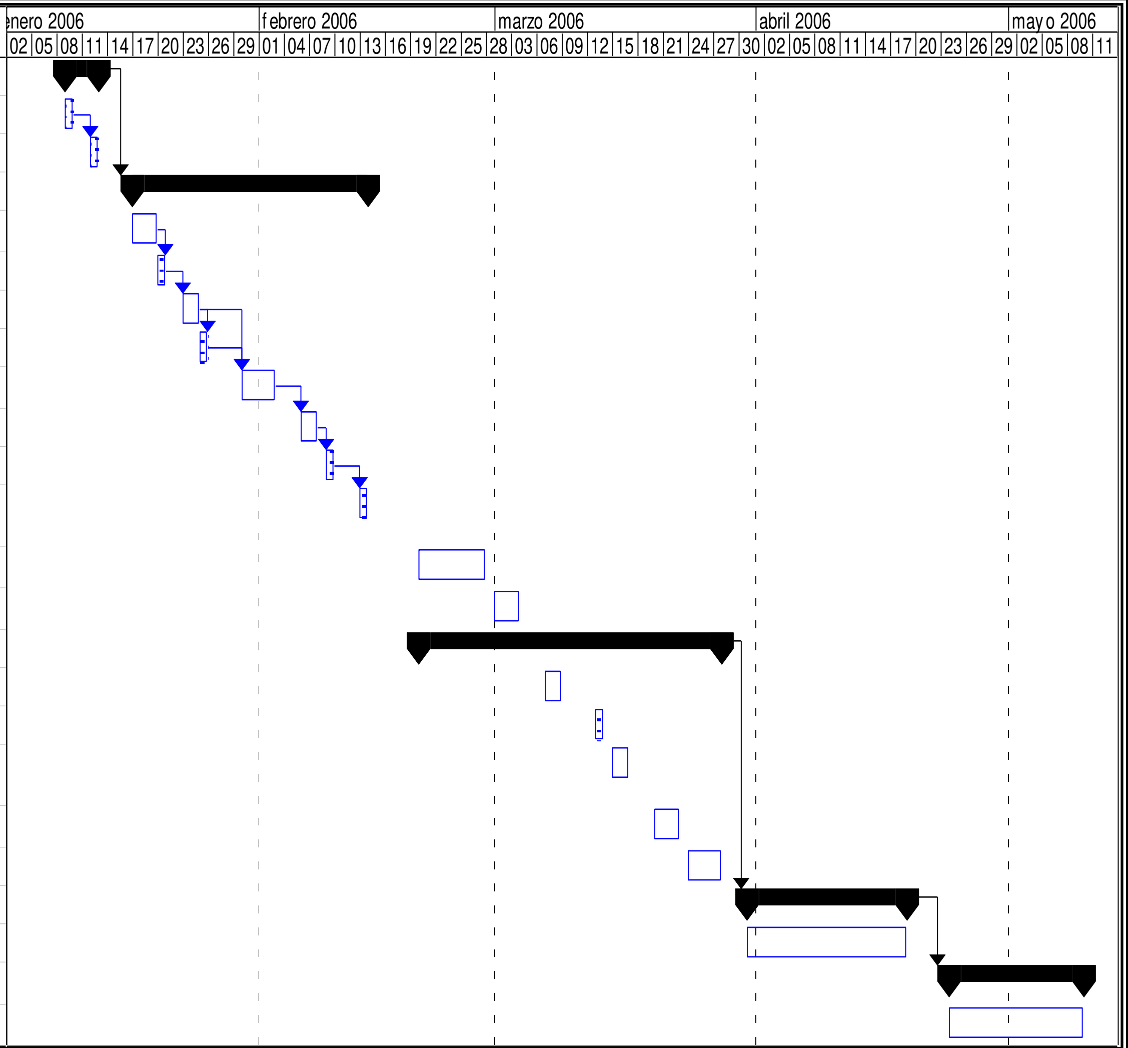
ANEXO 1

CRONOGRAMA DE TRABAJO

Id	Nombre de tarea	Duración	Comienzo	Fin
1	**RECONOCIMIENTO DEL ÁREA**	**4 días?**	**lun 09/01/06**	**jue 12/01/06**
2	Realizar cuestionario de Guía de Visita previa	1 día?	lun 09/01/06	lun 09/01/06
3	Entrevistar al Jefe del Departamento de Sistemas para tener conoc	1 día?	jue 12/01/06	jue 12/01/06
4	**IDENTIFICACIÓN DE VULNERABILIDADES**	**20 días?**	**mar 17/01/06**	**lun 13/02/06**
5	Entrevistar a los integrantes del Dpto de Sistemas para evaluar la seguridad física	3 días?	mar 17/01/06	jue 19/01/06
6	Solicitar plano físico de la organización	1 día?	vie 20/01/06	vie 20/01/06
7	Realizar la constatación física de los equipos	2 días?	lun 23/01/06	mar 24/01/06
8	Solicitar el contrato de mantenimiento	1 día?	mié 25/01/06	mié 25/01/06
9	Valorar la seguridad lógica mediante un cuestionario dirigido a los integrantes de Sistemas	4 días?	lun 30/01/06	jue 02/02/06
10	Realizar una entrevista a los encargados de la red	2 días?	lun 06/02/06	mar 07/02/06
11	Entrevistar al Jefe de Recursos Humanos para determinar la vulne	1 día?	jue 09/02/06	jue 09/02/06
12	Efectuar entrevista al Jede de Sistemas para tener conocimiento d los términos del contrato de outsourcing	1 día?	lun 13/02/06	lun 13/02/06
13	Determinar las vulnerabilidades que originan los factores de riesgo	6 días?	lun 20/02/06	lun 27/02/06
14	Definir los criterios que identifican a los factores de riesgo	3 días?	mié 01/03/06	vie 03/03/06
15	**ANÁLISIS DE RIESGOS**	**26 días?**	**lun 20/02/06**	**lun 27/03/06**
16	Realizar la ponderación de los factores de riesgo	2 días?	mar 07/03/06	mié 08/03/06
17	Realizar la valoración de los factores de riesgo	1 día?	lun 13/03/06	lun 13/03/06
18	Realizar la matriz descriptiva de factores de riesgo y valoraci asociada a los recursos informáticos	2 días?	mié 15/03/06	jue 16/03/06
19	Realizar la matriz ponderada de factores de riesgo y valoraci asociada a los recursos informáticos	3 días?	lun 20/03/06	mié 22/03/06
20	Realizar la matriz categorizada	2 días?	vie 24/03/06	lun 27/03/06
21	**POLÍTICAS DE SEGURIDAD**	**13 días?**	**vie 31/03/06**	**mar 18/04/06**
22	Elaborar políticas de seguridad informática	13 días?	vie 31/03/06	mar 18/04/06
23	**PLAN ESTRATÉGICO DE SEGURIDAD INFORMÁTICA**	**12 días?**	**lun 24/04/06**	**mar 09/05/06**
24	Elaborar el plan estratégico de seguridad informática	12 días?	lun 24/04/06	mar 09/05/06



