Ejemplos de Preguntas a realizar en una auditoria de sistemas.

Los ejemplos siguientes han sido extraidos de la Auditoría informática en la Municipalidad Provincial Mariscal Nieto, Perú. Son a título informativo, para que el alumno las tome como ejemplo de que preguntar, no para que copie las preguntas ya que son aplicables en este ejemplo y en otro caso pueden no ser aplicables.

### AUDITORIA FISICA

1. **Alcance de la Auditoria**
	1. Organización y cualificación del personal de Seguridad.
	2. Remodelar el ambiente de trabajo.
	3. Planes y procedimientos.
	4. Sistemas técnicos de Seguridad y Protección.
2. **Objetivos**
	1. Revisión de las políticas y Normas sobre seguridad Física.
	2. Verificar la seguridad de personal, datos, hardware, software e instalaciones
	3. 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 casode 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 unposible 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 unaemergencia (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 debendesalojar 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 siexiste? | **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 estascopias? |  | **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 establecidoprocedimientos de operación? |  | **X** |  |
| 37. ¿Se ha establecido que información puede ser acezada y por qué persona? |  | **X** |  |

**AUDITORIA DE LA OFIMATICA**

1. **Alcance de la Auditoria.-**
2. Planes y procedimientos
3. Políticas de Mantenimiento
4. Inventarios Ofimaticos
5. Capacitación del Personal
6. **Objetivos de la Auditoria.-**
	1. 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? |  | **X** |  |
| 2. ¿Existe un comité que coordine y seresponsabilice de todo el proceso de adquisición e instalación? |  | **X** |  |
| 3. ¿Han elaborado un instructivo con procedimientos a seguir para la selección y adquisición de equipos, programas y servicios computacionales? | **X** |  |  |
| 4. ¿se cuenta con software de oficina? | **X** |  |  |
| 5. ¿Se han efectuado las acciones necesarias para una mayor participación de proveedores? | **X** |  |  |
| 6. ¿Se ha asegurado un respaldo de mantenimiento y asistencia técnica? | **X** |  |  |
| 7. ¿El acceso al centro de cómputo cuenta con las seguridades necesarias para reservar el ingreso al personal autorizado? |  | **X** |  |
| 8. ¿Se han implantado claves o password para garantizar operación de consola y equipo central (mainframe), a personal autorizado? | **X** |  |  |
| 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 deviolación? | **X** |  |  |
| 10. ¿Se mantiene un registro permanente (bitácora) de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos? |  | **X** |  |
| 11. ¿Los operadores del equipo central están entrenados para recuperar o restaurar información en caso de destrucción de archivos? | **X** |  |  |
| 12. ¿Los backups son mayores de dos (padres e hijos) y se guardan en lugares seguros y adecuados, preferentemente en bóvedas de bancos?  |  | **X** |  |
| 13. ¿Se han implantado calendarios de operación a fin de establecer prioridades de proceso? |  | **X** |  |
| 14. ¿Todas las actividades del Centro de Computo están normadas mediante manuales, instructivos, normas, reglamentos, etc.? | **X** |  |  |
| 15. ¿Las instalaciones cuentan con sistema de alarma por presencia de fuego, humo, así como extintores de incendio,conexiones eléctricas seguras, entre otras? |  |  | **X** |
| 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? |  | **X** |  |
| 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? | **X** |  |  |
| 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? | **X** |  |  |
| 19. ¿Si se vence la garantía de mantenimiento del proveedor se contrata mantenimiento preventivo y correctivo? | **X** |  |  |
| 20. ¿Se establecen procedimientos para obtención de backups de paquetes y de archivos de datos? | **X** |  |  |
| 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? |  |  | **X** |
| 22. ¿Se mantiene programas y procedimientos de detección e inmunización de virus en copias no autorizadas o datos procesados en otros equipos? | **X** |  |  |
| 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? | **X** |  |  |
| 24. ¿existen licencias? | **X** |  |  |

