción de archivos?	✔		
12. ¿Los backups son mayores de dos (padres e hijos) y se guardan en lugares seguros y adecuados, preferentemente en bóvedas de bancos?		✔	
13. ¿Se han implantado calendarios de operación a fin de establecer prioridades de proceso?		✔	
14. ¿Todas las actividades del Centro de Computo están normadas mediante manuales, instructivos, normas, reglamentos, etc.?	✔		
15. ¿Las instalaciones cuentan con sistema de alarma por presencia de fuego, humo, así como extintores de incendio, conexiones eléctricas			✔

seguras, entre otras?			
16. ¿Se han instalado equipos que protejan la información y los dispositivos en caso de variación de voltaje como: reguladores de voltaje, supresores pico, UPS, generadores de energía?		✔	
17. ¿Se han contratado pólizas de seguros para proteger la información, equipos, personal y todo riesgo que se produzca por casos fortuitos o mala operación?	✔		
18. ¿Se han Adquirido equipos de protección como supresores de pico, reguladores de voltaje y de ser posible UPS previo a la adquisición del equipo?	✔		
19. ¿Si se vence la garantía de mantenimiento del proveedor se contrata mantenimiento preventivo y correctivo?	✔		
20. ¿Se establecen procedimientos para obtención de backups de paquetes y de archivos de datos?	✔		
21. ¿Se hacen revisiones periódicas y sorpresivas del contenido del disco para verificar la instalación de aplicaciones no relacionadas a la gestión de la empresa?			✔
22. ¿Se mantiene programas y procedimientos de detección e inmunización de virus en copias no autorizadas o datos procesados en otros equipos?	✔		
23. ¿Se propende a la estandarización del Sistema Operativo, software utilizado como procesadores de palabras, hojas electrónicas, manejadores de base de datos y se mantienen actualizadas las versiones y la capacitación sobre modificaciones incluidas?	✔		

24. existen licencias	✔		

Auditoria Ofimática .-

- **Para hallar el SI**

  24 ⟶ 100%
  15 ⟶ X

  X = 62.5

- **Para hallar el NO**

  24 ⟶ 100%
  7 ⟶ X

  X = 18.91

INFORME DE AUDITORIA

1. **Identificación del informe**

   Auditoria de la Ofimática

2. **Identificación del Cliente**

   El área de Informática

3. **Identificación de la Entidad Auditada**

   Municipalidad Provincial Mariscal Nieto

4. **Objetivos**

- Verificar si el hardware y software se adquieren siempre y cuando tengan la seguridad de que los sistemas computarizados proporcionaran mayores beneficios que cualquier otra alternativa.
- Verificar si la selección de equipos y sistemas de computación es adecuada
- Verificar la existencia de un plan de actividades previo a la instalación
- Verificar que los procesos de compra de Tecnología de Información, deben estar sustentados en Políticas, Procedimientos, Reglamentos y Normatividad en General, que aseguren que todo el proceso se realiza en un marco de legalidad y cumpliendo con las verdaderas necesidades de la organización para hoy y el futuro, sin caer en omisiones, excesos o incumplimientos.
- Verificar si existen garantías para proteger la integridad de los recursos informáticos.
- Verificar la utilización adecuada de equipos acorde a planes y objetivos.

5. Hallazgos Potenciales

- Falta de licencias de software.
- Falta de software de aplicaciones actualizados
- No existe un calendario de mantenimiento ofimatico.
- Faltan material ofimática.

- Carece de seguridad en Acceso restringido de los equipos ofimaticos y software.

6. Alcance de la auditoria

Nuestra auditoria, comprende el presente periodo 2004 y se ha realizado especialmente al Departamento de centro de cómputo de acuerdo a las normas y demás disposiciones aplicable al efecto.

El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoria Ofimática, se complementa con los objetivos de ésta.

7. Conclusiones:

- Como resultado de la Auditoria podemos manifestar que hemos cumplido con evaluar cada uno de los objetivos contenidos en el programa de auditoria.
- El Departamento de centro de cómputo presenta deficiencias sobre el debido cumplimiento de Normas de seguridad.
- La escasez de personal debidamente capacitado.
- Cabe destacar que la sistema ofimatico pudiera servir de gran apoyo a la organización, el cual no es explotado en su totalidad por falta de personal capacitado.

8. Recomendaciones

- Se recomienda contar con sellos y firmas digitales
- Un de manual de funciones para cada puesto de trabajo dentro del área.
- Reactualizacion de datos.
- Implantación de equipos de ultima generación

- Elaborar un calendario de mantenimiento de rutina periódico .
- Capacitar al personal.

9. Fecha Del Informe

	PLANEAMIENTO	EJECUCION	INFORME
FECHAS	01–10–04 al 15–10-04	16-10–04 al 20–11-04	23–11–04 al 28–11-04

10. Identificación Y Firma Del Auditor

APELLIDOS Y NOMBRES	CARGO
QUIÑONEZ MAYTA CARMEN	AUDITOR SUPERIOR

AUDITORIA DE LA DIRECCION

1. Alcance de la Auditoria.-

- Organización y calificación de la dirección de Informática
- Plan Estratégico de Sistemas de Información.
- Análisis de puestos
- Planes y Procedimientos
- Normativa
- Gestión Económica.

2. Objetivos de la Auditoria.-

Realizar un informe de Auditoria con el objeto de verificar la adecuación de las medidas aplicadas a las amenazas definidas, así como el cumplimiento de los requisitos exigidos.

3. Resultados: Se obtendrá:

- Informe de Auditoria detectando riesgos y deficiencias en la Dirección de Informática.
- Plan de recomendaciones a aplicar en función de:
    - Normativa a cumplir

PREGUNTAS	SI	NO	N/A
1. ¿La dirección de los servicios de información desarrollan regularmente planes a corto, medio y largo plazo que apoyen el logro de la misión y las metas generales de la organización?	✔		
2. ¿Dispone su institución de un plan Estratégico de Tecnología de Información?	✔		

3. ¿Durante el proceso de planificación, se presta adecuada atención al plan estratégico de la empresa?	✔		
4. ¿Las tareas y actividades en el plan tiene la correspondiente y adecuada asignación de recursos?		✔	
5. ¿Existe un comité de informática?			✔
6. ¿Existen estándares de funcionamiento y procedimientos que gobiernen la actividad del área de Informática por un lado y sus relaciones con los departamentos usuarios por otro?		✔	
7. ¿Existen estándares de funcionamiento y procedimientos y descripciones de puestos de trabajo adecuados y actualizados?		✔	
8. ¿Los estándares y procedimientos existentes promueven una filosofía adecuada de control?		✔	
9. ¿Las descripciones de los puestos de trabajo reflejan las actividades realizadas en la práctica?	✔		
10. ¿La selección de personal se basa en criterios objetivos y tiene en cuenta la formación, experiencia y niveles de responsabilidad?	✔		
11. ¿El rendimiento de cada empleado se evalúa regularmente en base a estándares establecidos?	✔		
12. ¿Existen procesos para determinar las necesidades de formación de los empleados en base a su experiencia?	✔		
13. ¿Existen controles que tienden a asegurar que el cambio de puesto de trabajo y la finalización de los contratos laborales no afectan a los controles internos y a la seguridad informática?	✔		
14. ¿Existe un presupuesto económico? ¿y hay un proceso para elaborarlo?	✔		

15. ¿Existen procedimientos para la adquisición de bienes y servicios?	✔		
16. ¿Existe un plan operativo anual?	✔		
17. ¿Existe un sistema de reparto de costes informáticos y que este sea justo?		✔	
18. ¿Cuentan con pólizas de seguros?	✔		
19. ¿Existen procedimientos para vigilar y determinar permanentemente la legislación aplicable?			✔

OBJETIVOS

- Determinación de la utilidad de políticas, planes y procedimientos, así como su nivel de cumplimiento
- Examinar el proceso de planificación de sistemas de información y evaluar si cumplen los objetivos de los mismos.
- Verificar si el comité de Informática existe y cumple su papel adecuadamente.
- Revisar el emplazamiento del departamento de Informática y evaluar su dependencia frente a otros.
- Evaluar la existencia de estándares de funcionamiento, procedimientos y descripciones de puestos de trabajo adecuados y actualizados.
- Evaluar las características de la comunicación entre la Dirección de Informática y el personal del Departamento.
- Verificar la existencia de un sistema de reparto de costes informáticos y que este sea justo.

Auditoria Direccion .-

- **Para hallar el SI**

  17 ⟶ 100%
  12 ⟶ X

  X = 70.58

- **Para hallar el NO**

  17 ⟶ 100%
  5 ⟶ X

  X = 29.41

AUDITORIA DE LA EXPLOTACION

1. Alcance de la Auditoria

- Evaluación del personal y coherencia de cargos de la propia institución.
- Normas y Procedimientos del área de informática

2. Objetivos

Realizar un informe de Auditoria con el objeto de verificar la adecuación de las funciones que sirven de apoyo a las tecnologías de la información.

PREGUNTAS	SI	NO	N/A
1. ¿existe personal con conocimiento y experiencia suficiente que organiza el trabajo para que resulte lo mas eficaz posible ?	✔		
2. ¿existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?			✔
3. ¿se aprueban por personal autorizado las solicitudes de nuevas aplicaciones?	✔		
4. ¿existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?	✔		
5. ¿existen procedimientos adecuados para mantener la documentación al día ?		✔	
6. ¿tienen manuales todas las aplicaciones ?			✔
7. ¿existen controles que garanticen el uso adecuado de discos y cintas?	✔		
8. ¿existen procedimientos adecuados para conectarce y desconectarce de los equipos remotos?	✔		

9. ¿se aprueban los programas nuevos y los que se revisan antes de ponerlos en funcionamiento?	✔		
10. ¿revizan y evaluan los deparatamentop de usuario los resultados de las pruevas finales dando su aprobación antes de poner en funcionamiento las aplicaciones ?	✔		
11. al poner en funcionamiento nuevas aplicaciones o versiones actualizada ¿funcionan en paralelo las existentes durante un cierto tiempo?	✔		
1. ¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento, al personal autorizado?	✔		
2. ¿Se tiene relación del personal autorizado para firmar la salida de archivos confidenciales?		✔	
3. ¿Existe un procedimiento para registrar los archivos que se prestan y la fecha en que se devolverán?	✔		
4. ¿Se lleva control sobre los archivos prestados por la instalación?			✔
5. ¿Se conserva la cinta maestra anterior hasta después de la nueva cinta?	✔		
6. ¿El cintotecario controla la cinta maestra anterior previendo su uso incorrecto o su eliminación prematura?	✔		
7. ¿La operación de reemplazo es controlada por el cintotecario?	✔		
8. ¿Se utiliza la política de conservación de archivos hijo-padre-abuelo?	✔		
9. En los procesos que manejan archivos en línea, ¿Existen procedimientos para recuperar los archivos?	✔		
10. ¿Estos procedimientos los conocen los operadores?		✔	
11. ¿Existe un responsable en caso de falla?	✔		

12. ¿Explique que políticas se siguen para la obtención de archivos de respaldo?	✔		
13. ¿Existe un procedimiento para el manejo de la información de la cintoteca?		✔	
14. ¿Lo conoce y lo sigue el cintotecario?			✔
15. ¿Existe un programa de trabajo de captación de datos?		✔	
16. ¿se controla las entradas de documentos fuente?	✔		
17. ¿Que cifras de control se obtienen? Sistema Cifras que se Observaciones Obtienen		✔	
18. ¿existen documento de entrada se tienen? Sistemas Documentos Dpto. que periodicidad Observaciones proporciona el documento	✔		
19. ¿Se anota que persona recibe la información y su volumen?		✔	
20. ¿Se anota a que capturista se entrega la información, el volumen y la hora?		✔	
21. ¿Se verifica la cantidad de la información recibida para su captura?	✔		
22. ¿Se revisan las cifras de control antes de enviarlas a captura?		✔	
23. ¿Para aquellos procesos que no traigan cifras de control se ha establecido criterios a fin de asegurar que la información es completa y valida?	✔		
24. ¿Existe un procedimiento escrito que indique como tratar la información inválida (sin firma ilegible, no corresponden las cifras de control)?		✔	
25. En caso de resguardo de información de entrada en sistemas, ¿Se custodian en un lugar seguro?	✔		
26. Si se queda en el departamento de sistemas, ¿Por cuanto tiempo se guarda?		✔	

27. ¿Existe un registro de anomalías en la información debido a mala codificación?		✔	
28. ¿Existe una relación completa de distribución de listados, en la cual se indiquen personas, secuencia y sistemas a los que pertenecen?			✔
29. ¿Se verifica que las cifras de las validaciones concuerden con los documentos de entrada?	✔		
¿Se hace una relación de cuando y a quién fueron distribuidos los listados?		✔	
30. ¿Se controlan separadamente los documentos confidenciales?	✔		
31. ¿Se aprovecha adecuadamente el papel de los listados inservibles?		✔	
32. ¿Existe un registro de los documentos que entran a capturar?	✔		
33. ¿Se lleva un control de la producción por persona?	✔		
34. ¿existe parámetros de control?			✔

Auditoria Explotación:

- **Para hallar el SI**

  40 ⟶ 100%
  26 ⟶ X

  X = 65

- **Para hallar el NO**

  40 ⟶ 100%
  14 ⟶ X

  X = 35

INFORME DE AUDITORIA

1. **Identificación del informe**

   Auditoria de la Explotación

2. **Identificación del Cliente**

   El área de Informática

3. **Identificación de la Entidad Auditada**

   Municipalidad Provincial Mariscal Nieto

4. **Objetivos**

   - Verificar el cumplimiento de plazos y calendarios de tratamientos y entrega de datos; la correcta transmisión de datos entre entornos diferentes.
   - Verificar la existencia de normas generales escritas para el personal de explotación en lo que se refiere a sus funciones
   - Verificar la realización de muestreos selectivos de la Documentación de las Aplicaciones explotadas.
   - Verificar cómo se prepara, se lanza y se sigue la producción diaria. Básicamente, la explotación Informática ejecuta procesos por cadenas o lotes sucesivos (Batch*), o en tiempo real (Tiempo Real*).
   - Evaluar las relaciones personales y la coherencia de cargos y salarios, así como la equidad en la asignación de turnos de trabajo.
   - Verificar la existencia de un responsable de Sala en cada turno de trabajo.
   - Revisar la adecuación de los locales en que se almacenan cintas y discos, así como la perfecta y visible identificación de estos medios

5. **Hallazgos Potenciales**

- Incumplimiento de plazos y calendarios de tratamientos y entrega de datos
- Inexistencia y falta de uso de los Manuales de Operación
- Falta de planes de formación
- No existe programas de capacitación y actualización al personal

6. **Alcance de la auditoria**

Nuestra auditoria, comprende el presente periodo 2004 y se ha realizado especialmente al área de Informática de acuerdo a las normas y demás disposiciones aplicable al efecto.