ANEXO 2

PROGRAMA DE TRABAJO

1 - 4

Empresa: AGROPEC S.A. **Dpto:** Sistemas

OBJETIVOS/PROCEDIMIENTOS	REF.	HECHO POR	FECHA
Reconocimiento del área			
Objetivo:			
1. Obtener información de la funcionalidad del departamento dentro de la organización y el entorno en que realizan sus actividades			
Procedimientos:			
1. Realizar un cuestionario de visita previa que nos permitirá conocer los objetivos y actividades que realizá el Dpto. de Sistemas, su estructura organica junto con las funciones de cada integrante del área, quienes son las áreas usuarias de sistemas, la existencia de manuales y esquemas de seguridad.	Anexo 3	M.G.H.P	09-ene-06
2. Entrevistar al Jefe del Departamento con la finalidad de adquirir conocimiento de los recursos tecnológicos con que cuenta el área para realizar sus actividades y brindar un buen soporte de la información a la empresa	Anexo 4	M.G.H.P	12-ene-06

ANEXO 2
(CONTINUACIÓN)

PROGRAMA DE TRABAJO **2 - 4**

Empresa: AGROPEC S.A. **Dpto:** Sistemas

OBJETIVOS/PROCEDIMIENTOS	REF.	HECHO POR	FECHA
Identificación de riesgos			
Objetivo:			
1. Determinar los factores de riesgos de la organización.			
Procedimientos:			
1 Entrevista a los integrantes del área para evaluar la seguridad física.	Anexo 5 y 6	M.G.H.P	17-Ene-06 19-Ene-06
2. Solicitar plano físico de la organización.	Anexo 7	M.G.H.P	20-Ene-06
3. Realizar la constatación física de los equipos	Anexo 8 al 11	M.G.H.P	23-Ene-06 24-Ene-06
4. Solicitar el contrato de mantenimiento.	Anexo 12	M.G.H.P	25-Ene-06
5. Valorar la seguridad lógica mediante un cuestionario dirigido a los encargados de manejar el sistema y asignar las claves a los usuarios	Anexo 13 al 16	M.G.H.P	30-Ene-06 02-Feb-06
6. Realizar una entrevista a los encargados del manejo de la redes para evaluar su seguridad	Anexo 17 y 18	M.G.H.P	06-Feb-06 07-Feb-06
7. Entrevistar al jefe de recursos humanos para determinar la vulnerabilidad a traves del personal	Anexo 19	M.G.H.P	09-feb-06
8. Efectuar una entrevista al Jede de Sistemas para tener conocimiento de los términos del contrato de outsourcing	Anexo 20	M.G.H.P	13-Feb-06
9. Determinar las vulnerabilidades que originan los factores de riesgo	Anexo 21	M.G.H.P	20-Feb-06 27-Feb-06
10. Definir los criterios que identifican a los factores de riesgo	Anexo 22	M.G.H.P	01-Mar-06 02-Mar-06

ANEXO 2
(CONTINUACIÓN)

PROGRAMA DE TRABAJO 2 - 4

Empresa: AGROPEC S.A. **Dpto:** Sistemas

OBJETIVOS/PROCEDIMIENTOS	REF.	HECHO POR	FECHA
Identificación de riesgos			
Objetivo:			
1. Determinar los factores de riesgos de la organización.			
Procedimientos:			
1 Entrevista a los integrantes del área para evaluar la seguridad física.	Anexo 5 y 6	M.G.H.P	17-Ene-06 19-Ene-06
2. Solicitar plano físico de la organización.	Anexo 7	M.G.H.P	20-Ene-06
3. Realizar la constatación física de los equipos	Anexo 8 al 11	M.G.H.P	23-Ene-06 24-Ene-06
4. Solicitar el contrato de mantenimiento.	Anexo 12	M.G.H.P	25-Ene-06

5. Valorar la seguridad lógica mediante un cuestionario dirigido a los encargados de manejar el sistema y asignar las claves a los usuarios	Anexo 13 al 16	M.G.H.P	30-Ene-06 02-Feb-06
6. Realizar una entrevista a los encargados del manejo de la redes para evaluar su seguridad	Anexo 17 y 18	M.G.H.P	06-Feb-06 07-Feb-06
7. Entrevistar al jefe de recursos humanos para determinar la vulnerabilidad a traves del personal	Anexo 19	M.G.H.P	09-feb-06
8. Efectuar una entrevista al Jede de Sistemas para tener conocimiento de los términos del contrato de outsourcing	Anexo 20	M.G.H.P	13-Feb-06
9. Determinar las vulnerabilidades que originan los factores de riesgo	Anexo 21	M.G.H.P	20-Feb-06 27-Feb-06
10. Definir los criterios que identifican a los factores de riesgo	Anexo 22	M.G.H.P	01-Mar-06 02-Mar-06

ANEXO 2
(CONTINUACIÓN)

PROGRAMA DE TRABAJO **3 - 4**

Empresa: AGROPEC S.A. **Dpto:** Sistemas

OBJETIVOS/PROCEDIMIENTOS	REF.	HECHO POR	FECHA
Análisis de riesgos			
Objetivo:			

1. Cuantificar los niveles de riesgos			
Procedimientos:			
1. Realizar la ponderación de los factores de riesgo.	Anexo 23	M.G.H.P	07-Mar-06 08-Mar-06
2. Realizar la valoración de los factores de riesgo.	Anexo 24	M.G.H.P	13-mar-06
3. Realizar la matriz descriptiva de factores de riesgo y valoración asociada a los recursos informáticos.	Anexo 25	M.G.H.P	15-Mar-06 16-Mar-06
4. Realizar la matriz ponderada de factores de riesgo y valoración asociada a los recursos informáticos.	Anexo 26	M.G.H.P	20-Mar-06 22-Mar-06
5. Realizar la matriz categorizada.	Anexo 27	M.G.H.P	24-Mar06 27-Mar-06

ANEXO 2

(CONTINUACIÓN)

PROGRAMA DE TRABAJO			
Empresa: AGROPEC S.A.	**Dpto:** Sistemas	**4 - 4**	
OBJETIVOS/PROCEDIMIENTOS	**REF.**	**HECHO POR**	**FECHA**
Póliticas de Seguridad			
Objetivo:			
1. Establecer políticas de seguridad de acuerdo a la organización y su nivel de implementación en la organización.			
Procedimientos:			
1. Elaboración de las políticas de seguridad informática	Anexo 28	M.G.H.P	31-Mar-06 18-Ab-06
Plan Estratégico de Seguridad Informática			
1. Disminuir los factores de riesgos que la organización tiene.			
Procedimiento:			
1. Elaboración del plan estratégico de seguridad informática	Anexo 29	M.G.H.P	24-Ab-06 09-May-06
		ELAB. Ma. Gabriela Hernández Pinto	**FECHA:** 02-En-06

		REV. Ing. Alice Naranjo	**FECHA:** 04-En-06

ANEXO 3

CUESTIONARIO DE VISITA PREVIA

A. Información general

Nombre de la entidad: Agropec S.A.