**AUDITORIA DE LA DIRECCION**

1. **Alcance de la Auditoria.-**
	1. Organización y calificación de la dirección de Informática
	2. Plan Estratégico de Sistemas de Información.
	3. Análisis de puestos
	4. Planes y Procedimientos
	5. Normativa
	6. Gestión Económica.
2. **Objetivos de la Auditoria.-**
	1. Realizar un informe de Auditoria con el objeto de verificar la adecuación de las
	2. medidas aplicadas a las amenazas definidas, así como el cumplimiento de los
	3. requisitos exigidos.
3. **Resultados: Se obtendrá:**
	1. Informe de Auditoria detectando riesgos y deficiencias en la Dirección de Informática.
	2. Plan de recomendaciones a aplicar en función de:
		1. 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? | **X** |  |  |
| 2. ¿Dispone su institución de un plan Estratégico de Tecnología de Información? | **X** |  |  |
| 3. ¿Durante el proceso de planificación, se presta adecuada atención al plan estratégico de la empresa? | **X** |  |  |
| 4. ¿Las tareas y actividades en el plan tiene la correspondiente y adecuada asignación de recursos? |  | **X** |  |
| 5. ¿Existe un comité de informática? |  |  | **X** |
| 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? |  | **X** |  |
| 7. ¿Existen estándares de funcionamiento y procedimientos y descripciones de puestos de trabajo adecuados y actualizados? |  | **X** |  |
| 8. ¿Los estándares y procedimientos existentes promueven una filosofía adecuada de control? |  | **X** |  |
| 9. ¿Las descripciones de los puestos de trabajo reflejan las actividades realizadas en la práctica? | **X** |  |  |
| 10. ¿La selección de personal se basa en criterios objetivos y tiene en cuenta la formación, experiencia y niveles de responsabilidad? | **X** |  |  |
| 11. ¿El rendimiento de cada empleado se evalúa regularmente en base a estándares establecidos? | **X** |  |  |
| 12. ¿Existen procesos para determinar las necesidades de formación de los empleados en base a su experiencia? | **X** |  |  |
| 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? | **X** |  |  |
| 14. ¿Existe un presupuesto económico? ¿y hay un proceso para elaborarlo? | **X** |  |  |
| 15. ¿Existen procedimientos para la adquisición de bienes y servicios? | **X** |  |  |
| 16. ¿Existe un plan operativo anual? | **X** |  |  |
| 17. ¿Existe un sistema de reparto de costes informáticos y que este sea justo? |  | **X** |  |
| 18. ¿Cuentan con pólizas de seguros? | **X** |  |  |
| 19. ¿Existen procedimientos para vigilar y determinar permanentemente la legislación aplicable? |  |  | **X** |

**AUDITORIA DE LA EXPLOTACION**

1. **Alcance de la Auditoria**
	1. Evaluación del personal y coherencia de cargos de la propia institución.
	2. 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 ?
 | **X** |  |  |
| 1. ¿existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros manuales y programas, que permitan construir las operaciones que sean necesarias?
 |  |  | **X** |
| 1. ¿se aprueban por personal autorizado las solicitudes de nuevas aplicaciones?
 | **X** |  |  |
| 1. ¿existe personal con autoridad suficiente que es el que aprueba los cambios de unas aplicaciones por otras?
 | **X** |  |  |
| 1. ¿existen procedimientos adecuados para mantener la documentación al día ?
 |  | **X** |  |
| 1. ¿tienen manuales todas las aplicaciones ?
 |  |  | **X** |
| 1. ¿existen controles que garanticen el uso adecuado de discos y cintas?
 | **X** |  |  |
| 1. ¿existen procedimientos adecuados para conectarce y desconectarce de los equipos remotos?
 | **X** |  |  |
| 1. ¿se aprueban los programas nuevos y los que se revisan antes de ponerlos en funcionamiento?
 |  |  |  |
| 1. ¿revisan y evalúan los resultados de las pruebas finales dando su aprobación los departamentos de usuario antes de poner en funcionamiento las aplicaciones?
 | **X** |  |  |
| 1. al poner en funcionamiento nuevas aplicaciones o versiones actualizada ¿funcionan en paralelo las existentes durante un cierto tiempo?
 | **X** |  |  |
| 1. ¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento, al personal autorizado?
 | **X** |  |  |
| 1. ¿Se tiene relación del personal autorizado para firmar la salida de archivos confidenciales?
 |  | **X** |  |
| 1. ¿Existe un procedimiento para registrar los archivos que se prestan y la fecha en que se devolverán?
 | **X** |  |  |
| 1. ¿Se lleva control sobre los archivos prestados por la instalación?
 |  |  | **X** |
| 1. ¿Se conserva la cinta maestra anterior hasta después de la nueva cinta?
 | **X** |  |  |
| 1. ¿El cintotecario controla la cinta maestra anterior previendo su uso incorrecto o su eliminación prematura?
 | **X** |  |  |
| 1. ¿La operación de reemplazo es controlada por el cintotecario?
 | **X** |  |  |
| 1. ¿Se utiliza la política de conservación de archivos hijo-padre-abuelo?
 | **X** |  |  |
| 1. En los procesos que manejan archivos en línea, ¿Existen procedimientos para recuperar los archivos?
 | **X** |  |  |
| 1. ¿Estos procedimientos los conocen los operadores?
 |  | **X** |  |
| 1. ¿Existe un responsable en caso de falla?
 | **X** |  |  |
| 1. ¿Explique que políticas se siguen para la obtención de archivos de respaldo?
 | **X** |  |  |
| 1. ¿Existe un procedimiento para el manejo de la información de la cintoteca?
 |  | **X** |  |
| 1. ¿Lo conoce y lo sigue el cintotecario?
 |  |  | **X** |
| 1. ¿Existe un programa de trabajo de captación de datos?
 |  | **X** |  |
| 1. ¿se controla las entradas de documentos fuente?
 | **X** |  |  |
| 1. ¿Que cifras de control se obtienen?