7. Conclusiones:

- Como resultado de la Auditoria de la Seguridad realizada al Municipio, por el período comprendido entre el 01 de Setiembre al 24 de Diciembre del 2004, podemos manifestar que hemos cumplido con evaluar cada uno de los objetivos contenidos en el programa de auditoria.
- El área de Informática presenta deficiencias sobre todo en el debido cumplimiento de sus funciones y por la falta de ellos.

8. Recomendaciones

- Deberán realizarse muestreos selectivos de la Documentación de las Aplicaciones explotadas
- Asignar un responsable del Centro de Cómputos en cada turno de trabajo.
- Crear y hacer uso de manuales de operación.
- Revisar los montajes diarios y por horas de cintas o cartuchos, así como los tiempos transcurridos entre la petición de montaje por parte del Sistema hasta el montaje real.
- Realizar funciones de operación, programación y diseño de sistemas deben estar claramente delimitadas.
- Crear mecanismos necesarios a fin de asegurar que los programadores y analistas no tengan acceso a la operación del computador y los operadores a su vez no conozcan la documentación de programas y sistemas

9. Fecha Del Informe

	PLANEAMIENTO	EJECUCION	INFORME
FECHAS	01–10–04 al 15–10-04	16-10–04 al 20–11-04	23–11–04 al 28–11-04

10. Identificación Y Firma Del Auditor

APELLIDOS Y NOMBRES	CARGO
AROHUANCA ANTAHUANACO MICHELLA	AUDITOR SUPERIOR

AUDITORIA DEL DESARROLLO

1. Alcance de la Auditoria

- Conexiones
- Cifrado
- Salidas gateway y routers
- Correo Electrónico
- Páginas WEB
- Firewalls

2. Objetivos

- revisar el cumplimiento del proceso completo de desarrollo de proyectos
- verificar las metodologías utilizadas
- verificar el control interno de las aplicaciones, satisfacción de los usuarios y control de procesos y ejecuciones de programas críticos.
- Revisar el ciclo de desarrollo del software.

PREGUNTAS	SI	NO	N/A
1. ¿Existe el documento que contiene las funciones que son competencia del área de desarrollo, esta aprobado por la dirección de informática y se respeta?	✔		
2. ¿se comprueban los resultados con datos reales?	✔		
3. ¿Existe un organigrama con la estructura de organización del área?	✔		
4. ¿Existe un manual de organización que regula las relaciones	✔		

entre puestos?			
5. ¿Existe la relación de personal adscrito al área, incluyendo el puesto ocupado por cada persona?	✔		
6. ¿El plan existe, es claro y realista?	✔		
7. ¿Están establecidos los procedimientos de promoción de personal a puestos superiores, teniendo en cuenta la experiencia y formación?	✔		
8. ¿El área de desarrollo lleva su propio control presupuestario?		✔	
9. ¿Se hace un presupuesto por ejercicio y se cumple?	✔		
10. ¿El presupuesto esta en concordancia con los objetivos a cumplir?	✔		
11. ¿El personal de área de desarrollo cuenta con la formación adecuada y son motivados para la realización de su trabajo?		✔	
12. ¿Existen procedimientos de contratación?	✔		
13. ¿Las personas seleccionadas cumplen los requisitos del puesto al que acceden?	✔		
14. ¿Las ofertas de puestos del área se difunden de forma suficiente fuera de la organización y las selecciones se hacen de forma objetiva?		✔	
15. ¿Existe un plan de formación que este en consonancia con los objetivos tecnológicos que se tenga en el área?			✔
16. ¿El plan de trabajo del área tiene en cuenta los tiempos de formación?	✔		
17. ¿Existe un protocolo de recepción / abandono para las personas que se incorporan o dejan el área?			✔
18. ¿Existe un protocolo y se respeta para cada incorporación / abandono?			✔
19. ¿En los abandonos del personal se garantiza la protección del		✔	

área?			
20. ¿Existe una biblioteca y una hemeroteca accesibles por el personal del área?	✔		
21. ¿Esta disponible un numero suficiente de libros, publicaciones periódicas, monografías, de reconocido prestigio y el personal tiene acceso a ellos?	✔		
22. ¿El personal esta motivado en la realización de su trabajo?	✔		
23. ¿Existe algún mecanismo que permita a los empleados hacer sugerencias sobre mejoras en la organización del área?	✔		
24. ¿Existe rotación de personal y existe un buen ambiente de trabajo?	✔		
25. ¿La realización de nuevos proyectos se basa en el plan de sistemas en cuanto a objetivos?	✔		
26. ¿Las fechas de realización coinciden con los del plan de sistemas?	✔		
27. ¿El plan de sistemas se actualiza con la información que se genera a lo largo de un proceso?	✔		
28. ¿Los cambios en los planes de los proyectos se comunican al responsable de mantenimiento del plan de sistemas?	✔		
29. ¿Existe un procedimiento para la propuesta de realización de nuevos proyectos?	✔		
30. ¿Existe un mecanismo para registrar necesidades de desarrollo de nuevos sistemas?		✔	
31. ¿Se respeta este mecanismo en todas las propuestas?		✔	
32. ¿Existe un procedimiento de aprobación de nuevos proyectos?	✔		
33. ¿Existe un procedimiento para asignar director y equipo de desarrollo a cada nuevo proyecto?			✔
34. ¿Se tiene en cuenta a todas las personas disponibles cuyo perfil sea adecuado a los riesgos de cada proyecto y que tenga		✔	

disponibilidad para participar?			
35. ¿Existe un protocolo para solicitar al resto de las áreas la participación del personal en el proyecto y se aplica dicho protocolo?	✔		
36. ¿Existe un procedimiento para conseguir los recursos materiales necesarios para cada proyecto?	✔		
37. ¿Se tiene implantada una metodología de desarrollo de sistemas de información soportada por herramientas de ayuda?	✔		
38. ¿La metodología cubre todas las fases del desarrollo y es adaptable a distintos tipos de proyectos?			✔
39. ¿La metodología y las técnicas asociadas a la misma están adaptadas al entorno tecnológico y a la organización del área de desarrollo?			✔
40. ¿Existe un catalogo de las aplicaciones disponible en el área?		✔	
41. ¿Existe un registro de problemas que se producen en los proyectos del área?		✔	
42. ¿Existe un catalogo de problemas?		✔	
43. ¿El catalogo es accesible para todos los miembros del área?			✔
44. ¿Se registran y controlan todos los proyectos fracasados?	✔		

Auditoria Desarrollo:

- **Para hallar el SI**

37 ⟶ 100%
27 ⟶ X

X = 72.97

- **Para hallar el NO**

37 ⟶ 100%
10 ⟶ X

X = 27.02

INFORME DE AUDITORIA

1. **Identificación del informe**

   Auditoria de Desarrollo

2. **Identificación del Cliente**

   El área de Informática

3. **Identificación de la Entidad Auditada**

   Municipalidad Provincial Mariscal Nieto

4. **Objetivos**

   - Verificar el cumplimiento de los proyectos en proceso.
   - Revisar el cumplimiento de la normas generales
   - Revisar los recursos de la organización
   - Verificar los avances tecnológicos.

5. **Hallazgos Potenciales**

- Incumplimiento de plazos y calendarios de tratamientos y entrega de datos
- Inexistencia y falta de uso de los Manuales de Operación
- Falta de planes de formación
- No existe programas de capacitación y actualización al personal

6. **Alcance de la auditoria**

Nuestra auditoria, comprende el presente periodo 2004 y se ha realizado especialmente al área de Informática de acuerdo a las normas y demás disposiciones aplicable al efecto.

7. Conclusiones:

- La municipalidad no desarrolla software de paliación si no la adquiere.
- .se calificado el ciclo de desarrollo de los procesos de la entidad en su ámbito de trabajo

8. Recomendaciones

- Asignar un responsable un responsable para todos los procesos del Centro de Cómputos.
- Se debe asignar un grupo para el desarrollo de sofware.
- Crear y hacer uso de manuales de operación.
- Realizar funciones de operación, diseño de sistemas.

9. Fecha Del Informe

	PLANEAMIENTO	EJECUCION	INFORME
FECHAS	01–10–04 al 15–10-04	16-10–04 al 20–11-04	23–11–04 al 28–11-04

10. Identificación Y Firma Del Auditor

APELLIDOS Y NOMBRES	CARGO

MUÑOZ ORTEGA, MADELEINE.	AUDITOR SUPERIOR

AUDITORIA DEL MANTENIMIENTO

1. Alcance de la Auditoria.-

- Planes y procedimientos de Mantenimiento
- Normativa

2. Objetivos de la Auditoria.-

Realizar un informe de Auditoria con el objeto de evaluar el mantenimiento correctivo y preventivo del software.

3. Referencia Legal:

• Estándares

– ISO/IEC 12207

– IEEE 1074

– IEEE 1219

– ISO/IEC 14764

PREGUNTAS	SI	NO	N/A
1. Existe un contrato de mantenimiento.		✔	
2. ¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo?	✔		
3. ¿Se lleva a cabo tal programa?	✔		
4. ¿Existen tiempos de respuesta y de compostura estipulados en los contratos?			✔

5. Si los tiempos de reparación son superiores a los estipulados en el contrato, ¿Qué acciones correctivas se toman para ajustarlos a lo convenido?			✔
6. ¿Existe plan de mantenimiento preventivo. ?		✔	
7. ¿Este plan es proporcionado por el proveedor?		✔	
8. ¿Se notifican las fallas?	✔		
9. ¿Se les da seguimiento?		✔	
10. ¿Tiene un plan logístico para dar soporte al producto software?		✔	
11. ¿Los requerimientos de mantenibilidad se incluyen en la Actividad de Iniciación durante el Proceso de Adquisición (ISO 12207) y se evalúa durante el Proceso de Desarrollo?	✔		
12. ¿Las variaciones en el diseño son supervisadas durante el desarrollo para establecer su impacto sobre la mantenibilidad?	✔		
13. ¿Se realizan varios tipos de medidas para poder estimar la calidad del software?	✔		
14. ¿La mantenibilidad se tiene en cuenta antes de empezar a desarrollar?	✔		
15. ¿El desarrollador prepara un Plan de Mantenibilidad que establece prácticas específicas de mantenibilidad, así como recursos y secuencias relevantes de actividades?	✔		
16. ¿Durante el análisis de requerimientos, los siguientes aspectos que afectan a la mantenibilidad, son tomados en cuenta? ➢ Identificación y definición de funciones, especialmente las opcionales. ➢ Exactitud y organización lógica de los datos. ➢ Los Interfaces (de máquina y de usuario). ➢ Requerimientos de rendimiento.	✔		

➢ Requerimientos impuestos por el entorno (presupuesto). ➢ Granularidad (detalle) de los requerimientos y su impacto sobre la trazabilidad. ➢ Énfasis del Plan de Aseguramiento de Calidad del Software (SQAP) en el cumplimiento de las normas de documentación			
17. ¿La transición del software consiste en una secuencia controlada y coordinada de acciones para trasladar un producto software desde la organización que inicialmente ha realizado el desarrollo a la encargada del mantenimiento?		✔	
18. ¿La responsabilidad del mantenimiento se transfiere a una organización distinta, se elabora un Plan de Transición? ¿que es lo que incluye este plan? ➢ La transferencia de hardware, software, datos y experiencia desde el desarrollador al mantenedor. ➢ Las tareas necesarias para que el mantenedor pueda implementar una estrategia de mantenimiento del software.	✔		
19. ¿El mantenedor a menudo se encuentra con un producto software con documentación?		✔	
20. ¿Si no hay documentación, el mantenedor deberá crearla? ¿Realiza lo siguiente? a. Comprender el dominio del problema y operar con el producto software. b. Aprender la estructura y organización del producto software. c. Determinar qué hace el producto software. Revisar las especificaciones (si las hubiera)	✔		
21. ¿Documentos como especificaciones, manuales de mantenimiento para programadores, manuales de usuario o guías de instalación pueden ser modificados o creados,	✔		

si fuese necesario?			
22. El Plan de Mantenimiento es preparado por el mantenedor durante el desarrollo del software.	✔		
23. ¿Los elementos software reflejan la documentación de diseño?	✔		
24. ¿Los productos software fueron suficientemente probados y sus especificaciones cumplidas?	✔		
25. ¿Los informes de pruebas son correctos y las discrepancias entre resultados actuales y esperados han sido resueltas?	✔		
26. ¿La documentación de usuario cumple los estándares especificados?	✔		
27. ¿Los costes y calendarios se ajustan a los planes establecidos?	✔		

Auditoria Mantenimiento:

- **Para hallar el SI**

  25 ⟶ 100%
  18 ⟶ X

  X = 72

- **Para hallar el NO**

  25 ⟶ 100%
  7 ⟶ X

  X = 28

INFORME DE AUDITORIA

1. **Identificación del informe**

   Auditoria del Mantenimiento

2. **Identificación del Cliente**

   El área de Informática

3. **Identificación de la Entidad Auditada**

   Municipalidad Provincial Mariscal Nieto

4. **Objetivos**

   - Revisar los contratos y las cláusulas que estén perfectamente definidas en las cuales se elimine toda la subjetividad y con penalización en caso de incumplimiento, para evitar contratos que sean parciales.
   - Verificar el cumplimiento del contrato sobre el control de fallas, frecuencia, y el tiempo de reparación.
   - Diagnóstico del sistema actual de mantenimiento.
   - Verificar el montaje de métodos de recopilación de información en áreas específicas.
   - Verificar la existencia de de planes estratégicos de desarrollo.
   - Verificación de la efectividad del mantenimiento actual y los desarrollos y programas proyectados.
   - Verificar la optimización de almacenes y repuestos.

