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