Área: Sistemas

Dirección: Av. Juan Tanca Marengo Km. 2

Teléfono: 2-235263 Ext. 113

Jefe responsable: Ing. Milton Parrales

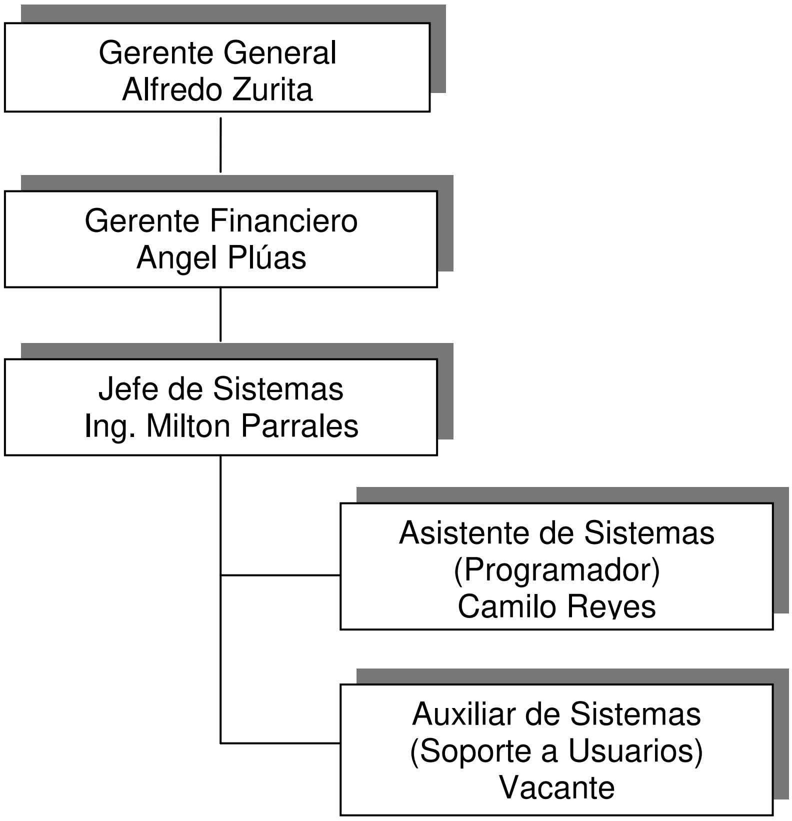
Colaborador: Camilo Reyes (Auxiliar de sistemas)

B. Conocimiento del área

1. ¿Cuales son los objetivos del área?

- Mejorar la plataforma tecnológica con el fin de optimizar los procesos operativos de la empresa.
- Mantener la información disponible y generar nueva información estadística en base a la necesidad de la gerencia.
- Mediante el uso de la tecnología minimizar los costos operativos y de los servicios.
- Mantener el buen funcionamiento de los equipos de la red de computación y los programas.

2. ¿Cuál es la estructura orgánica?



3. ¿Ha existido alguna modificación en la estructura orgánica?

Si **No**

4. ¿Existe un manual de las funciones?

Si No

5. ¿Existe un manual de políticas?

Si No

6. ¿Existe un manual de procedimientos?

Si No

7. ¿Existe un manual de políticas y procedimientos de seguridad?

   Si **No**

8. ¿Existe una persona encargada de administrar la seguridad?

   Si **No**

9. ¿Cuenta el área con asesoramiento en materia de seguridad?

   Si **No**

10. ¿Se ha evaluado la seguridad antes?

    Si **No**

11. ¿Qué esquemas de seguridad tiene su área?

- Procedimientos de respaldo en CD y disco duro.
- Control de claves de acceso y permisos a usuarios.
- Control de permisos en los servicios (internet, impresiones y uso del teléfono).
- Inventario mensual de los equipos.
- Escaneo de los equipos para evitar que se infecten con algún virus.

12. ¿Quienes son los usuarios del área?

- Financiero y Administrativo
- Compras e Importaciones
- Contabilidad
- Bodega

- Reenvase
- Ventas
- Recursos Humanos
- Legal

13. ¿Qué actividades lleva a cabo su área?

- Control de Inventario.
- Desarrollo de nuevas opciones en el sistema.
- Soporte a los usuarios.
- Mantenimiento de la red.
- Mantenimiento de la base de datos.
- Mantenimiento de la conexión a internet.
- Control del consumo telefónico.
- Control del uso de las impresoras.
- Control de nuevas adquisiciones tecnológicas por ejemplo protectores electrónicos.
- Correcciones en la base de datos como eliminaciones, cambio de fechas a movimientos, previa autorización del jefe de área y gerencia.
- Esquemas de seguridad mencionados anteriormente.

14. ¿Cuántas personas conforman actualmente el departamento de sistemas?

Dos personas: Jefe de sistemas y asistente de sistemas.

15. ¿Qué funciones tienen?

Jefe de sistemas:

- Administrar los recursos del área.
- Control y mantenimiento de la red y programas que dan servicio a la empresa.
- Gestión de las adquisiciones de equipos.
- Control del mantenimiento a los equipos.
- Implementación de nuevas aplicaciones para mejorar el sistema.
- Elaboración de un plan tecnológico.

Asistente de sistemas:

- Dar soporte técnico a los usuarios
- Realizar los inventarios de los equipos en conjunto con personal de contabilidad.
- Chequear las conexiones de datos con las oficinas regionales.
- Realizar correcciones de datos por errores de usuarios
- Ciertas tareas de programación.

Firma del Entrevistador	Firma del Entrevistado
Ma. Gabriela Hernández	Ing. Milton Parrales

ANEXO 4

DESCRIPCIÓN DEL ENTORNO INFORMÁTICO

Empresa: Agropec S.A.
Area: Sistemas
Nombre: Ing. Milton Parrales
Cargo: Jefe del Departamento

A. Entorno de red

1. ¿Qué tipo de red poseen?
   Red LAN con conexión ethernet 10/100 Base T

2. **¿Qué topología tienen?**
   Estrella

3. **¿Qué medio de transmisión usan?**
   Usamos modems para comunicarnos con la sucursal de Quito

4. **¿Cuentan con servicio de internet?**
   Si No
   Observación:
   El servicio nos lo brinda TELCONET

B. Hardware

1. ¿Con qué equipos cuenta el departamento?
   Existen cuatro servidores:
   - Base de Datos
   - Firewall
   - IAC
   - Acceso de datos para la sucursal de Quito

   Contamos además con tres computadoras.
   Observación:
   La empresa tiene bajo su responsabilidad tres equipos dados por Telconet que son usados para firewall, IAC, acceso de datos para la sucursal de Quito

2. ¿Con qué equipos de comunicación y de red cuenta en el departamento?
   Contamos con un switch, un hub y dos modems.

C. Software

1 ¿Qué lenguaje de programación manejan?
Se manejan:

- SQL Server versión 6.5 para los procesos en la Base de Datos
- Power Builder versión 5.04 para hacer las interfases en caso de mejoras de las aplicaciones

2 ¿Qué sistema aplicativo utilizan?
Utilizamos un sistema administrativo-financiero llamado Spyral

3 ¿Qué módulos tiene el sistema aplicativo?

- Facturación y Cuentas por Cobrar
- Tesorería
- Inventario
- Contabilidad
- Control de Bodegas
- Reportes Estadísticos
- Seguridad

4 ¿Algún modulo ha sido desarrollado por el área?
Si No

4.1. Si la respuesta fue sí, ¿Qué modulo es?
Modulo de seguridad

5 ¿Qué modulo ha sido modificado por su área?
Todos menos el modulo de contabilidad porque no hay las fuentes

6 ¿Qué software básico y utilitarios que poseen?
Contamos con:

- Sistemas Operativos:
  - Windows 95, 98, ME, XP, NT
  - LINUX

- Utilitarios:
  - Office 97
  - Outlook Express
  - Mira scan

- Epson scan
- Microsoft SQL Server 6.5
- Acrobat reader
- CCT (software de control de consumo telefónico)
- Nero
- Antivirus: AVG, Norton 2005, Antivid

Firma del Entrevistador	Firma del Entrevistado
Ma. Gabriela Hernández	Ing. Milton Parrales

ANEXO 5

EVALUACIÓN SEGURIDAD FÍSICA DEPARTAMENTO DE SISTEMAS

Empresa: Agropec S.A.