Sistema Cifras que se Observaciones Obtienen |  | **X** |  |
| 1. ¿existen documento de entrada se tienen? Sistemas Documentos Dpto. que periodicidad Observaciones proporciona el documento
 | **X** |  |  |
| 1. ¿Se anota que persona recibe la información y su volumen?
 |  | **X** |  |
| 1. ¿Se anota a que capturista se entrega la información, el volumen y la hora?
 |  | **X** |  |
| 1. ¿Se verifica la cantidad de la información recibida para su captura?
 | **X** |  |  |
| 1. ¿Se revisan las cifras de control antes de enviarlas a captura?
 |  | **X** |  |
| 1. ¿Para aquellos procesos que no traigan cifras de control se ha establecido criterios a fin de asegurar que la información es completa y valida?
 | **X** |  |  |
| 1. ¿Existe un procedimiento escrito que indique como tratar la información inválida (sin firma ilegible, no corresponden las cifras de control)?
 |  | **X** |  |
| 1. En caso de resguardo de información de entrada en sistemas, ¿Se custodian en un lugar seguro?
 | **X** |  |  |
| 1. Si se queda en el departamento de sistemas, ¿Por cuanto tiempo se
2. guarda?
 |  | **X** |  |
| 1. ¿Existe un registro de anomalías en la información debido a mala codificación?
 |  | **X** |  | **X** |  |
| 1. ¿Existe una relación completa de distribución de listados, en la cual se indiquen personas, secuencia y sistemas a los que pertenecen?
 |  |  |  |  |
| 1. ¿Se verifica que las cifras de las validaciones concuerden con los documentos de entrada?
 | **X** |  |  |
| 1. ¿Se hace una relación de cuando y a quién fueron distribuidos los listados?
 |  | **X** |  |
| 1. ¿Se controlan separadamente los documentos confidenciales?
 | **X** |  |  |
| 1. ¿Se aprovecha adecuadamente el papel de los listados inservibles?
 |  | **X** |  |
| 1. ¿Existe un registro de los documentos que entran a capturar?
 | **X** |  |  |
| 1. ¿Se lleva un control de la producción por persona?
 | **XX** |  |  |
| 1. ¿existe parámetros de control?
 |  |  | **X** |