5. **Hallazgos Potenciales**

   - Pérdida de control
   - Pérdida de una fuente de aprendizaje, porque una actividad interna pasa a ser externa.
   - Dependencias del suministrador.

- Variaciones en la calidad del producto entregado al usuario final.
- Problemas entre el personal.
- Uso de metodologías para nuevos desarrollos, pero ausencia de ellas para el mantenimiento.
- Tendencia a la desestructuración
- Dificultad progresiva de modificación
- Falta de presupuesto
- Falta de personal
- Falta de apoyo de la Dirección

6. Alcance de la auditoria

Nuestra auditoria, comprende el presente periodo 2004 y se ha realizado especialmente al área de Informática de acuerdo a las normas y demás disposiciones aplicable al efecto.

7. Conclusiones:

- Como resultado de la Auditoria del Mantenimiento realizada al Municipio, por el período comprendido entre el 01 de Setiembre al 24 de Diciembre del 2004, podemos manifestar que hemos cumplido con evaluar cada uno de los objetivos contenidos en el programa de auditoria.
- El área de Informática presenta deficiencias sobre todo en el debido cumplimiento de sus funciones y por la falta de ellos.

8. Recomendaciones

- Modificación de un producto software, o de ciertos componentes, usando para el análisis del sistema existente técnicas de Ingeniería Inversa y, para la etapa

- de reconstrucción, herramientas de Ingeniería Directa, de tal manera que se oriente este cambio hacia mayores niveles de facilidad en cuanto a mantenimiento, reutilización, comprensión o evolución.

- Categorizar los tipos de mantenimiento del software y para cada tipo planificar las actividades y tareas a realizar.
- Elaborar un procedimiento organizado para realizar la migración de un producto software desde un entorno operativo antiguo a otro nuevo.
- Establecer un acuerdo o contrato de mantenimiento entre el mantenedor y el cliente y las obligaciones de cada uno estos.
- Elaborar un plan de mantenimiento que incluya el alcance del mantenimiento, quién lo realizará, una estimación de los costes y un análisis de los recursos necesarios.

9. Fecha Del Informe

	PLANEAMIENTO	EJECUCION	INFORME
FECHAS	01–10–04 al 15–10-04	16-10–04 al 20–11-04	23–11–04 al 28–12-04

10. Identificación Y Firma Del Auditor

APELLIDOS Y NOMBRES	CARGO
QUIÑONEZ MAYTA, CARMEN	AUDITOR SUPERIOR

AUDITORIA DE BASE DE DATOS

1. Alcance de la auditoria:

Esta auditoria comprende solamente al área de cetro de computo de la municipalidad de mariscal nieto, con respecto al cumplimiento del proceso "De Gestión administración de la Base de Datos " de la de manera que abarca la explotación, mantenimiento, diseño carga, post implementación, Los sistemas de gestión de base de datos (SGBD), software de auditoria , sistema operativo protocolos y sistemas distribuidos.

2. Objetivos

- ”Verificar la responsabilidad para la planificación de planillas y control de los activos de datos de la organización” (administrador de datos)
- “Verificar la responsabilidad de la administración del entorno de la base de datos” (administrador de la base de datos)
- Proporcionar servicios de apoyo en aspectos de organización y métodos,

mediante la definición, implantación y actualización de Base de Datos y/o procedimientos administrativos con la finalidad de contribuir a la eficiencia

PREGUNTAS	SI	NO	N/A
1. Existe equipos o software de SGBD	✔		
2. La organización tiene un sistema de gestión de base de datos (SGBD)	✔		
3. Los datos son cargados correctamente en la interfaz grafica	✔		
4. Se verificará que los controles y relaciones de datos se realizan de acuerdo a Normalización libre de error	✔		
5. Existe personal restringido que tenga acceso a la BD	✔		
6. El SGBD es dependiente de los servicios que ofrece el Sistema Operativo		✔	

7. La interfaz que existe entre el SGBD y el SO es el adecuado	✔		
8. ¿Existen procedimientos formales para la operación del SGBD?	✔		
9. ¿Están actualizados los procedimientos de SGBD?	✔		
10. ¿La periodicidad de la actualización de los procedimientos es Anual ?	✔		
11. ¿Son suficientemente claras las operaciones que realiza la BD?	✔		
12. ¿Existe un control que asegure la justificación de los procesos en el computador? (Que los procesos que están autorizados tengan una razón de ser procesados)	✔		
13. ¿Se procesa las operaciones dentro del departamento de cómputo?	✔		
14. ¿Se verifican con frecuencia la validez de los inventarios de los archivos magnéticos?	✔		
15. ¿Existe un control estricto de las copias de estos archivos?	✔		
16. ¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos?	✔		
17. ¿Se registran como parte del inventario las nuevas cintas magnéticas que recibe el centro de computo?	✔		
18. ¿Se tiene un responsable del SGBD?	✔		
19. ¿Se realizan auditorias periódicas a los medios de almacenamiento?		✔	
20. ¿Se tiene relación del personal autorizado para manipular la BD?		✔	
21. ¿Se lleva control sobre los archivos trasmitidos por el sistema?		✔	
22. ¿Existe un programa de mantenimiento preventivo para el dispositivo del SGBD?			✔
23. ¿Existen integridad de los componentes y de seguridad de datos?	✔		

24. De acuerdo con los tiempos de utilización de cada dispositivo del sistema de cómputo, ¿existe equipo capaces que soportar el trabajo?	✔		
25. ¿El SGBD tiene capacidad de teleproceso?		✔	
26. ¿Se ha investigado si ese tiempo de respuesta satisface a los usuarios?			✔
27. ¿La capacidad de almacenamiento máximo de la BD es suficiente para atender el proceso por lotes y el proceso remoto?			✔

Auditoria Explotación:

- **Para hallar el SI**

  24 ⟶ 100%
  19 ⟶ X

  X = 79.16

- **Para hallar el NO**

  24 ⟶ 100%
  5 ⟶ X
  X = 20.83

INFORME DE AUDITORIA

1. **Identificación del informe**

   Auditoria de Base de Datos.

2. **Identificación del Cliente**

   El área de Informática

3. **Identificación de la Entidad Auditada**

   Municipalidad Provincial de Moquegua.

4. **Objetivos**

   - Evaluar el tipo de Base de Datos, relaciones, plataforma o sistema operativo que trabaja, llaves, administración y demás aspectos que repercuten en su trabajo.
   - Revisar del software institucional para la administración de la Base de Datos.
   - Verificar la actualización de la Base de Datos.
   - Verificar la optimización de almacenes de los Base de Datos
   - Revisar que el equipo utilizado tiene suficiente poder de procesamiento y velocidad en red para optimizar el desempeño de la base de datos.

5. **Hallazgos Potenciales**

   - No están definidos los parámetros o normas de calidad.
   - Falta de presupuesto
   - Falta de personal

- La gerencia de Base de datos no tiene un plan que permite modificar en forma oportuna el plan a largo plazo de tecnología, teniendo en cuenta los posibles cambios tecnológicos y el incremento de la base de datos..
- No existe un calendario de mantenimiento de rutina periódico del software definido por la Base de datos.

6. Alcance de la auditoria

Nuestra auditoria, comprende el presente periodo 2004 y se ha realizado especialmente al Departamento de centro de cómputo de acuerdo a las normas y demás disposiciones aplicable al efecto.

7. Conclusiones:

- Como resultado de la Auditoria podemos manifestar que hemos cumplido con evaluar cada uno de los objetivos contenidos en el programa de auditoria.
- El Departamento de centro de cómputo presenta deficiencias sobre todo en el debido cumplimiento de Normas de seguridad de datos y administración de la Base de Datos.

8. Recomendaciones

- Elaborar toda la documentación lógica correspondiente a los sistemas de administración de la BD. Evaluar e implementar un software que permita mantener el resguardo de acceso de los archivos de programas y aún de los programadores.
- Implementar la relaciones con las diferentes áreas en cuanto al compartimiento de archivos permitidos por las normas
- Elaborar un calendario de mantenimiento de rutina periódico .
- Capacitar al personal al manejo de la BD.
- Dar a conocer la importancia del SGBD al usuario

9. Fecha Del Informe

	PLANEAMIENTO	EJECUCION	INFORME
FECHAS	01–10–04 al 15–10-04	16-10–04 al 20–11-04	23–11–04 al 28–11-04

10. Identificación Y Firma Del Auditor

APELLIDOS Y NOMBRES	CARGO
MAMANI CUTIPA WILY	AUDITOR SUPERIOR

AUDITORIA DE CALIDAD

Objetivos:

- Verificar los procesos aplicables del programa de la calidad han sido desarrollados y documentados.
- Evaluar la capacidad de realizar un trabajo especifico.

	SI	NO	N/A
¿Se reflejan el software codificado tal como en el diseño en la documentación?		X	
¿Fueron probados con éxito los productos de software usados en el centro de computo?	X		
¿Se cumplen las especificaciones de la documentación del usuario del software?	X		
¿Los procesos de gestión administrativa aplicados en el área de informática de la institución son lo suficientemente óptimos?		X	
¿El funcionamiento del software dentro del área de trabajo están de acuerdo con los requerimientos específicos?	X		
¿Los documentos de gestión administrativa se cumplen satisfactoriamente en el área de computo?		X	
¿Los productos de software que utilizan en el área de informática esta de acuerdo con los estándares establecidos?	X		
¿Los dispositivos de trabajo en el área de informática se les	X		

realizan una revisión técnica correcta?			
¿Los costos fijados en la revisión técnica se encuentran dentro de los límites fijados?		**X**	

Auditoria Calidad:

- **Para hallar el SI**

  9 ⟶ 100%
  5 ⟶ X

  X = 55.5

- **Para hallar el NO**

  9 ⟶ 100%
  4 ⟶ X
  X = **44.4**

INFORME DE AUDITORIA

11. Identificación del informe

Auditoria de Calidad

12. Identificación del Cliente

El área de Informática

13. Identificación de la Entidad Auditada

Municipalidad Provincial de Moquegua.

14. Objetivos

- Verificar la calidad de servicio que ofrece el Software.
- Evaluar el software institucional para la administración.
- Revisar que el equipo utilizado tiene suficiente poder de procesamiento y velocidad en red para optimizar el desempeño de la organización.

15. Alcance de la auditoria

Nuestra auditoria, comprende el presente periodo 2004 y se ha realizado especialmente al Departamento de centro de cómputo de acuerdo a las normas y demás disposiciones aplicable al efecto.

16. Conclusiones:

- El Departamento de centro de cómputo presenta deficiencias sobre todo en el debido cumplimiento de Normas de seguridad de datos y administración de la Base de Datos con respecto a calidad.

17. Fecha Del Informe

	PLANEAMIENTO	EJECUCION	INFORME
FECHAS	01–10–04 al 15–10-04	16-10–04 al 20–11-04	23–11–04 al 28–11-04

18. Identificación Y Firma Del Auditor

APELLIDOS Y NOMBRES	CARGO
MAMANI CUTIPA WILY	AUDITOR SUPERIOR

AUDITORIA DE LA SEGURIDAD

1. **Alcance de la Auditoria.-**

   - Organización y calificación del personal
   - Planes y procedimientos
   - Sistemas técnicos de detección y comunicación
   - Análisis de puestos
   - Mantenimiento
   - Normativa

2. **Objetivos de la Auditoria.-**

   Realizar un informe de Auditoria con el objeto de verificar la adecuación de las medidas aplicadas a las amenazas definidas, así como el cumplimiento de los requisitos exigidos.

3. **Referencia Legal**:

   - Manual de Autoprotección aprobado por O.M. de 29/11/84, NBE-CPI 96 (RD 2177/96),
   - Normativa de las Comunidades Autónomas y Ordenanzas Municipales, CEPREVEN.