Persona entrevistada: Ing. Milton Parrales (Dato ficticio)
Cargo: Jefe del departamento

1. **¿Existe un manual documentado de políticas y procedimientos de seguridad física?**
   Si ( ) **No** (X)

2. **¿Existe uno de estos métodos para controlar el acceso a personas ajenas a la organización?**

	Si	**No**
• **Guardias de seguridad**	(X)	( )
• **Detectores de Metales**	( )	(X)
• **Sistemas Biométricos**	( )	(X)
• **Seguridad con Animales**	( )	(X)
• **Protección Electrónica**	( )	(X)

3. **¿Con el método anterior cuál es el control que se lleva?**
   Al ingresar a garita se solicita la cedula a la persona y se solicita autorización para su entrada al empleado que busca esta persona.

4. **¿Existe uno de estos métodos para controlar el acceso a personas ajenas al área?**

	Si	**No**
• **Puerta con cerradura**	(X)	( )
• **Puerta de combinación**	( )	(X)
• **Puerta electrónica**	( )	(X)
• **Puertas sensoriales**	( )	(X)
• **Registros de entrada**	( )	(X)
• **Videocámaras**	( )	(X)
• **Escolta controladora para el acceso de visitantes**	( )	(X)
• **Puertas dobles**	( )	(X)
• **Alarmas**	( )	(X)

5. **¿El personal de la organización cuenta con alguna identificación que los diferencie de los visitantes?**
   Si ( ) **No (X)**

6. **¿El departamento está ubicado en un lugar de alto tráfico de personas?**
   Si (X) **No** ( )

7. **¿El departamento mantiene sus puertas cerradas con seguro?**
   Si (X) **No** ( )

   Observación:
   Solo cuando no hay nadie en el departamento.

8. **¿Las ventanas y puertas del departamento cuentan con protección que eviten el fácil acceso?**
   Si ( ) **No** (X)

   Observación:
   Solo cerradura de la puerta

9. **¿El departamento esta alejado de almacenes de materiales peligrosos?**
   Si (X) **No** ( )

10. **¿Es lo suficiente el espacio físico del departamento para el equipo y que el personal realice sus funciones?**
    Si ( ) **No** (X)

    Observación:
    Falta área para reparar los equipos.

11. **¿Está prohibido comer, fumar y beber dentro del departamento para evitar daños en los equipos?**
    Si (X) **No** ( )

12. **¿Existe un inventario actualizado de los equipos donde se detalle su ubicación y la persona responsable del mismo?**
    Si(X) **No** ( )

13. **¿Los equipos permanecen libres de comida, limpios, sin cenizas, clips, entre otras cosas?**
    Si (x) **No** ( )

14. **¿Los equipos son protegidos con cubiertas plásticas o de otro material?**
    Si ( ) **No** (X)

15. **¿Los equipos inactivos en las áreas públicas están configurados para despejar la pantalla o apagarse automáticamente luego de un determinado período de inactividad?**

Si **No** (X)

16. **¿Posee el departamento aire acondicionado?**
    Si (X) **No** ( )

17. **¿Los equipos trabajan bajo la temperatura y humedad que recomienda el proveedor?**
    Si (X) **No** ( )
    Observación:
    En lo posible se trata de seguir las recomendaciones del proveedor.

18. **¿Se cuenta con algún equipo de ventilación de respaldo en caso de que el principal falle?**
    Si **No** (X)

19. **¿Qué medidas emplean para proteger a los equipos de fallas eléctricas?**

	Si	**No**
• **Reguladores**	(X)	( )
• **Sistema de energía no interrumpido (UPS)**	(X)	( )
• **Switch de emergencia**	(X)	( )
• **Protecciones generales (fuentes de energía alterna)**	( )	(X)

20. **¿Se revisan regularmente estos equipos de suministro de energía?**
    Si ( ) **No** (X)

21. **¿Los cables de red y de energía están protegidos?**
    Si ( ) **No** (X)
22. **¿Se tienen conectados a los contactos de los equipos otros equipos electrónicos?**
    Si (X) **No** ( )
    Observación:
    Solo ciertos usuarios tienen radios y celulares conectados en los contactos de los equipos.

23. **¿Los equipos reciben mantenimiento?**
    Si (X) **No** ( )

24. **¿El mantenimiento a los equipos es realizado por:**
    Compañía externa (X) **Personal de sistemas** ( )

25. **¿Es supervisado el tipo de trabajo realizado por los técnicos sobre los equipos durante el período de mantenimiento?**
    Si (X) **No** ( )

26. **¿Qué tipo de mantenimiento reciben los equipos?**
    Preventivo y correctivo

27. **¿El intervalo de tiempo en que reciben mantenimiento los equipos es el recomendado por el proveedor?**
    Si ( ) **No** (X)
    Observación:
    Trimestralmente reciben mantenimiento excepto los equipos en garantía que son propiedad de TELCONET.

28. **¿Existe un registro de cada mantenimiento realizado a los equipos?**
    Si (X) **No** ( )
    Observación:
    Estos registros se llevan en mail y en un archivo en Excel.

29. **¿Se dispone de equipos de respaldo que puedan utilizarse en caso de contingencias?**
    Si ( ) **No** (X)

30. **¿Existe un registro de los cambios de partes efectuados sobre los equipos?**
    Si (X) **No** ( )
    Observación:
    Toda bitácora de control se lo lleva en mail y en un archivo en Excel.

31. **¿Existe un registro de las fallas que son reportadas por usuarios de los equipos?**
    Si (X) **No** ( )
    Observación:
    Estos registros se llevan en mail y en un archivo en Excel; son actualizados semanalmente.

32. **¿Se les da el respectivo seguimiento a estas fallas?**
    Si (X) **No** ( )

33. **¿Existe un registro de los equipos, software o información que entran y salen de la empresa?**
    Si (X) **No** ( )
    Observación:
    Estos registros se llevan en mail y en un archivo en Excel.

34. **¿Quién da la autorización para estos permisos?**
El jefe de sistemas y el gerente administrativo

35. **¿Cuál es el procedimiento para recibir esta autorización?**
La persona solicitante deberá presentar el requerimiento escrito dirigido a las personas encargadas de dar esta autorización

36. **¿Existen procedimientos para dar de baja los equipos?**
Si ( ) **No** (X)

37. **¿Son destruidos físicamente los dispositivos de almacenamiento sensible (CD`s, disquete) que ya no serán utilizados?**
Si (X) **No** ( )

38. **¿En el caso de ser otra vez utilizados estos dispositivos de almacenamiento, se aseguran de que sean correctamente borrados o formateados?**
Si (X) **No** ( )

39. **¿Los discos duros antes de ser eliminados u otra vez usados, se comprueba que hayan sido borrados?**
Si (X) **No** ( )

40. **¿Se realiza una revisión completa a discos duros de equipos dañados para verificar si deberían ser destruidos o reparados?**
Si (X) **No** ( )

41. **¿Se han tomado medidas para minimizar las posibilidades de fuego como:**

	Si	**No**
• **Evitando artículos inflamables en el departamento**	( )	(X)
• **Prohibiendo fumar a los empleados dentro del departamento**	(X)	( )
• **Vigilando y manteniendo el sistema Eléctrico**	( )	(X)

42. **¿Existen alarmas contra incendios?**
Si ( ) **No** (X)

Si existen, ¿se prueban estas alarmas periódicamente?
Si ( ) **No** ( )

43. **¿El personal está capacitado para actuar en caso de emergencias como un incendio?**
    Si (X) **No** ( )

44. **¿Existen extintores dentro del departamento de sistemas?**
    Si ( ) **No** (X)

45. **¿Existen extintores en la organización?**
    Si (X) **No** ( )

46. **¿Estos extintores son:**
    Automáticos ( ) **Manuales** (X)

47. **¿El extintor es cargado periódicamente?**
    Si (X) **No** ( )

48. **¿El personal está capacitado en el uso de los extintores?**
    Si ( ) **No** (X)
    Observación:
    Solo cierto personal está capacitado en el manejo de extintores.