**AUDITORIA DEL DESARROLLO**

1. **Alcance de la Auditoria**
	1. Conexiones
	2. Cifrado
	3. Salidas gateway y routers
	4. Correo Electrónico
	5. Páginas WEB
	6. Firewalls
2. **Objetivos**
	1. revisar el cumplimiento del proceso completo de desarrollo de proyectos
	2. verificar las metodologías utilizadas
	3. verificar el control interno de las aplicaciones, satisfacción de los usuarios y control de procesos y ejecuciones de programas críticos.
	4. 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? | X |  |  |
| 2. ¿se comprueban los resultados con datos reales? | X |  |  |
| 3. ¿Existe un organigrama con la estructura de organización delárea? | X |  |  |
| 4. ¿Existe un manual de organización que regula las relaciones entre puestos? | X |  |  |  |
| 5. ¿Existe la relación de personal adscrito al área, incluyendo el puesto ocupado por cada persona? | X |  |  |
| 6. ¿El plan existe, es claro y realista? | X |  |  |
| 7. ¿Están establecidos los procedimientos de promoción de personal a puestos superiores, teniendo en cuenta la experienciay formación? | X |  |  |
| 8. ¿El área de desarrollo lleva su propio control presupuestario? |  | X |  |
| 9. ¿Se hace un presupuesto por ejercicio y se cumple? | X |  |  |
| 10. ¿El presupuesto esta en concordancia con los objetivos acumplir? | X |  |  |
| 11. ¿El personal de área de desarrollo cuenta con la formaciónadecuada y son motivados para la realización de su trabajo? |  | X |  |
| 12. ¿Existen procedimientos de contratación? | X |  |  |
| 13. ¿Las personas seleccionadas cumplen los requisitos del puestoal que acceden? | X |  |  |
| 14. ¿Las ofertas de puestos del área se difunden de forma suficientefuera de la organización y las selecciones se hacen de forma objetiva? |  | X |  |
| 15. ¿Existe un plan de formación que este en consonancia con losobjetivos tecnológicos que se tenga en el área? |  |  | X |
| 16. ¿El plan de trabajo del área tiene en cuenta los tiempos deformación? | X |  |  |
| 17. ¿Existe un protocolo de recepción / abandono para las personasque se incorporan o dejan el área? |  |  | X |
| 18. ¿Existe un protocolo y se respeta para cada incorporación /abandono? |  |  | X |
| 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? | X |  |  |
| 21. ¿Esta disponible un numero suficiente de libros, publicacionesperiódicas, monografías, de reconocido prestigio y el personal tiene acceso a ellos? | X |  |  |
| 22. ¿El personal esta motivado en la realización de su trabajo? | X |  |  |
| 23. ¿Existe algún mecanismo que permita a los empleados hacersugerencias sobre mejoras en la organización del área? | X |  |  |
| 24. ¿Existe rotación de personal y existe un buen ambiente de trabajo? | X |  |  |
| 25. ¿La realización de nuevos proyectos se basa en el plan desistemas en cuanto a objetivos? | X |  |  |
| 26. ¿Las fechassistemas? | de | realización | coinciden | con | los | del | plan | de | X |  |  |
| 27. ¿El plan de sistemas se actualiza con la información que segenera a lo largo de un proceso? | X |  |  |
| 28. ¿Los cambios en los planes de los proyectos se comunican alresponsable de mantenimiento del plan de sistemas? | X |  |  |
| 29. ¿Existe un procedimiento para la propuesta de realización denuevos proyectos? | X |  |  |
| 30. ¿Existe un mecanismo para registrar necesidades de desarrollode nuevos sistemas? |  | X |  |
| 31. ¿Se respeta este mecanismo en todas las propuestas? |  | X |  |
| 32. ¿Existe un procedimiento de aprobación de nuevos proyectos? | X |  |  |
| 33. ¿Existe un procedimiento para asignar director y equipo dedesarrollo a cada nuevo proyecto? |  |  | X |
| 34. ¿Se tiene en cuenta a todas las personas disponibles cuyo perfilsea adecuado a los riesgos de cada proyecto y que tenga disponibilidad para participar? |  |  | X |  |  |
| 35. ¿Existe un protocolo para solicitar al resto de las áreas la participación del personal en el proyecto y se aplica dicho protocolo? | X |  |  |
| 36. ¿Existe un procedimiento para conseguir los recursos materialesnecesarios para cada proyecto? | X |  |  |
| 37. ¿Se tiene implantada una metodología de desarrollo de sistemasde información soportada por herramientas de ayuda? | X |  |  |
| 38. ¿La metodología cubre todas las fases del desarrollo y esadaptable a distintos tipos de proyectos? |  |  | X |
| 39. ¿La metodología y las técnicas asociadas a la misma están adaptadas al entorno tecnológico y a la organización del área de desarrollo? |  |  | X |
| 40. ¿Existe un catalogo de las aplicaciones disponible en el área? |  | X |  |
| 41. ¿Existe un registro de problemas que se producen en los proyectos del área? |  | X |  |
| 42. ¿Existe un catalogo de problemas? |  | X |  |
| 43. ¿El catalogo es accesible para todos los miembros del área? |  |  | X |
| 44. ¿Se registran y controlan todos los proyectos fracasados? | X |  |  |