4. **Resultados**: Se obtendrá:

   - Informe de Auditoria detectando riesgos y deficiencias en el Sistema de Seguridad.
   - Plan de recomendaciones a aplicar en función de:
     - Riesgos
     - Normativa a cumplir
     - Costes estimados de las recomendaciones

AUDITORIA LOGICA

PREGUNTAS	SI	NO	N/A
1. ¿Existen medidas, controles, procedimientos, normas y estándares de seguridad?		✔	
2. ¿Existe un documento donde este especificado la relación de las funciones y obligaciones del personal?		✔	
3. ¿Existen procedimientos de notificación y gestión de incidencias?			✔
4. ¿Existen procedimientos de realización de copias de seguridad y de recuperación de datos?	✔		
5. ¿Existe una relación del personal autorizado a conceder, alterar o anular el acceso sobre datos y recursos?	✔		
6. ¿Existe una relación de controles periódicos a realizar para verificar el cumplimiento del documento?		✔	
7. ¿Existen medidas a adoptar cuando un soporte vaya a ser desechado o reutilizado?		✔	
8. ¿Existe una relación del personal autorizado a acceder a los locales donde se encuentren ubicados los sistemas que tratan datos personales?		✔	
9. ¿Existe una relación de personal autorizado a acceder a los soportes de datos?		✔	
10. ¿Existe un período máximo de vida de las contraseñas?	✔		
11. ¿Existe una relación de usuarios autorizados a acceder a los sistemas y que incluye los tipos de acceso permitidos?		✔	
12. ¿Los derechos de acceso concedidos a los usuarios son los necesarios y suficientes para el ejercicio de las funciones que tienen encomendadas, las cuales a su vez se encuentran o deben estar- documentadas en el Documento de Seguridad?		✔	
13. ¿Hay dadas de alta en el sistema cuentas de usuario genéricas, es decir, utilizadas por más de una persona, no permitiendo por		✔	

tanto la identificación de la persona física que las ha utilizado?			
14. ¿En la práctica las personas que tienen atribuciones y privilegios dentro del sistema para conceder derechos de acceso son las autorizadas e incluidas en el Documento de Seguridad?			✔
15. ¿El sistema de autenticación de usuarios guarda las contraseñas encriptadas?	✔		
16. ¿En el sistema están habilitadas para todas las cuentas de usuario las opciones que permiten establecer: • Un número máximo de intentos de conexión. • Un período máximo de vigencia para la contraseña, coincidente con el establecido en el Documento de Seguridad.	✔		
17. ¿Existen procedimientos de asignación y distribución de contraseñas?	✔		

AUDITORIA FISICA

PREGUNTAS	SI	NO	N/A
1. ¿Existen procedimientos para la realización de las copias de seguridad?	✔		
2. ¿Existen procedimientos que aseguran que, de todos los ficheros con datos de carácter personal, se realiza copia al menos una vez cada semana?		✔	
3. ¿Hay procedimientos que aseguran la realización de copias de todos aquellos ficheros que han experimentado algún cambio en su contenido?		✔	
4. ¿Existen controles para la detección de incidencias en la realización de las pruebas?		✔	
5. ¿Existen controles sobre el acceso físico a las copias de seguridad?	✔		
6. ¿Sólo las personas con acceso autorizado en el documento de			

seguridad tienen acceso a los soportes que contienen las copias de seguridad?		✔	
7. ¿Las copias de seguridad de ficheros de nivel alto incluyen los ficheros cifrados, si estas copias se transportan fuera de las instalaciones?			✔
8. ¿Las copias de seguridad de los ficheros de nivel alto se almacenan en lugar diferente al de los equipos que las procesan?	✔		g
9. ¿Existe un inventario de los soportes existentes?	✔		
10. ¿Dicho inventario incluye las copias de seguridad?		✔	
11. ¿Las copias de seguridad, o cualquier otro soporte, se almacenan fuera de la instalación?			✔
12. ¿Existen procedimientos de actualización de dicho inventario?		✔	
13. ¿Existen procedimientos de etiquetado e identificación del contenido de los soportes?	✔		
14. ¿Existen procedimientos en relación con la salida de soportes fuera de su almacenamiento habitual?		✔	
15. ¿Se evalúan los estándares de distribución y envío de estos soportes?	✔		
16. ¿Se Obtiene una relación de los ficheros que se envían fuera de la empresa, en la que se especifique el tipo de soporte, la forma de envío, el estamento que realiza el envío y el destinatario?		✔	
17. ¿Se Comprueba que todos los soportes incluidos en esa relación se encuentran también en el inventario de soportes mencionado anteriormente?			✔
18. ¿Se Obtiene una copia del Registro de Entrada y Salida de Soportes y se comprueba que en él se incluyen: • Los soportes incluidos en la relación del punto anterior (y viceversa) • Los desplazamientos de soportes al almacenamiento			✔

exterior (si existiera)			
19. ¿Se Verifica que el Registro de Entrada y Salida refleja la información requerida por el Reglamento: a) Fecha y hora b) Emisor/Receptor c) Nº de soportes d) Tipo de información contenida en el soporte. e) Forma de envío f) Persona física responsable de la recepción/entrega	✔		
20. ¿Se Analiza los procedimientos de actualización del Registro de Entrada y Salida en relación con el movimiento de soportes?	✔		
21. ¿Existen controles para detectar la existencia de soportes recibidos/enviados que no se inscriben en el Registro de Entrada/Salida?		✔	
22. ¿Se Comprueba, en el caso de que el Inventario de Soportes y/o el Registro de Entrada/Salida estén informatizados, que se realizan copias de seguridad de ellos, al menos, una vez a la semana?	✔		
23. ¿Se realiza una relación de soportes enviados fuera de la empresa con la relación de ficheros de nivel alto?			✔
24. ¿Se Verifica que todos los soportes que contiene ficheros con datos de nivel Alto van cifrados?			✔
25. ¿Se Comprobar la existencia, como parte del Documento de Seguridad, de una relación de usuarios con acceso autorizado a la sala?		✔	
26. ¿Se Verifica que la inclusión del personal en la relación anterior es coherente con las funciones que tienen encomendadas?		✔	
27. ¿Se Comprueba que la relación es “lógica” (¿personal de limpieza? ¿Vigilantes de seguridad?).			✔
28. ¿Existen políticas de la instalación en relación con los accesos ocasionales a la sala’			✔
29. ¿Se Determina que personas tienen llaves de acceso, tarjetas, etc. de acceso a la sala?g.		✔	

30. ¿Se Comprueba que están activados los parámetros de activación del Registro para todos los ficheros de Nivel Alto?			✔
31. ¿Se Analizan los procedimientos de descarga a cinta de este Registro de Accesos y el período de retención de este soporte?			✔
32. ¿Existen procedimientos de realización de copias de seguridad del Registro de Accesos y el período de retención de las copias?		✔	
33. ¿Se Verifica la asignación de privilegios que permitan activar/desactivar el Registro de Accesos para uno o más ficheros?		✔	
34. ¿Se Comprueba que el Registro de Accesos se encuentra bajo el control directo del Responsable de Seguridad pertinente?		✔	

Auditoria Calidad:

- **Para hallar el SI**

  39 ⟶ 100%
  15 ⟶ X

  X = 38.46

- **Para hallar el NO**

  39 ⟶ 100%
  24 ⟶ X
  X = **61.53**

AREAS CRÍTICAS DE LA AUDITORIA DE SEGURIDAD

Evaluación de la seguridad en el acceso al Sistema

Preguntas	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Evaluar los atributos de acceso al sistema.					✔
Evaluar los niveles de acceso al sistema.			✔		
Evaluar la administración de contraseñas al sistema				✔	
Evaluar el monitoreo en el acceso al sistema.					✔
Evaluar las funciones del administrador del acceso al sistema.				✔	
Evaluar las medidas preventivas o correctivas en caso de siniestros n el acceso.			✔		

Evaluación de la seguridad en el acceso al Área Física

Preguntas	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Evaluar el acceso del personal al centro de cómputo.		✔			
Evaluar el acceso de los usuarios y terceros al centro de cómputo.				✔	
Evaluar el control de entradas y				✔	

salidas de bienes informáticos del centro de cómputo.					
Evaluar la vigilancia del centro de cómputo.					✔
Evaluar las medidas preventivas o correctivas en caso de siniestro en el centro de cómputo.				✔	
Analizar las políticas de la instalación en relación con los accesos ocasionales a la sala.			✔		

Evaluación de los planes de contingencias informáticos

Preguntas	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Evaluar la existencia, difusión, aplicación y uso de contra contingencias de sistemas.				✔	
Evaluar la aplicación de simulacros, así como el plan contra contingencias.					✔
Evaluar la confidencialidad, veracidad y oportunidad en la aplicación de las medidas del plan contra contingencias.			✔		

Evaluación de la seguridad en los sistemas computacionales

Preguntas	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Evaluar el rendimiento y uso del sistema computacional y de sus periféricos asociados.			✔		
Evaluar la existencia, protección y periodicidad de los respaldos de				✔	

bases de datos, software e información importante de la organización.					
Evaluar la configuración, instalaciones y seguridad del equipo de cómputo, mobiliario y demás equipos.				✔	
Evaluar el rendimiento, aplicación y utilidad del equipo de cómputo, mobiliario y demás equipos.			✔		
Evaluar la seguridad en el procesamiento de información.				✔	
Evaluar los procedimientos de captura, procesamiento de datos y emisión de resultados de los sistemas computacionales.					✔

Evaluación de la protección contra la piratería y robo de información

Preguntas	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Medidas preventivas.		✔			
Protección de archivos.			✔		
Limitación de accesos.					✔
Protección contra robos				✔	
Protección ante copias ilegales		✔			

Evaluación de la protección contra virus informáticos

Preguntas	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Medidas preventivas y correctivas.			✔		
Uso de vacunas y buscadores de virus.				✔	
Protección de archivos, programas e información.				✔	

Evaluación de la seguridad del hardware

Preguntas	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Realización de inventarios de hardware, equipos y periféricos asociados.			✔		
Evaluar la configuración del equipo de computo (hardware).				✔	
Evaluar el rendimiento y uso del sistema computacional y sus periféricos asociados.					✔
Evaluar el estado físico del hardware, periféricos y equipos asociados			✔		

Evaluación de la seguridad del Software

Preguntas	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Realización de inventarios de software, paqueterías y desarrollos empresariales.				✔	
			✔		

Evaluar las licencias permisos y usos de los sistemas computacionales.					
Evaluar el rendimiento y uso del software de los sistemas computacionales.					✔
Verificar que la instalación del software, paqueterías y sistemas desarrollados en la empresa sea la adecuada para cubrir las necesidades de esta ultima.				✔	

INFORME DE AUDITORIA

1. Identificación del informe

Auditoria de la Seguridad

2. Identificación del Cliente

El área de Informática

3. Identificación de la Entidad Auditada

Municipalidad Provincial

4. Objetivos

Hacer un estudio cuidadoso de los riesgos potenciales a los que está sometida el área de informática.

Revisar tanto la seguridad física del Centro de Proceso de Datos en su sentido más amplio, como la seguridad lógica de datos, procesos y funciones informáticas más Importantes de aquél.

5. Hallazgos Potenciales

- No existe documentaciones técnicas del sistema integrado de la Cooperativa y tampoco no existe un control o registro formal de las modificaciones efectuadas.
- No se cuenta con un Software que permita la seguridad de las librerías de los programas y la restricción y/o control del acceso de los mismos.
- Las modificaciones a los programas son solicitadas generalmente sin notas internas, en donde se describen los cambios o modificaciones que se requieren.
- Falta de planes y Programas Informáticos.
- Poca identificación del personal con la institución
- Inestabilidad laboral del personal
- No existe programas de capacitación y actualización al personal

6. Alcance de la auditoria

Nuestra auditoria, comprende el presente periodo 2004 y se ha realizado especialmente al área de Informática de acuerdo a las normas y demás disposiciones aplicable al efecto.

7. Conclusiones:

- Como resultado de la Auditoria de la Seguridad realizada al Municipio, por el período comprendido entre el 01 de Setiembre al 24 de Diciembre del 2004, podemos manifestar que hemos cumplido con evaluar cada uno de los objetivos contenidos en el programa de auditoria.
- El área de Informática presenta deficiencias sobre todo en el debido cumplimiento de sus funciones y por la falta de ellos.

8. Recomendaciones

- Elaborar toda la documentación técnica correspondiente a los sistemas implementados y establecer normas y procedimientos para los desarrollos y su actualización.
- Evaluar e implementar un software que permita mantener el resguardo de acceso de los archivos de programas y aún de los programadores.
- Implementar y conservar todas las documentaciones de prueba de los sistemas, como así también las modificaciones y aprobaciones de programas realizadas por los usuarios
- El coste de la seguridad debe considerarse como un coste más entre todos los que son necesarios para desempeñar la actividad que es el objeto de la existencia de la entidad, sea ésta la obtención de un beneficio o la prestación de un servicio público.
- El coste de la seguridad, como el coste de la calidad, son los costes de funciones imprescindibles para desarrollar la actividad adecuadamente. Y por "adecuadamente" debe entenderse no sólo un nivel de calidad y precio que haga competitivo el servicio o producto suministrado, sino también un grado de garantía de que dichos productos o servicios van a seguir llegando a los usuarios en cualquier circunstancia.