49. **¿Los extintores están ubicados en un lugar visible y accesible?**
    Si ( ) **No** (X)

50. **¿Se tienen identificadas y señaladas las salidas de emergencia?**
    Si ( ) **No** (X)

51. **¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta?**
    Si (X) **No** ( )

52. **¿Existen respaldos o backups de los archivos en dispositivos externos (CD`s, medios magnéticos, entre otros)?**
    Si (X) **No** ( )

53. **¿Cada cuánto tiempo se hacen respaldos o backups de la información?**
    Mensualmente se realizan respaldos de la Base de datos en CD´s y semanalmente en el disco duro.

54. **¿Se almacenan los backups de la empresa en cajas de seguridad?**
    Si ( ) **No** (X)

55. **¿Existen respaldos de los archivos (programas fuentes, objetos y datos) fuera de la empresa?**
Si ( ) **No** (X)

56. **¿Quién es el responsable de los mismos?**
El jefe de sistemas es el responsable, quién se los lleva a su domicilio en un porta CD.

57. **En caso de que existan respaldos fuera de la empresa, ¿Estos se pueden recuperar en un tiempo tal que no interrumpa las operaciones normales de la empresa?**
Si ( ) **No** ( )

58. **¿Existen registros de los backups?**
Si ( ) **No** (X)

59. **¿Están etiquetados los backups de acuerdo a su contenido?**
Si (X) **No** ( )

60. **¿Existe algún control o bloqueo para las impresoras cuando no son utilizadas?**
Si ( ) **No** (X)

61. **¿Existe algún control para el fax?**
Si ( ) **No** (X)
Observación:
Dentro del área de sistemas no hay fax y no se tiene control para el fax que se encuentra en el área administrativa.

62. **¿Existe alguna clave en las copiadoras que impida el acceso al personal ajeno de la empresa o a quienes cuya función les es innecesario el uso de este equipo?**
Si ( ) **No** (X)

63. **¿Es inmediatamente retirada la impresión que el usuario necesita de las impresoras?**
Si ( ) **No** (X)

64. **¿El equipo está cubierto por el seguro?**
Si (X) **No** ( )

65. **¿Los requisitos del seguro son satisfactorios para la empresa?**
Si (X) **No** ( )

66. **¿Alguno de los servicios del departamento es manejado por una compañía o contratista externo (terceros)?**
Si (X) **No** ( )
Observación:
Mantenimiento de equipos de computación.

Firma del Entrevistador	Firma del Entrevistado
Ma. Gabriela Hernández	Ing. Milton Parrales

ANEXO 6

EVALUACIÓN SEGURIDAD FÍSICA
DEPARTAMENTO DE SISTEMAS

Empresa: Agropec S.A.
Persona entrevistada: Camilo Reyes (Dato ficticio)
Cargo: Asistente de sistemas

67. **¿Existe un manual documentado de políticas y procedimientos de seguridad física?**
Si ( ) **No** (X)

68. **¿Existe uno de estos métodos para controlar el acceso a personas ajenas a la organización?**

	Si	**No**
• **Guardias de seguridad**	(X)	( )
• **Detectores de Metales**	( )	(X)
• **Sistemas Biométricos**	( )	(X)
• **Seguridad con Animales**	( )	(X)
• **Protección Electrónica**	( )	(X)

69. **¿Con el método anterior cuál es el control que se lleva?**
Para que un ajeno a la empresa ingrese el guardia solicita la cedula de está persona y la anuncia con el empleado al cual busca y este da el permiso para que ingrese.

70. **¿Existe uno de estos métodos para controlar el acceso a personas ajenas al área?**

	Si	**No**
• **Puerta con cerradura**	(X)	( )
• **Puerta de combinación**	( )	(X)
• **Puerta electrónica**	( )	(X)
• **Puertas sensoriales**	( )	(X)
• **Registros de entrada**	( )	(X)
• **Videocámaras**	( )	(X)
• **Escolta controladora para el acceso de visitantes**	( )	(X)
• **Puertas dobles**	( )	(X)
• **Alarmas**	( )	(X)

71. **¿El personal de la organización cuenta con alguna identificación que los diferencie de los visitantes?**
Si ( ) **No** (X)

72. **¿El departamento está ubicado en un lugar de alto tráfico de personas?**
Si (X) **No** ( )

73. **¿El departamento mantiene sus puertas cerradas con seguro?**
Si ( ) **No** (X)
Observación:
Solo cuando no hay nadie en el departamento.

74. **¿Las ventanas y puertas del departamento cuentan con protección que eviten el fácil acceso?**
Si ( ) **No** (X)

Observación:
Solo cerradura de la puerta

75. **¿El departamento esta alejado de almacenes de materiales peligrosos?**
    Si (X) **No** ( )

76. **¿Es lo suficiente el espacio físico del departamento para el equipo y que el personal realice sus funciones?**
    Si ( ) **No** (X)

77. **¿Está prohibido comer, fumar y beber dentro del departamento para evitar daños en los equipos?**
    Si (X) **No** ( )

78. **¿Existe un inventario actualizado de los equipos donde se detalle su ubicación y la persona responsable del mismo?**
    Si(X) **No** ( )

79. **¿Los equipos permanecen libres de comida, limpios, sin cenizas, clips, entre otras cosas?**
    Si ( ) **No** (X)

80. **¿Los equipos son protegidos con cubiertas plásticas o de otro material?**
    Si ( ) **No** (X)

81. **¿Los equipos inactivos en las áreas públicas están configurados para despejar la pantalla o apagarse automáticamente luego de un determinado período de inactividad?**
    Si(X) **No** ( )
82. **¿Posee el departamento aire acondicionado?**
    Si (X) **No** ( )

83. **¿Los equipos trabajan bajo la temperatura y humedad que recomienda el proveedor?**
    Si (X) **No** ( )

84. **¿Se cuenta con algún equipo de ventilación de respaldo en caso de que el principal falle?**
    Si **No** (X)

85. **¿Qué medidas emplean para proteger a los equipos de fallas eléctricas?**

	Si	No
• **Reguladores**	(X)	( )
• **Sistema de energía no interrumpido (UPS)**	(X)	( )
• **Switch de emergencia**	(X)	( )
• **Protecciones generales (fuentes de energía alterna)**	( )	(X)

86. ¿Se revisan regularmente estos equipos de suministro de energía?
Si ( ) **No** (X)