**AUDITORIA DEL MANTENIMIENTO**

1. **Alcance de la Auditoria.-**
	1. Planes y procedimientos de Mantenimiento
	2. Normativa
2. **Objetivos de la Auditoria.-**

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

1. **Referencia Legal:**
	1. Estándares
		1. ISO/IEC 12207
		2. IEEE 1074
		3. IEEE 1219
		4. ISO/IEC 14764

|  |  |  |  |
| --- | --- | --- | --- |
| **PREGUNTAS** | **SI** | **NO** | **N/A** |
| 1. Existe un contrato de mantenimiento. |  | **X** |  |
| 2. ¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo? | **X** |  |  |
| 3. ¿Se lleva a cabo tal programa? | **X** |  |  |
| 4. ¿Existen tiempos de respuesta y de compostura estipulados en los contratos? |  |  | **X** |
| 5. Si los tiempos de reparación son superiores a los estipulados en el contrato, ¿Qué acciones correctivas se toman para ajustarlos a lo convenido? |  |  | **X** |  | **X** |
| 6. ¿Existe plan de mantenimiento preventivo? |  |  |  |  |
| 7. ¿Este plan es proporcionado por el proveedor? |  | **X** |  |
| 8. ¿Se notifican las fallas? | **X** |  |  |
| 9. ¿Se les da seguimiento? |  | **X** |  |
| 10. ¿Tiene un plan logístico para dar soporte al producto software? |  | **X** |  |
| 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? | **X** |  |  |
| 12. ¿Las variaciones en el diseño son supervisadas durante el desarrollo para establecer su impacto sobre la mantenibilidad? | **X** |  |  |
| 13. ¿Se realizan varios tipos de medidas para poder estimar lacalidad del software? | **X** |  |  |
| 14. ¿La mantenibilidad se tiene en cuenta antes de empezar adesarrollar? | **X** |  |  |
| 15. ¿El desarrollador prepara un Plan de Mantenibilidad que establece prácticas específicas de mantenibilidad, asícomo recursos y secuencias relevantes de actividades? | **X** |  |  |
| 1. ¿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
 | **X** |  |  |
| 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 delmantenimiento? |  | **X** |  |
| 1. ¿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. | **X** |  |  |
| 19. ¿El mantenedor a menudo se encuentra con un productosoftware con documentación? |  | **X** |  |
| 1. ¿Si no hay documentación, el mantenedor deberá crearla?

¿Realiza lo siguiente?* 1. Comprender el dominio del problema y operar con el producto software.
	2. Aprender la estructura y organización del producto software.
	3. Determinar qué hace el producto software. Revisar las especificaciones (si las hubiera)
 | **X** |  |  |
| 21. ¿Documentos como especificaciones, manuales de mantenimiento para programadores, manuales de usuarioo guías de instalación pueden ser modificados o creados, si fuese necesario? | **X** |  |  |
| 22. El Plan de Mantenimiento es preparado por el mantenedor durante el desarrollo del software. | **X** |  |  |
| 23. ¿Los elementos software reflejan la documentación de diseño? | **X** |  |  |
| 24. ¿Los productos software fueron suficientemente probados y sus especificaciones cumplidas? | **X** |  |  |
| 25. ¿Los informes de pruebas son correctos y las discrepancias entre resultados actuales y esperados han sido resueltas? | **X** |  |  |
| 26. ¿La documentación de usuario cumple los estándares especificados? | **X** |  |  |
| 27. ¿Los costesestablecidos? | y | calendarios | se | ajustan | a | los | Planes  | **X** |  |  |