9. Fecha Del Informe

	PLANEAMIENTO	EJECUCION	INFORME
FECHAS	01–10–04 al 15–10-04	16-10–04 al 20–11-04	23–11–04 al 28–12-04

10. Identificación Y Firma Del Auditor

APELLIDOS Y NOMBRES	CARGO
QUIÑONEZ MAYTA, CARMEN	AUDITOR SUPERIOR

AUDITORIA A LOS SISTEMAS DE REDES

1. Alcance de la Auditoria.-

- Calificación del personal
- Sistemas técnicos de la red
- Mantenimiento de la Red

2. Objetivos de la Auditoria.-

Realizar un informe de Auditoria con el objeto de verificar la adecuación de las medidas aplicadas a las amenazas definidas, así como el cumplimiento de los requisitos exigidos.

3. Referencia Legal.-

•Manual de Autoprotección aprobado por O.M. de 29/11/84, NBE-CPI 96 (RD 2177/96),

•Normativa de las Comunidades Autónomas y Ordenanzas Municipales, CEPREVEN.

4. Resultados.-

Se obtendrá:

- Informe de Auditoria detectando deficiencias en el Sistema de Redes.
- Plan de recomendaciones a aplicar en función de:
  - Normativa a cumplir
  - Recomendaciones

PREGUNTAS	SI	NO	N/A
1. La gerencia de redes tiene una política definida de planeamiento de tecnología de red?	✔		
2. Esta política es acorde con el plan de calidad de la organización		✔	
3. La gerencia de redes tiene un plan que permite modificar en forma oportuna el plan a largo plazo de tecnología de redes , teniendo en cuenta los posibles cambios tecnológicos o en la organización?		✔	
4. Existe un inventario de equipos y software asociados a las	✔		

5. redes de datos?			
6. Existe un plan de infraestructura de redes?	✔		
7. El plan de compras de hardware y software para el sector redes está de acuerdo con el plan de infraestructura de redes?		✔	
8. La responsabilidad operativa de las redes esta separada de las de operaciones del computador?		✔	
9. Están establecidos controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados		✔	
10. Existen controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas?		✔	
11. Existen controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.?		✔	
12. Existen protocolos de comunicaron establecida	✔		
13. Existe una topología estandarizada en toda la organización		✔	
14. Existen normas que detallan que estándares que deben cumplir el hardware y el software de tecnología de redes?	✔		
15. ¿La transmisión de la información en las redes es segura?	✔		
16. ¿El acceso a la red tiene password?			

Auditoria de Redes:

- **Para hallar el SI**

  14 ⟶ 100%

  6 ⟶ X

  X = 42.85

- **Para hallar el NO**

14 ⟶ 100%
8 ⟶ X
X = 57.14

AREA CRITICA REDES

LISTADO DE VERIFICACIÓN DE AUDITORIA DE REDES

Gestión administrativa de la red.

	100% Excelente	80% Buena	60% Regular	40% Mínimo	20% No cumple
Los objetivos de la red De computo				✔	
Las características de la Red de computo			✔		
Los componentes físicos de la red de computo			✔		
La conectividad y las comunicaciones de la red de computo				✔	
Los servicios que proporcionan La red de computo				✔	
Las configuraciones , topologías , tipos Y cobertura de las redes de computo.			✔		
Los protocolos de comunicación interna de la red.				✔	
La administración de la red de Computo.			✔		

La seguridad de las redes de computo .				✔	

Evaluación de análisis de la red de computo

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
Evaluación de la existencia y uso de metodologías , normas ,estándares y políticas para el análisis y diseño de redes de computo .				✔	
Análisis de la definición de la problemática y solución para instalar redes de computo en la empresa .			✔		
Análisis de cumplimiento de los objetivos fundamentales de la organización para instalar una red de computo , evaluando en cada caso .			✔		
La forma de repartir los recursos informáticos de la organización , especialmente la información y los activos.			✔		
La cobertura de servicios informáticos para la captura , el procesamiento y la emisión de información en la organización .				✔	
La cobertura de los servicios de comunicación .				✔	
La frecuencia con que los usuarios recurren a los recursos de la red			✔		
La confiabilidad y seguridades el uso de la información institucional		✔			
La centralización , administración , operación asignación y el control de los recursos informáticos de la organización			✔		
La distribución equitativa de los costos de adquisición y el control de los recursos informáticos de la organización .			✔		
La escalabilidad y migración de los recursos computacionales de la organización .				✔	
La satisfacción de las necesidades de poder computacional de la organización ,sea con redes ,cliente				✔	

/servidor o mainframe					
La solución a los problemas de comunicación de información y datos en las áreas de la organización.			✔		

Análisis de los estudios de viabilidad y factibilidad en el diseño e instalación de la red de cómputo en la empresa:

Evaluar y calificar el cumplimiento de los siguientes aspectos	Excelente	Bueno	Regular	Mínimo	No cumple
El estudio de factibilidad tecnológica		✔			
El estudio factibilidad económica		✔			
El estudio de factibilidad administrativa			✔		
El estudio de factibilidad operativa			✔		

Evaluación del diseño e implementación de la red según el ámbito de cobertura

	Excelente	Bueno	Regular	Mínimo	No cumple
Análisis de las redes de multicomputadoras			✔		
Evaluar el funcionamiento de la cobertura de punto a punto		✔			
Evaluar el funcionamiento de la tecnología que se usa con un solo cable entre las máquinas conectadas		✔			
Evaluar el funcionamiento de las aplicaciones, usos y explotación de las redes			✔		

Análisis de la red de área local (L A N)

	Excelente	Bueno	Regular	Mínimo	No cumple
Evaluar el uso adecuado y confiable de la tecnología			✔		

utilizada internamente para la transmisión de datos.					
Evaluar la restricción adoptada para establecer el tamaño de la red			✔		
Evaluar la velocidad.		✔			

INFORME DE AUDITORIA

1. **Identificación del informe**

   Auditoria del Sistema de Redes

2. **Identificación del Cliente**

   El área de Informática

3. **Identificación de la Entidad Auditada**

   Municipalidad Provincial de Moquegua.

4. **Objetivos**

   Evaluar el tipo de red, arquitectura topología, protocolos de comunicación, las conexiones, accesos privilegios, administración y demás aspectos que repercuten en su instalación.

   Revisión del software institucional para la administración de la red.

5. **Hallazgos Potenciales**

- No se cuenta con un Software que permita la seguridad de restricción y/o control a la Red.

No existe un plan que asegure acciones correctivas asociadas a la conexión con redes externas.

- No están definidos los parámetros o normas de calidad.
- La gerencia de redes no tiene un plan que permite modificar en forma oportuna el plan a largo plazo de tecnología de redes , teniendo en cuenta los posibles cambios tecnológicos.
- No existe un calendario de mantenimiento de rutina periódico del hardware definido por la gerencia de redes.
- No existe un plan proactivo de tareas a fin de anticipar los problemas y solucionarlos antes de que los mismos afecten el desempeño de la red

6. Alcance de la auditoria

Nuestra auditoria, comprende el presente periodo 2004 y se ha realizado especialmente al área de Informática de acuerdo a las normas y demás disposiciones aplicable al efecto.

7. Conclusiones:

- Como resultado de la Auditoria podemos manifestar que hemos cumplido con evaluar cada uno de los objetivos contenidos en el programa de auditoria.
- El área de Informática presenta deficiencias sobre todo en el debido cumplimiento de Normas de redes y funciones.

8. Recomendaciones

- Elaborar toda la documentación técnica correspondiente a los sistemas de redes. Evaluar e implementar un software que permita mantener el resguardo de acceso de los archivos de programas y aún de los programadores.
- Implementar un plan que permita modificar en forma oportuna el plan a largo plazo de tecnología de redes.
- Elaborar un calendario de mantenimiento de rutina periódico del hardware.

9. Fecha Del Informe

	PLANEAMIENTO	EJECUCION	INFORME
FECHAS	01–10–04 al 15–10-04	16-10–04 al 20–11-04	23–11–04 al 28–11-04

10. Identificación Y Firma Del Auditor

APELLIDOS Y NOMBRES	CARGO
MAMANI POMA, ORLANDO JIMMY	AUDITOR SUPERIOR

AUDITORIA DE APLICACIONES

1. Alcance de la Auditoria

- Selección y evaluación del personal de le propia institución.
- Estándares de Funcionamiento y Procedimientos del área de informática
- Gestión Económica del área de Informática
- Estándares de funcionamiento y procedimiento del área de informática.

2. Objetivos

Realizar un informe de Auditoria con el objeto de verificar la adecuación de los estándares de funcionamiento y procedimiento del área de informática.

PREGUNTAS	SI	NO	N/A
1. ¿Existe una lista de proyectos de sistema de procedimiento de información y fechas programadas de implantación que puedan ser considerados como plan maestro?	X		
2. ¿Está relacionado el plan maestro con un plan general de desarrollo de la dependencia?		X	
3. ¿Ofrece el plan maestro la atención de solicitudes urgentes de los usuarios?		X	
4. ¿Asigna el plan maestro un porcentaje del tiempo total de producción al reproceso o fallas de equipo?		X	
5. Existe la lista de proyectos a corto plazo y largo plazo	X		
6. Existe una lista de sistemas en proceso periodicidad y usuarios	X		
7. Incluir el plazo estimado de acuerdo con los proyectos que se tienen en que el departamento de informática podría satisfacer las necesidades de la dependencia, según la situación actual	X		
8. ¿Considera que el Departamento de Sistemas de Información de los resultados esperados?	X		
9. ¿Existen fallas de exactitud en los procesos de información?	X		
10. ¿Se cuenta con un manual de usuario por Sistema?		X	
11. ¿Es claro y objetivo el manual del usuario?			X
12. ¿Que opinión tiene el manual? _____			X
13. ¿Se interviene de su departamento en el diseño de sistemas? _____		X	

Auditoria de Aplicaciones:

- **Para hallar el SI**

  11 ⟶ 100%
  6 ⟶ X

  X = 54.54

- **Para hallar el NO**

  11 ⟶ 100%
  5 ⟶ X
  X = 45.45

INFORME DE AUDITORIA

1. **Identificación del informe**

   Auditoria de Aplicaciones

2. **Identificación del Cliente**

   El área de Informática

3. **Identificación de la Entidad Auditada**

   Municipalidad Provincial Mariscal Nieto

4. **Objetivos**

   - Evaluar el papel del área de informática en la Institución
   - Evaluar el plan estratégico del área de Informática.
   - Evaluar la seguridad de los programas en el sentido de garantizar que los ejecutados por la maquina sean exactamente los previstos y no otros.
   - Evaluar la existencia del plan operativo anual del área de Informática
   - Verificar el cumplimiento de los objetivos, planes y presupuestos contenidos en el plan de sistemas de información.

- Evaluar el nivel de satisfacción de los usuarios del sistema.
- Verificar el grado de fiabilidad de la información.

5. Hallazgos Potenciales

- Incumplimiento de los plazos previstos en cada una de las fases del proyecto.
- Ineficacia e inseguridad del sistema de control de accesos diseñado.
- Falta de metodologías utilizadas que asegure la modularidad de las posibles futuras ampliaciones de la Aplicación y el fácil mantenimiento de las mismas.
- Incompatibilidad de las herramientas técnicas utilizadas en los diversos programas.
- Falta de sencillez, modularidad y economía de recursos del diseño de programas.

6. Alcance de la auditoria

Nuestra auditoria, comprende el presente periodo 2004 y se ha realizado especialmente al área de Informática de acuerdo a las normas y demás disposiciones aplicable al efecto.

7. Conclusiones:

- Como resultado de la Auditoria de Aplicaciones realizada al Municipio, por el período comprendido entre el 01 de Setiembre al 24 de Diciembre del 2004, podemos manifestar que hemos cumplido con evaluar cada uno de los objetivos contenidos en el programa de auditoria.
- El área de Informática presenta deficiencias sobre todo en la falta de metodologías que son necesarias al realizar un proyecto.

8. Recomendaciones

- Emplear metodologías que asegure la modularidad de las posibles futuras ampliaciones de la Aplicación y el fácil mantenimiento de las mismas.
- Realizar un control Interno de las Aplicaciones, verificando que las mismas fases se utilicen en el área correspondiente de Desarrollo
- Hacer un estudio de Vialidad de la Aplicación sobre todo para aquellas que son largas complejas y caras.
- Utilizar herramientas técnicas compatibles
- Capacitar al personal para el diseño de Programas para realizarlos con la máxima sencillez, modularidad y economía de recursos

9. Fecha Del Informe

	PLANEAMIENTO	EJECUCION	INFORME
FECHAS	01–10–04 al 15–10-04	16-10–04 al 20–11-04	23–11–04 al 28–11-04

10. Identificación Y Firma Del Auditor

APELLIDOS Y NOMBRES	CARGO
MAMANI POMA ORLANDO	AUDITOR SUPERIOR

Auditoria	SI	NO
Fisica	31.1	68.86
Ofimatica	67.5	18.91
Direccion	70.58	29.41
Explotación	65	35
Desarrollo	72.97	22.02
Mantenimiento	72	28
Base de Datos	79.16	20.83
Calidad	55.5	44.4
Seguridad	38.46	61.53
Redes	42.85	57.14
Aplicacion	54.54	45.45

CONCLUSIÓN

Al realizar el anterior trabajo se investigo acerca de todos los elementos que componen "La Municipalidad Provincial de Mariscal Nieto", tanto materiales como humanos, con lo anterior, se puede dar uno cuenta auditar una institución no es nada fácil, ya que si falla un elemento del que se compone, trae consigo un efecto domino, que hace que los demás elementos bajen su rendimiento, o en el peor de los casos sean causantes del fracaso de la institución.