87. ¿Los cables de red y de energía están protegidos?
Si ( ) **No** (X)

88. ¿Se tienen conectados a los contactos de los equipos otros equipos electrónicos?
Si (X) **No** ( )

89. ¿Los equipos reciben mantenimiento?
Si (X) **No** ( )

90. ¿El mantenimiento a los equipos es realizado por:
Compañía externa (X) **Personal de sistemas** ( )

91. ¿Es supervisado el tipo de trabajo realizado por los técnicos sobre los equipos durante el período de mantenimiento?
Si (X) **No** ( )

92. ¿Qué tipo de mantenimiento reciben los equipos?
Preventivo y correctivo

93. ¿El intervalo de tiempo en que reciben mantenimiento los equipos es el recomendado por el proveedor?
Si ( ) **No** (X)

94. ¿Existe un registro de cada mantenimiento realizado a los equipos?
Si (X) **No** ( )

95. ¿Se dispone de equipos de respaldo que puedan utilizarse en caso de contingencias?
Si ( ) **No** (X)

96. ¿Existe un registro de los cambios de partes efectuados sobre los equipos?

Si (X) **No** ( )

97. **¿Existe un registro de las fallas que son reportadas por usuarios de los equipos?**
    Si (X) **No** ( )

98. **¿Se les da el respectivo seguimiento a estas fallas?**
    Si (X) **No** ( )

99. **¿Existe un registro de los equipos, software o información que entran y salen de la empresa?**
    Si (X) **No** ( )

100. **¿Quién da la autorización para estos permisos?**
    El jefe de sistemas y el jefe de recursos humanos o el gerente administrativo

101. **¿Cuál es el procedimiento para recibir esta autorización?**
    Se crea un aviso de salida, se lo hace firmar por el jefe de sistemas y por la persona solicitante, después se pide la firma del gerente financiero administrativo o jefe de recursos humanos y finalmente se saca una copia de este permiso y se la entrega al guardia de la garita.

102. **¿Existen procedimientos para dar de baja los equipos?**
    Si (X) **No** ( )

103. **¿Son destruidos físicamente los dispositivos de almacenamiento sensible (CD`s, disquete) que ya no serán utilizados?**
    Si ( ) **No** (X)

104. **¿En el caso de ser otra vez utilizados estos dispositivos de almacenamiento, se aseguran de que sean correctamente borrados o formateados?**
    Si (X) **No** ( )

105. **¿Los discos duros antes de ser eliminados u otra vez usados, se comprueba que hayan sido borrados?**
    Si (X) **No** ( )

106. **¿Se realiza una revisión completa a discos duros de equipos dañados para verificar si deberían ser destruidos o reparados?**
    Si (X) **No** ( )

107. **¿Se han tomado medidas para minimizar las posibilidades de fuego como:**

	Si	No
• **Evitando artículos inflamables en el departamento**	(X)	( )
• **Prohibiendo fumar a los empleados dentro del departamento**	(X)	( )
• **Vigilando y manteniendo el sistema Eléctrico**	( )	(X)

108. ¿Existen alarmas contra incendios?
Si ( ) **No** (X)

Si existen, ¿se prueban estas alarmas periódicamente?
Si ( ) **No** ( )

109. ¿El personal está capacitado para actuar en caso de emergencias como un incendio?
Si (X) **No** ( )

110. ¿Existen extintores dentro del departamento de sistemas?
Si ( ) **No** (X)

111. ¿Existen extintores en la organización?
Si (X) **No** ( )

112. ¿Estos extintores son:
Automáticos ( ) **Manuales** (X)

113. ¿El extintor es cargado periódicamente?
Si (X) **No** ( )

114. ¿El personal está capacitado en el uso de los extintores?
Si (X) **No** ( )

115. ¿Los extintores están ubicados en un lugar visible y accesible?
Si (X) **No** ( )

116. ¿Se tienen identificadas y señaladas las salidas de emergencia?
Si ( ) **No** (X)

117. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta?
Si ( ) **No** (X)

118. ¿Existen respaldos o backups de los archivos en dispositivos externos (CD`s, medios magnéticos, entre otros)?
Si (X) **No** ( )

119. ¿Cada cuánto tiempo se hacen respaldos o backups de la información?
Diariamente.

120. ¿Se almacenan los backups de la empresa en cajas de seguridad?
Si ( ) **No** (X)

121. ¿Existen respaldos de los archivos (programas fuentes, objetos y datos) fuera de la empresa?
Si ( ) **No** (X)

122. ¿Quién es el responsable de los backups?
El jefe de sistemas es el responsable.

123. En caso de que existan respaldos fuera de la empresa, ¿Estos se pueden recuperar en un tiempo tal que no interrumpa las operaciones normales de la empresa?
Si ( ) **No** ( )

124. ¿Existen registros de los backups?
Si (X) **No** ( )

125. ¿Están etiquetados los backups de acuerdo a su contenido?
Si ( ) **No** (X)

126. ¿Existe algún control o bloqueo para las impresoras cuando no son utilizadas?
Si ( ) **No** (X)

127. ¿Existe algún control para el fax?
Si ( ) **No** (X)

128. ¿Existe alguna clave en las copiadoras que impida el acceso al personal ajeno de la empresa o a quienes cuya función les es innecesario el uso de este equipo?
Si (X) **No** ( )

129. ¿Es inmediatamente retirada la impresión que el usuario necesita de las impresoras?
Si (X) **No** ( )