**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.

1. **Objetivos**
	1. ”Verificar la responsabilidad para la planificación de planillas y control de los activos de datos de la organización” (administrador de datos)
	2. “Verificar la responsabilidad de la administración del entorno de la base de datos” (administrador de la base de datos)
	3. 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 | **X** |  |  |
| 2. La organización tiene un sistema de gestión de base de datos (SGBD) | **X** |  |  |
| 3. Los datos son cargados correctamente en la interfaz grafica | **X** |  |  |
| 4. Se verificará que los controles y relaciones de datos se realizan de acuerdo a Normalización libre de error | **X** |  |  |
| 5. Existe personal restringido que tenga acceso a la BD | **X** |  |  |
| 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 | **X** |  |  |
| 8. ¿Existen procedimientos formales para la operación del SGBD? | **X** |  |  |
| 9. ¿Están actualizados los procedimientos de SGBD? | **X** |  |  |
| 10. ¿La periodicidad de la actualización de los procedimientos es Anual ? | **X** |  |  |
| 11. ¿Son suficientemente claras las operaciones que realiza la BD? | **X** |  |  |
| 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) | **X** |  |  |
| 13. ¿Se procesa las operaciones dentro del departamento de cómputo? | **X** |  |  |
| 14. ¿Se verifican con frecuencia la validez de los inventarios de los archivos magnéticos? | **X** |  |  |
| 15. ¿Existe un control estricto de las copias de estos archivos? | **X** |  |  |
| 16. ¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos? | **X** |  |  |
| 17. ¿Se registran como parte del inventario las nuevas cintas magnéticas que recibe el centro de computo? | **X** |  |  |
| 18. ¿Se tiene un responsable del SGBD? | **X** |  |  |
| 19. ¿Se realizan auditorias periódicas a los medios de almacenamiento? |  | **X** |  |
| 20. ¿Se tiene relación del personal autorizado para manipular la BD? |  | **X** |  |
| 21. ¿Se lleva control sobre los archivos trasmitidos por el sistema? |  | **X** |  |
| 22. ¿Existe un programa de mantenimiento preventivo para el dispositivo del SGBD? |  |  | **X** |
| 23. ¿Existen integridad de los componentes y de seguridad de datos? | **X** |  |  |
| 24. De acuerdo con los tiempos de utilización de cada dispositivo del sistema de cómputo, ¿existe equipo capaces que soportar el trabajo? | **X** |  |  |
| 25. ¿El SGBD tiene capacidad de teleproceso? |  | **X** |  |
| 26. ¿Se ha investigado si ese tiempo de respuesta satisface a los usuarios? |  |  | **X** |
| 27. ¿La capacidad de almacenamiento máximo de la BD essuficiente para atender el proceso por lotes y el proceso remoto? |  |  | **X** |

**AUDITORIA DE CALIDAD**

1. **Objetivos:**
	1. Verificar los procesos aplicables del programa de la calidad han sido desarrollados y documentados.
	2. Evaluar la capacidad de realizar un trabajo especifico.

|  |  |  |  |
| --- | --- | --- | --- |
| **PREGUNTAS** | **SI** | **NO** | **N/A** |
| ¿Se reflejan el software codificado tal como en el diseño en ladocumentación? |  | **X** |  |
| ¿Fueron probados con éxito los productos de software usados enel centro de computo? | **X** |  |  |
| ¿Se cumplen las especificaciones de la documentación delusuario del software? | **X** |  |  |
| ¿Los procesos de gestión administrativa aplicados en el área deinformática de la institución son lo suficientemente óptimos? |  | **X** |  |
| ¿El funcionamiento del software dentro del área de trabajo estánde acuerdo con los requerimientos específicos? | **X** |  |  |
| ¿Los documentos de gestión administrativa se cumplensatisfactoriamente en el área de computo? |  | **X** |  |
| ¿Los productos de software que utilizan en el área de informáticaesta de acuerdo con los estándares establecidos? | **X** |  |  |
| ¿Los dispositivos de trabajo en el área de informática se les realizan una revisión técnica correcta? | **X** |  |  |
| ¿Los costos fijados en la revisión técnica se encuentran dentro delos límites fijados? |  | **X** |  |

**AUDITORIA DE LA SEGURIDAD**

1. **Alcance de la Auditoria.-**
	1. Organización y calificación del personal
	2. Planes y procedimientos
	3. Sistemas técnicos de detección y comunicación
	4. Análisis de puestos
	5. Mantenimiento
	6. 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.

1. **Referencia Legal:**
	1. Manual de Autoprotección aprobado por O.M. de 29/11/84, NBE-CPI 96 (RD 2177/96),
	2. Normativa de las Comunidades Autónomas y Ordenanzas Municipales, CEPREVEN.
2. **Resultados: Se obtendrá:**
	1. Informe de Auditoria detectando riesgos y deficiencias en el Sistema de Seguridad.
	2. Plan de recomendaciones a aplicar en función de:
		1. Riesgos
		2. Normativa a cumplir
		3. Costes estimados de las recomendaciones