Es mentira que lo más importante para una empresa sea el equipo informático con el que se trabaja. El factor humano es lo mas importante, ya que si se cuenta con tecnología de punta, pero con personal no calificado o en desacuerdo con el desarrollo del Centro de Computo optara por renunciar, o bien por seguir rezagando al mismo Asimismo la capacitación es importantísima, ya que si no hay capacitación permanente, el personal técnico de la empresa decide abandonarla para buscar nuevos horizontes y mayor oportunidad, aun sacrificando el aspecto económico.

El aspecto organizativo también debe estar perfectamente estructurado, y las líneas de mando deben estar bien definidas, evitando de esta manera la rotación innecesaria de personal, la duplicidad de funciones, las líneas alternas demando, etc. y que conllevan al desquiciamiento de la estructura organizacional.

Hablando de seguridad, es indispensable el aseguramiento del equipo y de las instalaciones, así como de la información, el control de los accesos también es punto fundamental para evitar las fugas de información o manipulación indebida de esta.

El Departamento de informática es la parte medular de la empresa, es en donde los datos se convierten en información útil a las diferentes áreas, es donde se guarda esta información y por consecuencia, donde en la mayoría de los casos se toman las decisiones importantes para la empresa.

Además al realizar la presente auditoria nos damos cuenta que dentro del ambiente empresarial es de vital importancia contar con la información lo más valiosa que sea, a tiempo, de forma oportuna, clara, precisa y con cero errores para que se constituya en una herramienta poderosa para la toma de decisiones, viéndose reflejada en la obtención de resultados benéficos a los fines de la organización y justificar el existir de toda la organización o empresa.

Como resultado de la Auditoria Informática realizada a la Municipalidad Provincial de Mariscal Nieto, por el período comprendido entre el 01 de Setiembre al 29 de Diciembre del 2004, podemos manifestar que hemos cumplido con evaluar cada uno de los objetivos contenidos en el programa de auditoria.

El área de Informática presenta deficiencias en:

En su Seguridad

En el área Física

En de Redes

Y en el debido cumplimiento de sus funciones.

Podremos estar tranquilos y seguros que nuestra función de auditores está funcionando como se debe, y saber que cuando se siguen estos lineamientos se obtendrán sistemas que no van a necesitar mantenimiento excesivo, que el cómputo va a ser parte de la solución y no parte del problema, como lo es hoy en día.

Informe Final de la Auditoria

LA MUNICIPALIDAD PROVINCIAL DE MARISCAL NIETO

Moquegua, 29 de Diciembre de 2.004
Señor Cervantes Games, Ivan
JEFE DEL ÁREA DE INFORMÁTICA

De nuestra consideración:
Tenemos el agrado de dirigirnos a Ud. a efectos de elevar a vuestra consideración el alcance del trabajo de Auditoría del Área de Informática practicada los días 16 de Setiembre al 23 de Diciembre, sobre la base del análisis y procedimientos detallados de todas las informaciones recopiladas y emitidos en el presente informe, que a nuestro criterio es razonable.

Síntesis de la revisión realizada, clasificado en las siguientes secciones:
1. **En su Seguridad**
2. **En el área Física**
3. **En Redes**

El contenido del informe ha sido dividido de la siguiente forma a efectos de facilitar su análisis.
a. Situación. Describe brevemente las debilidades resultantes de nuestro análisis.
b. Efectos y/o implicancias probables. Enuncian los posibles riesgos a que se encuentran expuestos las operaciones realizadas por la Cooperativa.
c. Índice de importancia establecida. Indica con una calificación del 0 al 3 el grado crítico del problema y la oportunidad en que se deben tomar las acciones correctivas del caso.
0 = Alto (acciones correctivas inmediatas)
1 = Alto (acciones preventivas inmediatas)
2 = Medio (acciones diferidas correctivas)
3 = Bajo (acciones diferidas preventivas)

Según el análisis realizado hemos encontrado falencias en que no existe un Comité y plan informático; falencias en la seguridad física y lógica; no existe auditoria de sistemas; falta de respaldo a las operaciones; accesos de los usuarios.
El detalle de las deficiencias encontradas, como así también las sugerencias de solución se encuentran especificadas en el Anexo adjunto. La aprobación y puesta en práctica de estas sugerencias ayudarán a la empresa a brindar un servicio más eficiente a los ciudadanos de la Ciudad de Moquegua.

Agradecemos la colaboración prestada durante nuestra visita por todo el personal de la Municipalidad y quedamos a vuestra disposición para cualquier aclaración y/o ampliación de la presente que estime necesaria.

Atentamente.

ORLANDO JIMMY MAMANI POMA
MICHELLA AROHUANCA A.
WILLY MAMANI CUTIPA
CARMEN QUIÑONEZ MAYTA
MADELEINE MUÑOZ ORTEGA
NELSSY POCOHUANCA TURPO

A. Organización y Administración del Área

A.1. Comité y Plan Informático
a. Situación

Con respecto al relevamiento efectuado, hemos notado lo siguiente:
• No existe un Comité de Informática o al menos no se encuentra formalmente establecido.
• No existe ninguna metodología de planificación, concepción y/o seguimiento de proyectos.

b. Efectos y/o implicancias probables
• Posibilidad de que las soluciones que se implementen para resolver problemas operativos sean
parciales, tanto en Hardware como en Software.

c. Indice de importancia establecida
1 (uno)

d. Sugerencias
• Establecer un Comité de Informática integrado por representantes de las áreas funcionales claves (Gerencia Administrativa, responsables de las Áreas Operativas, responsables de Informática y el responsable Contable).
• Trazar los lineamientos de dirección del Área de Informática.
• Implementar normas y/o procedimientos que aseguren la eficaz administración de los recursos
informáticos, y permitan el crecimiento coherente del área conforme a la implementación de las
soluciones que se desarrollen y/o se requieran de terceros.

. Efectos y/o implicancias probables
• La escasez de personal debidamente capacitado, aumenta el nivel de riesgo de errores al disminuir la posibilidad de los controles internos en el procesamiento de la información; y limita la
cantidad de soluciones que pueden implementarse en tiempo y forma oportuna a los efectos de satisfacer los requerimientos de las áreas funcionales.

B. Seguridad Física Y Lógica

B.1. Entorno General
a. Situación

Durante nuestra revisión, hemos observado lo siguiente:

• No existe una vigilancia estricta del Área de Informática por personal de seguridad dedicado a
este sector.
• No existe detectores, ni extintores automáticos.
• Existe material altamente inflamable.
• Carencia de un estudio de vulnerabilidad de la Cooperativa, frente a las riesgos físicos o no físicos, incluyendo el riesgo Informático.
• No existe un puesto o cargo especifico para la función de seguridad Informática.

b. Efectos y/o implicancias probables

• Probable difusión de datos confidenciales.
• Alta facilidad para cambios involuntarios o intencionales de datos, debido a la falta de controles
internos.
• Debido a la debilidad del servicio de mantenimiento del equipo central, la continuidad de las actividades informáticas podrían verse seriamente afectadas ante eventuales roturas y/o desperfectos de los sistemas.

c. Índice de importancia establecida
0 (cero)

d. Sugerencias

A los efectos de minimizar los riesgos descriptos, se sugiere:
• Establecer guardia de seguridad, durante horarios no habilitados para el ingreso al Área de Informática.
• Colocar detectores y extintores de incendios automáticos en los lugares necesarios.
• Remover del Centro de Cómputos los materiales inflamables.
• Determinar orgánicamente la función de seguridad.
• Realizar periódicamente un estudio de vulnerabilidad, documentando efectivamente el mismo, a
los efectos de implementar las acciones correctivas sobre los puntos débiles que se detecten.

B.2. Auditoría de Sistema
a. Situación
• Hemos observado que la Municipalidad no cuenta con auditoría Informática , ni con políticas
formales que establezcan responsables, frecuencias y metodología a seguir para efectuar revisiones de los archivos de auditoría.
• Cabe destacar que el sistema integrado posee un archivo que pudiera servir de auditoria Informática, el cual no es habilitado por falta de espacio en el disco duro.

b. Efectos y/o implicancias probables
• Posibilidad de que adulteraciones voluntarias o involuntarias sean realizadas a los elementos componentes del procesamiento de datos (programas, archivos de datos, definiciones de seguridad de acceso, etc) o bien accesos a datos confidenciales por personas no autorizadas que no sean detectadas oportunamente.

c. Índice de importancia establecida
0 (cero)

d. Sugerencias
• Establecer normas y procedimientos en los que se fijen responsables, periodicidad y metodología de control de todos los archivos de auditoria que pudieran existir como asimismo, de
todos los elementos componentes de los sistemas de aplicación.

B.3. Operaciones de Respaldo
a. Situación
Durante nuestra revisión hemos observado que:
• Existe una rutina de trabajo de tomar una copia de respaldo de datos en Disckett, que se encuentra en el recinto del centro de cómputos, en poder del auxiliar de informática.
• Si bien existen la copia de seguridad, no se poseen normas y/o procedimientos que exijan la prueba sistemática de las mismas a efectos de establecer los mínimos niveles de confiabilidad.

b. Efectos y/o implicancias probables
• La Cooperativa está expuesta a la perdida de información por no poseer un chequeo sistemático
periódico de los back-up's, y que los mismas se exponen a riesgo por encontrarse en poder del auxiliar de informática.

c. Índice de importancia establecida
0 (cero)

d. Sugerencias
Minimizar los efectos, será posible a través de:
• Desarrollar normas y procedimientos generales que permitan la toma de respaldo necesarios,
utilitario a utilizar.
• Realizar 3 copias de respaldos de datos en Zip de las cuales, una se encuentre en el recinto del
área de informática, otra en la sucursal más cercana y la última en poder del Jefe de área.
• Implementar pruebas sistemáticas semanales de las copias y distribución de las mismas.

B.4. Acceso a usuarios
a. Situación

De acuerdo a lo relevado hemos constatado que:
• Existen niveles de acceso permitidos, los cuales son establecidos conforme a la función que cumple cada uno de los usuarios.

• Los usuarios definidos al rotar o retirarse del local no son borrados de los perfiles de acceso.
• Las terminales en uso y dado un cierto tipo de inactividad no salen del sistema.
• El sistema informático no solicita al usuario, el cambio del Password en forma mensual.

b. Efectos y/o implicancia probables
• Existe la imposibilidad de establecer responsabilidades dado que esta se encuentra dividida entre el área de sistema y los usuarios finales.
• La falta de seguridad en la utilización de los Password, podrían ocasionar fraudes por terceros.

c. Índice de importancia establecida
2 (dos)

d. Sugerencia
• Implementar algún software de seguridad y auditoria existente en el mercado o desarrollar uno
propio.
• Establecer una metodología que permita ejercer un control efectivo sobre el uso o modificación
de los programas o archivos por el personal autorizado.

B.5. Plan de Contingencias
a. Situación
En el transcurso de nuestro trabajo hemos observado lo siguiente:
• Ausencia de un Plan de Contingencia debidamente formalizado en el Área de Informática.
• No existen normas y procedimientos que indiquen las tareas manuales e informáticas que son
necesarias para realizar y recuperar la capacidad de procesamiento ante una eventual contingencia (desperfectos de equipos, incendios, cortes de energía con más de una hora), y que determinen los niveles de participación y responsabilidades del área de sistemas y de los usuarios.
• No existen acuerdos formalizados de Centro de Cómputos paralelos con otras empresas o proveedores que permitan la restauración inmediata de los servicios informáticos de la Cooperativa en tiempo oportuno, en caso de contingencia.

b. Efectos y/o implicancia probable
• Pérdida de información vital.
• Pérdida de la capacidad de procesamiento.

c. Índice de Importancia relativa
1 (uno)

d. Sugerencias
• Establecer un plan de contingencia escrito, en donde se establezcan los procedimientos manuales e informáticos para restablecer la operatoria normal de la Cooperativa y establecer los

responsables de cada sistema.
• Efectuar pruebas simuladas en forma periódica, a efectos de monitorear el desempeño de los funcionarios responsables ante eventuales desastres.
• Establecer convenios bilaterales con empresas o proveedores a los efectos de asegurar los equipos necesarios para sustentar la continuidad del procesamiento.

C. Desarrollo y mantenimiento de los sistemas de aplicaciones

C.1. Entorno de Desarrollo y mantenimiento de las aplicaciones
a. Situación
• No existe documentaciones técnicas del sistema integrado de la Cooperativa y tampoco no existe un control o registro formal de las modificaciones efectuadas.
• No se cuenta con un Software que permita la seguridad de las librerías de los programas y la restricción y/o control del acceso de los mismos.
• Las modificaciones a los programas son solicitadas generalmente sin notas internas, en donde
se describen los cambios o modificaciones que se requieren.

b. Efectos y/o implicancias probables
• La escasa documentación técnica de cada sistema dificulta la compresión de las normas, demandando tiempos considerables para su mantenimiento e imposibilitando la capacitación del
personal nuevo en el área.
• Se incrementa aún más la posibilidad de producir modificaciones erróneas y/o no autorizadas a
los programas o archivos y que las mismas no sean detectadas en forma oportuna.

c. Índice de importancia establecida
1 (uno)

d. Sugerencias
Para reducir el impacto sobre los resultados de los efectos y consecuencias probables sugerimos:
• Elaborar toda la documentación técnica correspondiente a los sistemas implementados y establecer normas y procedimientos para los desarrollos y su actualización.
• Evaluar e implementar un software que permita mantener el resguardo de acceso de los archivos de programas y aún de los programadores.
• Implementar y conservar todas las documentaciones de prueba de los sistemas, como así también las modificaciones y aprobaciones de programas realizadas por los usuarios

Hardware
Equipamiento Central
La cooperativa cuenta actualmente con un Equipo Central Pentium IV con las siguientes características:
• Procesador Intel Pentium IV de 1.600 mhz
• Memoria: Ram 128 MB

• Almacenamiento: 35 GB de 10 K RPM
• Conexión: Ethernet 10/100
Es un equipamiento ideal para las funciones que cumple y su configuración es aceptable. Tiene posibilidades de crecimiento y el fabricante cuenta con repuestos y mantenimientos que garantizan la buena utilización del mismo.