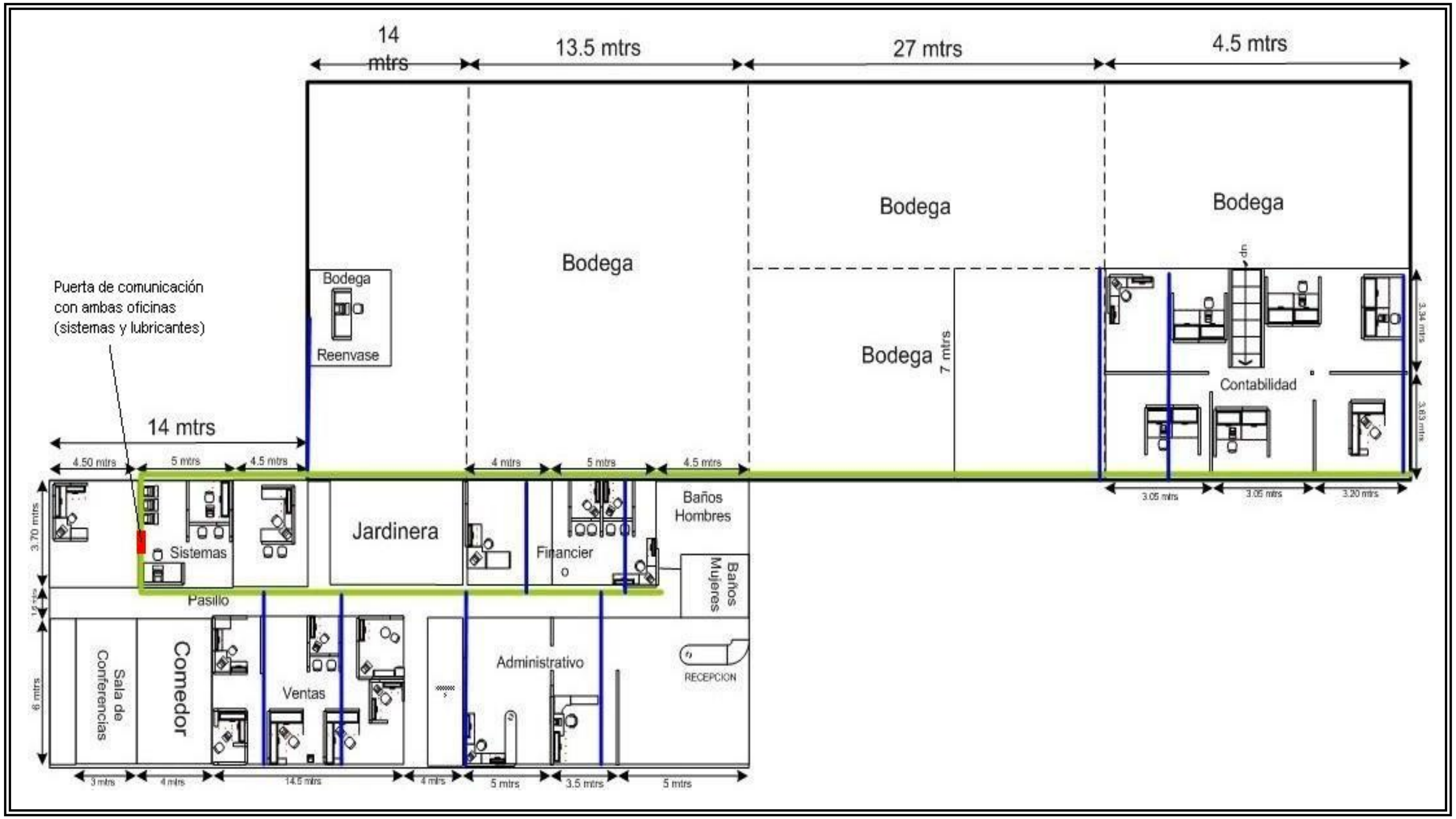
130. ¿El equipo está cubierto por el seguro?
Si (X) **No** ( )

131. ¿Los requisitos del seguro son satisfactorios para la empresa?
Si (X) **No** ( )

132. ¿Alguno de los servicios del departamento es manejado por una compañía o contratista externo (terceros)?
Si (X) **No** ( )

Firma del Entrevistador Ma. Gabriela Hernández	Firma del Entrevistado Camilo Reyes

ANEXO 7
PLANO FÍSICO DE LA EMPRESA AGROPEC S.A.



ANEXO 8

CONSTATACIÓN FÍSICA DEL INVENTARIO DE COMPUTADORAS

Nº	UBICACIÓN			Procesador	Sistema Operativo	Observación
	Área	Departamento	Encargado			
1	Financiera y Administrativa	Gerencia	Gerente General	Centrino	Windows XP Profesional	Sin novedad
2		Financiero	Recepción	Pentium II	Windows 95	Sin novedad
3		Financiero	Gerente Financiero	Pentium III	Windows XP Home Edición	Sin novedad
4		Financiero	Asistente Financiero	Pentium III	Windows ME	Sin novedad
5		Compras e Importaciones	Jefe de Compras e Importaciones	Pentium IV	Windows ME	Sin novedad

ANEXO 8

(CONTINUACIÓN)

CONSTATACIÓN FÍSICA DEL INVENTARIO DE COMPUTADORAS

Nº	UBICACIÓN			Procesador	Sistema Operativo	Observación
	Área	Departamento	Encargado			
6	Contabilidad, Legal y Recursos Humanos	Contabilidad	Operador de Inventario	Pentium III	Windows ME	Sin novedad
7		Contabilidad	Auxiliar de Contabilidad	Pentium III	Windows ME	Sin novedad
8		Contabilidad	Asistente de Contabilidad	Pentium III	Windows ME	Sin novedad
9		Contabilidad	Jefe de Contabilidad	Pentium IV	Windows ME	Sin novedad
10		Legal	Jefe de Legal	Pentium MMX	Windows 95	Sin novedad
11		Recursos Humanos	Jefe de Recursos Humanos	Pentium IV	Windows ME	Sin novedad

ANEXO 8

(CONTINUACIÓN)

CONSTATACIÓN FÍSICA DEL INVENTARIO DE COMPUTADORAS

Nº	UBICACIÓN			Procesador	Sistema Operativo	Observación
	Área	Departamento	Encargado			
12	Bodega	Bodega	Jefe de Bodega	Pentium III	Windows 98	Sin novedad
13	Reenvase	Reenvase	Jefe de Reenvase	Pentium III	Windows ME	Sin novedad
14	Ventas	Ventas	Asistente de Ventas	Pentium III	Windows 98	Sin novedad
15		Ventas	Asistente de Ventas	Pentium III	Windows ME	Sin novedad
16		Tesorería	Tesorera	Pentium III	Windows ME	Sin novedad
17		Cobranzas	Jefe de Crédito y Cobranzas	Pentium IV	Windows ME	Sin novedad
18		Cobranzas	Asistente de Crédito y Cobranzas	Pentium IV	Windows ME	Sin novedad

ANEXO 8

(CONTINUACIÓN)

CONSTATACIÓN FÍSICA DEL INVENTARIO DE COMPUTADORAS

Nº	UBICACIÓN			Procesador	Sistema Operativo	Observación
	Área	Departamento	Encargado			
19		Cobranzas	Asistente de Crédito y Cobranzas	Pentium III	Windows ME	Sin novedad
20		Ventas	Gerente Ventas/Mercadeo	Pentium III	Windows XP Home Edición	Sin novedad
21		Técnico	Asistente Técnico	Pentium IV	Windows ME	Sin novedad
22	Sistemas	Sistemas	Jefe de Sistemas	Pentium III	Windows ME	Sin novedad
23		Sistemas	Programador de Sistemas	Pentium III	Windows ME	Puesto Vacante
24		Sistemas	Asistente de Sistemas	Pentium III	Windows ME	Sin novedad

ANEXO 8
(CONTINUACIÓN)

CONSTATACIÓN FÍSICA DEL INVENTARIO DE COMPUTADORAS

Nº	UBICACIÓN			Procesador	Sistema Operativo	Observación
	Área	Departamento	Encargado			
25		Sistemas	Jefe de Sistemas	Pentium III	Linux	Propiedad de Telconet
26		Sistemas	Jefe de Sistemas	Pentium III	Linux	Propiedad de Telconet
27		Sistemas	Jefe de Sistemas	Pentium III	Linux	Propiedad de Telconet
28		Sistemas	Jefe de Sistemas	Pentium IV	Windows NT	Servidor de Desarrollo
29	Lubricantes	Lubricantes	Jefe de Sistemas	Pentium III	Windows NT	Ubicación del Servidor de producción: La oficina de lubricantes se conecta a la oficina de sistemas por una puerta interna. El servidor está expuesto a la manipulación de cualquier individuo que accede a la misma ya que no tiene ningún tipo de seguridad.