##### AUDITORIA LOGICA

|  |  |  |  |
| --- | --- | --- | --- |
| **PREGUNTAS** | **SI** | **NO** | **N/A** |
| 1. ¿Existen medidas, controles, procedimientos, normas yestándares de seguridad? |  | **X** |  |
| 2. ¿Existe un documento donde este especificado la relación de lasfunciones y obligaciones del personal? |  | **X** |  |
| 3. | ¿Existen procedimientos de notificación y gestión de incidencias?  |  |  | **X** |
| 4. ¿Existen procedimientos de realización de copias de seguridad yde recuperación de datos? | **X** |  |  |
| 5. ¿Existe una relación del personal autorizado a conceder, alterar o anular el acceso sobre datos y recursos? | **X** |  |  |
| 6. ¿Existe una relación de controles periódicos a realizar para verificar el cumplimiento del documento? |  | **X** |  |
| 7. ¿Existen medidas a adoptar cuando un soporte vaya a ser desechado o reutilizado? |  | **X** |  |
| 8. ¿Existe una relación del personal autorizado a acceder a los locales donde se encuentren ubicados los sistemas que tratan datos personales? |  | **X** |  |
| 9. ¿Existe una relación de personal autorizado a acceder a los soportes de datos? |  | **X** |  |
| 10. ¿Existe un período máximo de vida de las contraseñas? | **X** |  |  |
| 11. ¿Existe una relación de usuarios autorizados a acceder a los sistemas y que incluye los tipos de acceso permitidos? |  | **X** |  |
| 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? |  | **X** |  |
| 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? |  | **X** |  |
| 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? |  |  | **X** |
| 15. ¿El sistema de autenticación de usuarios guarda las contraseñas encriptadas? | **X** |  |  |
| 1. ¿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.
 | **X** |  |  |
| 17. ¿Existen procedimientoscontraseñas? | de | asignación | y | distribución | de  | **X** |  |  |

**AUDITORIA FISICA**

|  |  |  |  |
| --- | --- | --- | --- |
| PREGUNTAS | **SI** | **NO** | **N/A** |
| 1. ¿Existen procedimientos para la realización de las copias de seguridad? | **X** |  |  |
| 2. ¿Existen procedimientos que aseguran que, de todos los ficheros con datos de carácter personal, se realiza copia al menos una vez cada semana? |  | **X** |  |
| 3. ¿Hay procedimientos que aseguran la realización de copias de todos aquellos ficheros que han experimentado algún cambio en su contenido? |  | **X** |  |
| 4. ¿Existen controles para la detección de incidencias en la realización de las pruebas? |  | **X** |  |
| 5. ¿Existen controles sobre el acceso físico a las copias de seguridad? | **X** |  |  |
| 6. ¿Sólo las personas con acceso autorizado en el documento de seguridad tienen acceso a los soportes que contienen las copias de seguridad? |  | **X** |  |
| 7. ¿Las copias de seguridad de ficheros de nivel alto incluyen los ficheros cifrados, si estas copias se transportan fuera de las instalaciones? |  |  | **X** |
| 8. ¿Las copias de seguridad de los ficheros de nivel alto se almacenan en lugar diferente al de los equipos que las procesan? | **X** |  |  |
| 9. ¿Existe un inventario de los soportes existentes? | **X** |  |  |
| 10. ¿Dicho inventario incluye las copias de seguridad? |  | **X** |  |
| 11. ¿Las copias de seguridad, o cualquier otro soporte, se almacenan fuera de la instalación? |  |  | **X** |
| 12. ¿Existen procedimientos de actualización de dicho inventario? |  | **X** |  |
| 13. ¿Existen procedimientos de etiquetado e identificación del contenido de los soportes? | **X** |  |  |
| 14. ¿Existen procedimientos en relación con la salida de soportes fuera de su almacenamiento habitual? |  | **X** |  |
| 15. ¿Se evalúan los estándares de distribución y envío de estos soportes? | **X** |  |  |
| 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? |  | **X** |  |
| 17. ¿Se Comprueba que todos los soportes incluidos en esa relación se encuentran también en el inventario de soportes mencionado anteriormente? |  |  | **X** |
| 1. ¿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)
 |  |  | **X** |
| 1. ¿Se Verifica que el Registro de Entrada y Salida refleja la información requerida por el Reglamento:
	1. Fecha y hora
	2. Emisor/Receptor
	3. Nº de soportes
	4. Tipo de información contenida en el soporte.
	5. Forma de envío
	6. Persona física responsable de la recepción/entrega
 | **X** |  |  |
| 20. ¿Se Analiza los procedimientos de actualización del Registro deEntrada y Salida en relación con el movimiento de soportes? | **X** |  |  |
| 21. ¿Existen controles para detectar la existencia de soportes recibidos/enviados que no se inscriben en el Registro deEntrada/Salida? |  | **X** |  |
| 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 lasemana? | **X** |  |  |
| 23. ¿Se realiza una relación de soportes enviados fuera de laempresa con la relación de ficheros de nivel alto? |  | **X** |
|  |  |
| 24. ¿Se Verifica que todos los soportes que contiene ficheros con datos de nivel Alto van cifrados? |  |  | **X** |
| 25. ¿Se Comprobar la existencia, como parte del Documento de Seguridad, de una relación de usuarios con acceso autorizado a la sala? |  | **X** |  |
| 26. ¿Se Verifica que la inclusión del personal en la relación anterior es coherente con las funciones que tienen encomendadas? |  | **X** |  |
| 27. ¿Se Comprueba que la relación es “lógica” (¿personal de limpieza? ¿Vigilantes de seguridad?). |  |  | **X** |
| 28. ¿Existen políticas de la instalación en relación con los accesos ocasionales a la sala’ |  |  | **X** |
| 29. ¿Se Determina que personas tienen llaves de acceso, tarjetas, etc. de acceso a la sala?. |  | **X** |  |
| 30. ¿Se Comprueba que están activados los parámetros de activación del Registro para todos los ficheros de Nivel Alto? |  |  | **X** |
| 31. ¿Se Analizan los procedimientos de descarga a cinta de este Registro de Accesos y el período de retención de este soporte? |  |  | **X** |
| 32. ¿Existen procedimientos de realización de copias de seguridad del Registro de Accesos y el período de retención de las copias? |  | **X** |  |
| 33. ¿Se Verifica la asignación de privilegios que permitan activar/desactivar el Registro de Accesos para uno o más ficheros? |  | **X** |  |
| 34. ¿Se Comprueba que el Registro de Accesos se encuentra bajo el control directo del Responsable de Seguridad pertinente? |  | **X** |  |