Equipamiento Periférico
La cooperativa cuenta en su casa central con 30 PC´s de las cuales el 50%(cincuenta por ciento) aproximadamente son Pentium III de 550Mhs con 64 MB de memoria y discos de 5 GB. El resto son de menor porte, pero el parque de computadoras personales es suficientemente apto para los requerimientos actuales.
Las impresoras: de sistema (conectadas al equipo central) son de marca Epson 1170 y Epson 1200.
Además cuentan con equipos de HP 560 de chorro de tintas conectadas a algunos equipos.

Equipamiento en Sucursales
Las sucursales cuentan con PC´s AMD – Athlon de 750 Mhz, 64 de memoria y discos de 5 GB.
Equipamiento holgadamente apto para las funciones que cumple.
Las sucursales tienen una impresora matricial del sistema y algunos usuarios cuentan con impresoras a chorro de tinta.

Cableado
El cableado es estructurado y con cables del tipo UTP categoría 5, tanto en sucursales como Área Informática

Software
Software de Base
El sistema operativo con el que cuenta la Pentium IV es el de Windows Server 2000 que posee una importante estructura de seguridad.
Con sistema de red Windows 2000. Base de datos FOX .

ANEXOS

Encuesta

1. ¿El área cumple con las funciones asignadas en el MOF de la Institución?
2. ¿Cuántas personas laboran en el centro de cómputo?
   Laboran 4 Personas.
3. ¿Considera que el área de trabajo es la adecuada o apropiada para el desempeño de sus labores?
4. ¿Considera que es adecuado el número de personas que laboran en el área?
5. ¿Se deja de realizar alguna actividad por falta de personal?
6. ¿Esta el personal que utiliza el computador educado en las necesidades de seguridad?
7. Con respecto a la parte física de la OCI; ¿se cumple con las normas de seguridad establecidas para los equipos de cómputo?
8. ¿Esta el área del computador libre de material combustible, como suministro de papel en exceso de las necesidades inmediatas?
9. ¿Existe en la OCI extinguidores de incendio claramente identificados para lo que uso se refiere?
10. Sobre el mantenimiento del equipo; ¿cuenta con las herramientas necesarias para brindar un buen servicio en el momento requerido?
11. ¿El área cuenta con un respectivo plan de contingencias?
12. Si cuenta con un plan de contingencias ¿Se han identificado las aplicaciones vitales para operación del área?

Contrato de mantenimiento

Identificación de las partes

Objeto del contrato (*el cliente confía al proveedor un conjunto de prestaciones en el campo de los servicios informáticos que tiene como finalidad el mantenimiento del software registrado en el contexto de la propuesta técnica*).

Características de la prestación del servicio:

- Inventario de los objetos software a mantener.
- Estado inicial del software.
- Condiciones de organización del trabajo del proveedor y del cliente.
- Condiciones de formalización de la intervención de mantenimiento.
- Adaptación del Plan de Garantía de Calidad al cliente.
- Corrección de las anomalías.
- Mantenimiento de la competencia sobre el software aplicativo y sobre el software estándar por parte del proveedor.
- Redacción de la documentación facilitada a título de prestación anexa. Se determinan, entre otros aspectos, el formato y los plazos de entrega de ésta.
- Modalidad de asistencia a los usuarios finales.

Obligaciones del cliente

Obligaciones del proveedor

Cláusulas de exclusión

Cláusulas de organización

Garantía de las intervenciones

8.1 Recuperación de datos

8.2 Definición de responsabilidades

9) Otras cláusulas

CONSEJOS

1. Utiliza un buen antivirus y actualízalo frecuentemente.
2. Comprueba que tu antivirus incluye soporte técnico, resolución urgente de nuevos virus y servicios de alerta.
3. Asegúrate de que tu antivirus esté siempre activo.
4. Verifica, antes de abrir, cada nuevo mensaje de correo electrónico recibido.
5. Evita la descarga de programas de lugares no seguros en Internet.
6. Rechaza archivos que no hayas solicitado cuando estés en chats o grupos de noticias (news)
7. Analiza siempre con un buen antivirus los disquetes que vayas a usar en tu ordenador.
8. Retira los disquetes de las disqueteras al apagar o reiniciar tu ordenador.
9. Analiza el contenido de los archivos comprimidos.
10. Mantente alerta ante acciones sospechosas de posibles virus.
11. Añade las opciones de seguridad de las aplicaciones que usas normalmente a tu política de protección antivirus.
12. Realiza periódicamente copias de seguridad.
13. Mantente informado.
14. Utiliza siempre software legal.
15. Exige a los fabricantes de software, proveedores de acceso a Internet y editores de publicaciones, que se impliquen en la lucha contra los virus.

POLÍTICAS EN INFORMÁTICA PROPUESTA

TITULO I
DISPOSICIONES GENERALES

ARTICULO 1°.- El presente ordenamiento tiene por objeto estandarizar y contribuir al desarrollo informático de las diferentes unidades administrativas de la Empresa NN.
ARTICULO 2°.- Para los efectos de este instrumento se entenderá por:
Comité: Al equipo integrado por la Dirección , Subdirección, los Jefes departamentales y el personal administrativo de las diferentes unidades administrativas (Ocasionalmente) convocado para fines específicos como:

- Adquisiciones de Hardware y software
- Establecimiento de estándares de la Empresa NN tanto de hardware como de software
- Establecimiento de la Arquitectura tecnológica de grupo.
- Establecimiento de lineamientos para concursos de ofertas

Administración de Informática: Está integrada por la Dirección, Subdirección y Jefes Departamentales, las cuales son responsables de:

- Velar por el funcionamiento de la tecnología informática que se utilice en las diferentes unidades administrativas
- Elaborar y efectuar seguimiento del Plan Maestro de Informática
- Definir estrategias y objetivos a corto, mediano y largo plazo
- Mantener la Arquitectura tecnológica
- Controlar la calidad del servicio brindado
- Mantener el Inventario actualizado de los recursos informáticos
- Velar por el cumplimiento de las Políticas y Procedimientos establecidos.

ARTICULO 3°.- Para los efectos de este documento, se entiende por Políticas en Informática, al conjunto de reglas obligatorias, que deben observar los Jefes de Sistemas

responsables del hardware y software existente en la Empresa NN, siendo responsabilidad de la Administración de Informática, vigilar su estricta observancia en el

ámbito de su competencia, tomando las medidas preventivas y correctivas para que se cumplan.

ARTICULO 4°.- Las Políticas en Informática son el conjunto de ordenamientos y lineamientos enmarcados en el ámbito jurídico y administrativo de la Empresa NN. Estas normas inciden en la adquisición y el uso de los Bienes y Servicios Informáticos en la Empresa NN, las cuales se deberán de acatar invariablemente, por aquellas instancias que intervengan directa y/o indirectamente en ello.

ARTICULO 5°.- La instancia rectora de los sistemas de informática de la Empresa NN es la Administración, y el organismo competente para la aplicación de este ordenamiento, es el Comité.

ARTICULO 6°.- Las presentes Políticas aquí contenidas, son de observancia para la adquisición y uso de bienes y servicios informáticos, en la Empresa NN, cuyo incumplimiento generará que se incurra en responsabilidad administrativa; sujetándose a lo dispuesto en la sección Responsabilidades Administrativas de Sistemas.

ARTICULO 7°.- Las empresas de la Empresa NN deberán contar con un Jefe o responsable del Area de Sistemas, en el que recaiga la administración de los Bienes y Servicios, que vigilará la correcta aplicación de los ordenamientos establecidos por el Comité y demás disposiciones aplicables.

TITULO II

LINEAMIENTOS PARA LA ADQUISICION DE BIENES DE INFORMATICA

ARTICULO 8°.- Toda adquisición de tecnología informática se efectúa a través del Comité, que está conformado por el personal de la Administración de Informática y Gerente Administrativo de la unidad solicitante de bienes o servicios informáticos.

ARTICULO 9°.- La adquisición de Bienes de Informática en la Empresa NN, quedará sujeta a los lineamientos establecidos en este documento.

ARTICULO 10°.- La Administración de Informática, al planear las operaciones relativas a la adquisición de Bienes informáticos, establecerá prioridades y en su selección deberá tomar en cuenta: estudio técnico, precio, calidad, experiencia, desarrollo tecnológico, estándares y capacidad, entendiéndose por:

- Precio.- Costo inicial, costo de mantenimiento y consumibles por el período estimado de uso de los equipos;
- Calidad.- Parámetro cualitativo que especifica las características técnicas de los recursos informáticos.
- Experiencia.- Presencia en el mercado nacional e internacional, estructura de servicio, la confiabilidad de los bienes y certificados de calidad con los que se cuente;
- Desarrollo Tecnológico.- Se deberá analizar su grado de obsolescencia, su nivel tecnológico con respecto a la oferta existente y su permanencia en el mercado;

- Estándares.- Toda adquisición se basa en los estándares, es decir la arquitectura de grupo empresarial establecida por el Comité. Esta arquitectura tiene una permanencia mínima de dos a cinco años.
- Capacidades.- Se deberá analizar si satisface la demanda actual con un margen de holgura y capacidad de crecimiento para soportar la carga de trabajo del área.

ARTICULO 11°.- Para la adquisición de Hardware se o bservará lo siguiente:

a) El equipo que se desee adquirir deberá estar dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores del mismo y dentro de los estándares de la Empresa NN.

b) Deberán tener un año de garantía como mínimo

c) Deberán ser equipos integrados de fábrica o ensamblados con componentes previamente evaluados por el Comité.

d) La marca de los equipos o componentes deberá contar con presencia y permanencia demostrada en el mercado nacional e internacional, así como con asistencia técnica y refaccionaria local.

e) Tratándose de equipos microcomputadoras, a fin de mantener actualizado la arquitectura informático de la Empresa NN, el Comité emitirá periódicamente las especificaciones técnicas mínimas para su adquisición.

f) Los dispositivos de almacenamiento, así como las interfaces de entrada/salida, deberán estar acordes con la tecnología de punta vigente, tanto en velocidad de transferencia de datos, como en el ciclo del proceso.
g) Las impresoras deberán apegarse a los estándares de Hardware y Software vigentes en el mercado y la Empresa NN, corroborando que los suministros (cintas, papel, etc.) se consigan fácilmente en el mercado y no estén sujetas a un solo proveedor.

h) Conjuntamente con los equipos, se deberá adquirir el equipo complementario adecuado para su correcto funcionamiento de acuerdo con las especificaciones de los fabricantes, y que esta adquisición se manifieste en el costo de la partida inicial.
i)Los equipos complementarios deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente en el país.
j) Los equipos adquiridos deben contar, de preferencia con asistencia técnica durante la instalación de los mismos.
k) En lo que se refiere a los computadores denominados servidores, equipo de comunicaciones como enrutadores y concentradores de medios, y otros que se justifiquen por ser de operación crítica y/o de alto costo; al vencer su período de garantía, deben de contar con un programa de mantenimiento preventivo y correctivo que incluya el suministro de refacciones.
l) En lo que se refiere a los computadores denominados personales, al vencer su garantía por adquisición, deben de contar por lo menos con un programa de servicio de mantenimiento correctivo que incluya el suministro de refacciones.
Todo proyecto de adquisición de bienes de informática, debe sujetarse al análisis, aprobación y autorización del Comité.
ARTICULO 12°: En la adquisición de Equipo de cómput o se deberá incluir el Software vigente precargado con su licencia correspondiente considerando las disposiciones del artículo siguiente.

ARTICULO 13°.- Para la adquisición de Software base y utilitarios, el Comité dará a conocer periódicamente las tendencias con tecnología de punta vigente, siendo la lista de productos autorizados la siguiente:

a. Plataformas de Sistemas Operativos:

MS-DOS, MS- Windows 95 Español, Windows NT, Novell Netware, Unix(Automotriz).

b. Bases de Datos:

Foxpro, Informix

c. Manejadores de bases de datos:

Foxpro para DOS, VisualFox, Access

d. Lenguajes de programación:

Los lenguajes de programación que se utilicen deben ser compatibles con las plataformas enlistadas.

SQL Windows
Visual Basic
VisualFox
CenturaWeb
Notes Designer

e. Hojas de cálculo:

Excel

f. Procesadores de palabras:

Word

g. Diseño Gráfico:

Page Maker, Corel Draw

h. Programas antivirus.

F-prot, Command Antivirus, Norton Antivirus

i. Correo electrónico

Notes Mail

j. Browser de Internet

Netscape

En la generalidad de los casos, sólo se adquirirán las últimas versiones liberadas de los productos seleccionados, salvo situaciones específicas que se deberán justificar ante el Comité. Todos los productos de Software que se adquieran deberán contar con su licencia de uso, documentación y garantía respectivas.

ARTICULO 14°.- Todos los productos de Software que se utilicen a partir de la fecha en que entre en vigor el presente ordenamiento, deberán contar con su licencia de uso respectiva; por lo que se promoverá la regularización o eliminación de los productos ya instalados que no cuenten con la licencia respectiva.