**AUDITORIA A LOS SISTEMAS DE REDES**

1. **Alcance de la Auditoria.-**
	1. Calificación del personal
	2. Sistemas técnicos de la red
	3. 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.

1. **Referencia Legal.-**
	1. Manual de Autoprotección aprobado por O.M. de 29/11/84, NBE-CPI 96 (RD 2177/96),
	2. Normativa de las Comunidades Autónomas y Ordenanzas Municipales, CEPREVEN.
2. **Resultados.-**
3. **Se obtendrá:**
	1. Informe de Auditoria detectando deficiencias en el Sistema de Redes.
	2. Plan de recomendaciones a aplicar en función de:
		1. Normativa a cumplir
		2. Recomendaciones

|  |  |  |  |
| --- | --- | --- | --- |
| **PREGUNTAS** | **SI** | **NO** | **N/A** |
| 1. La gerencia de redes tiene una política definida de planeamiento de tecnología de red? | **X** |  |  |
| 2. Esta política es acorde con el plan de calidad de la organización |  | **X** |  |
| 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? |  | **X** |  |
| 4. Existe un inventario de equipos y software asociados a las redes de datos? |  | **X** |  |  |
| 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? |  |  | **X** |  |
| 8. La responsabilidad operativa de las redes esta separada de las de operaciones del computador? |  | **X** |  |
| 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 |  | **X** |  |
| 10. Existen controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas? |  | **X** |  |
| 11. Existen controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.? |  | **X** |  |
| 12. Existen protocolos de comunicaron establecida | **X** |  |  |
| 13. Existe una topología estandarizada en toda la organización |  | **X** |  |
| 14. Existen normas que detallan que estándares que deben cumplir el hardware y el software de tecnología de redes? | **X** |  |  |
| 15. ¿La transmisión de la información en las redes es segura? | **X** |  |  |
| 16. ¿El acceso a la red tiene password? | **X** |  |  |

**AUDITORIA DE APLICACIONES**

1. **Alcance de la Auditoria**
2. Selección y evaluación del personal de le propia institución.
3. Estándares de Funcionamiento y Procedimientos del área de informática
4. Gestión Económica del área de Informática
5. Estándares de funcionamiento y procedimiento del área de informática.
6. **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** |  |