ARTICULO 15°.- Para la operación del software de re d se debe tener en consideración lo siguiente:

a) Toda la información institucional debe invariablemente ser operada a través de un mismo tipo de sistema manejador de base de datos para beneficiarse de los mecanismos de integridad, seguridad y recuperación de información en caso de falla del sistema de cómputo.

b) El acceso a los sistemas de información, debe contar con los privilegios ó niveles de seguridad de acceso suficientes para garantizar la seguridad total de la información institucional. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser manipulado por software. Se deben delimitar las responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes para cada caso.

c) El titular de la unidad administrativa responsable del sistema de información debe autorizar y solicitar la asignación de clave de acceso al titular de la Unidad de Informática.

d) Los datos de los sistemas de información, deben ser respaldados de acuerdo a la frecuencia de actualización de sus datos, rotando los dispositivos de respaldo y guardando respaldos históricos periódicamente. Es indispensable llevar una bitácora oficial de los respaldos realizados, asimismo, las cintas de respaldo deberán guardarse en un lugar de acceso restringido con condiciones ambientales suficientes para garantizar su conservación. Detalle explicativo se aprecia en la Política de respaldos en vigencia.

e) En cuanto a la información de los equipos de cómputo personales, la Unidad de Informática recomienda a los usuarios que realicen sus propios respaldos en la red o en medios de almacenamiento alternos.

f) Todos los sistemas de información que se tengan en operación, deben contar con sus respectivos manuales actualizados. Uno técnico que describa la estructura interna del sistema así como los programas,

catálogos y archivos que lo conforman y otro que describa a los usuarios del sistema, los procedimientos para su utilización.

h) Los sistemas de información, deben contemplar el registro histórico de las transacciones sobre datos relevantes, así como la clave del usuario y fecha en que se realizó (Normas Básicas de Auditoría y Control).

i)Se deben implantar rutinas periódicas de auditoría a la integridad de los datos y de los programas de cómputo, para garantizar su confiabilidad.

ARTICULO 16°.- Para la contratación del servicio de desarrollo o construcción de Software aplicativo se observará lo siguiente:

Todo proyecto de contratación de desarrollo o construcción de software requiere de un estudio de factibilidad que permita establecer la rentabilidad del proyecto así como los beneficios que se obtendrán del mismo.

Todo proyecto deberá ser aprobado por el Comité en base a un informe técnico que contenga lo siguiente:

- Bases del concurso (Requerimientos claramente especificados)
- Análisis de ofertas (Tres oferentes como mínimo) y Selección de oferta ganadora

Bases del Concurso

Las bases del concurso especifican claramente los objetivos del trabajo, delimita las responsabilidades de la empresa oferente y la contratante.

De las empresas oferentes:

Los requisitos que se deben solicitar a las empresas oferentes son:

a. Copia de la Cédula de Identidad del o los representantes de la compañía
b. Copia de los nombramientos actualizados de los representantes legales de la compañía
c. Copia de los Estatutos de la empresa, en que aparezca claramente definido el objeto de la compañía, esto es para determinar si está o no facultada para realizar la obra
d. Copia del RUC de la compañía

e. Referencias de clientes (Mínimo 3)
f. La carta con la oferta definitiva del contratista debe estar firmada por el representante legal de la compañía oferente.

De la contratante

Las responsabilidades de la contratante son:

a. Delinear adecuadamente los objetivos y alcance del aplicativo.
b. Establecer los requerimientos del aplicativo
c. Definir responsabilidades de la contratista y contratante
d. Establecer campos de acción

Análisis de ofertas y Selección de oferta ganadora:

Para definir la empresa oferente ganadora del concurso, el Comité establecerá una reunión en la que se debe considerar los siguientes factores:

a. Costo
b. Calidad
c. Tiempo de permanencia en el mercado de la empresa oferente
d. Experiencia en el desarrollo de aplicativos
e. Referencias comprobadas de Clientes
f. Cumplimiento en la entrega de los requisitos

Aprobada la oferta se debe considerar los siguientes lineamientos en la elaboración de contratos:

Todo contrato debe incluir lo siguiente:

Antecedentes, objeto del contrato, precio, forma de pago, plazo, obligaciones del contratista, responsabilidades, fiscalizador de la obra, garantías, entrega recepción de obra provisional y definitiva, sanciones por incumplimientos, rescisión del contrato, disposiciones supletorias, documentos incorporados, solución de controversias, entre otros aspectos.

Las garantías necesarias para cada contrato deben ser incluídas en forma conjunta con el Departamento Legal, quienes deben asesorar el tipo de garantía necesaria en la elaboración de cada contrato.

Las garantías que se deben aplicar de acuerdo al tipo de contrato son:

a. Una garantía bancaria o una póliza de seguros, incondicional, irrevocable y de cobro inmediato por el 5% del monto total del contrato para asegurar su fiel cumplimiento, la cual se mantendrá vigente durante todo el tiempo que subsista la obligación motivo de la garantía.

b. Una garantía bancaria o una póliza de seguros, incondicional, irrevocable y de cobro inmediato equivalente al 100 % (ciento por ciento) del anticipo. Esta garantía se devolverá en su integridad una vez que el anticipo se haya amortizado en la forma de pago estipulada en el contrato.

c. Un fondo de garantía que será retenido de cada planilla en un porcentaje del 5 %.

Junto al contrato se deberá mantener la historia respectiva del mismo que se compone de la siguiente documentación soporte:

- Estudio de factibilidad
- Bases del concurso
- Ofertas presentadas
- Acta de aceptación de oferta firmada por los integrantes del Comité
- Informes de fiscalización
- Acta de entrega provisional y definitiva

TITULO III

INSTALACIONES

ARTICULO 17°.- La instalación del equipo de cómputo , quedará sujeta a los siguientes lineamientos:

a) Los equipos para uso interno se instalarán en lugares adecuados, lejos de polvo y tráfico de personas.

En las áreas de atención directa al público los equipos se instalarán en lugares adecuados.

b) La Administración de Informática, así como las áreas operativas deberán contar con un croquis actualizado de las instalaciones eléctricas y de comunicaciones del equipo de cómputo en red.

c) Las instalaciones eléctricas y de comunicaciones, estarán de preferencia fijas o en su defecto resguardadas del paso de personas o máquinas, y libres de cualquier interferencia eléctrica o magnética.
d) Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios;
e) En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.
f) Cuando en la instalación se alimenten elevadores, motores y maquinaria pesada, se deberá tener un circuito independiente, exclusivo para el equipo y/o red de cómputo.

ARTICULO 18°.- La supervisión y control de las instalaciones se llevará a cabo en los plazos y mediante los mecanismos que establezca el Comité.

TITULO IV
LINEAMIENTOS EN INFORMATICA
CAPITULO I
INFORMACION

ARTICULO 19°.- Los archivos magnéticos de información se deberán inventariar, anexando la descripción y las especificaciones de los mismos, clasificando la información en tres categorías:

1. Información histórica para auditorías
2. Información de interés de la Empresa NN
3. Información de interés exclusivo de algún área en particular.

ARTICULO 20°.- Los jefes de sistemas responsables del equipo de cómputo y de la información contenida en los centros de cómputo a su cargo, delimitarán las responsabilidades de sus subordinados y determinarán quien está autorizado a efectuar operaciones emergentes con dicha información tomando las medidas de seguridad pertinentes.
ARTICULO 21°.- Se establecen tres tipos de prioridad para la información:

1. Información vital para el funcionamiento de la unidad administrativa;
2. Información necesaria, pero no indispensable en la unidad administrativa;
3. Información ocasional o eventual.

ARTICULO 22°.- En caso de información vital para el funcionamiento de la unidad administrativa, se deberán tener procesos concomitantes, así como tener el respaldo diario de las modificaciones efectuadas, rotando los dispositivos de respaldo y guardando respaldos históricos semanalmente.

ARTICULO 23°.- La información necesaria pero no ind ispensable, deberá ser respaldada con una frecuencia mínima de una semana, rotando los dispositivos de respaldo y guardando respaldos históricos mensualmente.

ARTICULO 24°.- El respaldo de la información ocasio nal o eventual queda a criterio de la unidad administrativa.

ARTICULO 25°.- Los archivos magnéticos de informaci ón, de carácter histórico quedarán documentados como activos de la unidad académica y estarán debidamente resguardados en su lugar de almacenamiento.

Es obligación del responsable del equipo de cómputo, la entrega conveniente de los archivos magnéticos de información, a quien le suceda en el cargo.

ARTICULO 26°.- Los sistemas de información en opera ción, como los que se desarrollen deberán contar con sus respectivos manuales. Un manual del usuario que describa los procedimientos de operación y el manual técnico que describa su estructura interna, programas, catálogos y archivos.

CAPITULO II

FUNCIONAMIENTO

ARTICULO 27°.- Es obligación de la Administración d e Informática vigilar que el equipo de cómputo se use bajo las condiciones especificadas por el proveedor y de acuerdo a las funciones del área a la que se asigne.

ARTICULO 28°.- Los colaboradores de la empresa al u sar el equipo de cómputo, se abstendrán de consumir alimentos, fumar o realizar actos que perjudiquen el funcionamiento del mismo o deterioren la información almacenada en medios magnéticos, ópticos, etc.

ARTICULO 29°.- Por seguridad de los recursos inform áticos se deben establecer seguridades:

- Físicas

- Sistema Operativo
- Software
- Comunicaciones
- Base de Datos
- Proceso
- Aplicaciones

Por ello se establecen los siguientes lineamientos:

- Mantener claves de acceso que permitan el uso solamente al personal autorizado para ello.
- Verificar la información que provenga de fuentes externas a fin de corroborar que estén libres de cualquier agente externo que pueda contaminarla o perjudique el funcionamiento de los equipos.
- Mantener pólizas de seguros de los recursos informáticos en funcionamiento

ARTICULO 30°.- En ningún caso se autorizará la utilización de dispositivos ajenos a los procesos informáticos de la unidad administrativa.

Por consiguiente, se prohibe el ingreso y/o instalación de hardware y software particular, es decir que no sea propiedad de una unidad administrativa de la Empresa NN, excepto en casos emergentes que la Dirección autorice.

CAPITULO III
PLAN DE CONTINGENCIAS

ARTICULO 31°.- La Administración de Informática creará para las empresas y departamentos un plan de contingencias informáticas que incluya al menos los siguientes puntos:

a) Continuar con la operación de la unidad administrativa con procedimientos informáticos alternos;

b) Tener los respaldos de información en un lugar seguro, fuera del lugar en el que se encuentran los equipos.

c) Tener el apoyo por medios magnéticos o en forma documental, de las operaciones necesarias para reconstruir los archivos dañados;

d) Contar con un instructivo de operación para la detección de posibles fallas, para que toda acción correctiva se efectúe con la mínima degradación posible de los datos;
e) Contar con un directorio del personal interno y del personal externo de soporte, al cual se pueda recurrir en el momento en que se detecte cualquier anomalía;
f) Ejecutar pruebas de la funcionalidad del plan
f) Mantener revisiones del plan a fin de efectuar las actualizantes respectivas

CAPITULO IV
ESTRATEGIAS

ARTICULO 32.- La estrategia informática de la DDT se consolida en el Plan Maestro de Informática y está orientada hacia los siguientes puntos:
a) Plataforma de Sistemas Abiertos;
b) Descentralización del proceso de información
c) Esquemas de operación bajo el concepto cliente/servidor
d) Estandarización de hardware, software base, utilitarios y estructuras de datos
e) Intercomunicación entre unidades y equipos mediante protocolos estándares
f) Intercambio de experiencias entre Departamentos de Informática.
g) Manejo de proyectos conjuntos con las diferentes unidades administrativas.
h) Programa de capacitación permanente para los colaboradores de la empresa del área de informática
i) Integración de sistemas y bases de datos de la Empresa NN, para tener como meta final un Sistema Integral de Información Corporativo.
j) Programación con ayudas visuales e interactivas. Facilitando interfases amigables al usuario final.
k) Integración de sistemas teleinformáticos (Intranet De grupo empresarial).

ARTICULO 33°.- Para la elaboración de los proyectos informáticos y para la presupuestación de los mismos, se tomarán en cuentan tanto las necesidades de hardware y software de la unidad administrativa solicitante, como la disponibilidad de recursos con que éstas cuenten.

DISPOSICIONES TRANSITORIAS

ARTICULO PRIMERO.- Las disposiciones aquí enmarcadas, entrarán en vigor a partir del día siguiente de su difusión.

ARTICULO SEGUNDO.- Las normas y políticas objeto de este documento, podrán ser modificadas o adecuadas conforme a las necesidades que se vayan presentando, mediante acuerdo del Comité Técnico de Informática de la Empresa NN (CTI); una vez aprobadas dichas modificaciones o adecuaciones, se establecerá su vigencia.

ARTICULO TERCERO.- Las disposiciones aquí descritas constan de forma detallada en los manuales de políticas y procedimientos específicos existentes.

ARTICULO CUARTO.- La falta de desconocimiento de las normas aquí descritas por parte de los colaboradores no los libera de la aplicación de sanciones y/o penalidades por el incumplimiento de las mismas.

Bibliografía

- Audinet : http://www.audinet.org
- Sans Institute : http://www.sans.org
- AUDITORIA INFORMATICA. Un enfoque práctico
  Mario Piatini – Emilio del Peso Ed. Rama
- AUDITORIA DE LOS SISTEMAS DE INFORMACIÓN
  Rafael Bernal y Óscar Coltell – Univ. Politécnica de Valencia