ANEXO 9

CONSTATACIÓN FÍSICA DEL EQUIPO DE COMUNICACIÓN Y RED

Nº	EQUIPO	VELOCIDAD / PUERTO	UBICACIÓN	OBSERVACIÓN
1	Switch	10/100 base T	Dep. de sistemas	Sin novedad
2	HUB	10 base T	Dep. de ventas	Sin novedad
3	HUB	10 Base T	Dep. legal	Sin novedad
4	HUB	50base T	Junto a la central telefónica	Sin novedad
5	HUB	50base T	Dep. de sistemas	Sin novedad
6	MODEM	56kps	Dep. de sistemas	Sin novedad
7	MODEM	56kps	Sucursal centro	Sin novedad
8	MODEM	56kps	Dep. de sistemas	Sin novedad

ANEXO 10

CONSTATACIÓN FÍSICA DEL INVENTARIO DE IMPRESORAS

Nº	UBICACIÓN		Cantidad	Tipo	OBSERVACIÓN
	Área	Departamento			
1	Financiera y Administrativa	Gerencia	1	Inyección	Sin novedad
2		Financiero	1	Laser	Sin novedad
3	Contabilidad, Recursos Humanos	Contabilidad	1	Matricial	Sin novedad
4		Contabilidad	1	Laser	Sin novedad
5		Recursos Humanos	1	Matricial	Sin novedad
6	Reenvase	Reenvase	1	Térmica	Sin novedad
7	Ventas	Ventas	1	Inyección	Sin novedad
8		Ventas	1	Laser	Sin novedad
9		Ventas	1	Matricial	Sin novedad
10		Tesorería	1	Matricial	Sin novedad
11		Técnico	1	Inyección	Sin novedad

ANEXO 11

CONSTATACIÓN FÍSICA DEL INVENTARIO DE OTROS EQUIPOS

Nº	Ubicación		Cantidad	Hardware	OBSERVACIÓN
	Área	Departamento			
1	Sistemas	Sistemas	1	CD-Rewriter	Sin novedad
2		Sistemas	1	Disk Optico	Sin novedad
3	Financiero y Administrativo	Gerencia General	1	Scaner	Sin novedad
4		Compras e Importaciones	1	Scaner	Sin novedad

ANEXO 12

CONTRATO DE MANTENIMIENTO DE LA EMPRESA AGROPEC S.A.

INFOEXPRESS
Ventas e Instalación de Tecnología
www.iecompu.com

CONTRATO DE MANTENIMIENTO

En la ciudad de Guayaquil, al 1er día del mes de Abril, del Dos Mil Cuatro, se celebra el presente contrato entre el en calidad de **Vicepresidente Ejecutivo** de AGROPEC S.A y la en calidad de **Gerente de Ventas y Mantenimiento** de **INFOEXPRESS,** a quienes más adelante se les denominará contratante y contratista respectivamente, convienen en firmar este documento al tenor de las siguientes cláusulas:

PRIMERA: El contratista se compromete y se obliga a efectuar el servicio de mantenimiento preventivo y correctivo de los siguientes computadores e impresoras:

Guayaquil

29 Computadores
6 Impresoras Matriciales
2 Impresoras Láser
1 Impresora térmica
4 Impresoras de Inyección de Tinta
1 Router Cisco 2500
1 Hub Encore 10 Base T
1 Hub 3Com 50 Base T
1 Transceiver Avia 10 Base T
2 Modem USRobotic 56 Kbps
1 Cd-Writer Backpack
1 Scanner
1 Disk Optico Backpack

SEGUNDA:

El mantenimiento preventivo y correctivo de los equipos según el contrato, se refiere a:

Mantenimiento Preventivo

* Chequeo de computadoras personales mediante software de diagnóstico. * Optimización y configuración de PC. * Limpieza interior y exterior de los equipos. * Depuración de archivos temporales. * Chequeo y pruebas de impresión matricial, tinta y láser. * Inducción al usuario acerca del uso y solución de fallas (instructivos). * Lubricación completa de piezas móviles de impresoras.

Mantenimiento Correctivo

* Revisión, detección y solución de fallas mecánicas y eléctricas (cambio y reparación de piezas) en los equipos. * Recuperación de partes y piezas de pc´s. * Recuperación de partes y piezas de impresoras matriciales, inyección y láser. * Traslado de equipos PC por reemplazo o desincorporación.

DIRECCIÓN: Av. Juan Tanca Marengo Km 6.5 (Frente del colegio Americano)
TELEFONOS: 593 (4) 2 258496 - 2255106 TELEFAX: 2 - 258496
Web: www.iecompu.com

(CONTINUACIÓN)

CONTRATO DE MANTENIMIENTO DE LA EMPRESA AGROPEC S.A.

INFOEXPRESS
Ventas e Instalación de Tecnología
www.lecompu.com

TERCERA: Los trabajos de mantenimiento preventivo se realizarán tres veces en el año (frecuencia cuatrimestral), además de establecer un sistema de llamada de soporte inmediato por evento para el mantenimiento correctivo de los equipos que forman parte del ya mencionado inventario.

El mantenimiento requerido por los equipos adquiridos a INFOEXPRESS en el lapso de vigencia del contrato, no tendrá costo alguno.

Los trabajos por mantenimiento correctivo serán realizados en el laboratorio técnico del contratista, las partes y más repuestos utilizados en el mantenimiento correctivo serán facturados mas no la mano de obra.

CUARTA: INFOEXPRESS no está obligado a restablecer o instalar aplicaciones o programas que no hayan venido originalmente en las máquinas, así como tampoco configurar dispositivos distintos a los estándares de las máquinas.

QUINTA: El costo de mantenimiento de los antes mencionados equipo de computación es de **U.S. 114,oo (CIENTO CATORCE 00/100 DÓLARES)** Mensuales.

Los gastos que incurran fuera de la ciudad de Guayaquil, tales como: pasajes, viáticos y demás costos necesarios para mantener en buen estado los equipos amparados, correrán por cuenta del contratante.

SEXTA: Este contrato tendrá validez durante doce meses siendo indispensable para cada período firmar un nuevo contrato de mantenimiento.

SÉPTIMA: Las partes aceptan el contenido de todas y cada una de las cláusulas anteriores para lo cual firman el presente contrato en original y copia.

Gerente de Ventas y Mantenimiento
INFOEXPRESS

Vice-Presidente Ejecutivo
AGROPEC S.A.

DIRECCIÓN: Av. Juan Tanca Marengo, Km 6.5 (Frente del colegio Americano)
TELEFONOS: 593 (4) 2 258496 - 2256106 TELEFAX: 2 - 258496
Web: www.lecompu.com

EVALUACIÓN SEGURIDAD LÓGICA
DEPARTAMENTO DE SISTEMAS

Empresa: Agropec S.A.
Persona entrevistada: Ing. Milton Parrales (Dato ficticio)
Cargo: Jefe del departamento

133. ¿Cuentan con una política documentada para la gestión de las claves de acceso?
Si (X) **No ( )**

134. ¿Quién es la persona encargada de administrar las claves?
Jefe de sistemas

135. ¿Como están conformadas las claves de acceso?
Están formadas por el nombre de usuario y una clave secreta.

136. ¿Qué características debe tener el passwords?
Debe tener caracteres alfanuméricos, debe ser mínimo de seis caracteres.

137. ¿Qué método emplean para generar las claves?
Software (X) **Elegida por el usuario ( )**

Observación:
Primero el jefe de sistemas le crea una clave al usuario, donde la identificación será: la inicial del nombre, seguido del apellido y el password se lo asigna. Luego el usuario deberá ingresar al sistema y este le pedirá cambiar el password.

138. ¿Con qué periodicidad se actualizan las claves?
Cada treinta días

139. ¿Son utilizadas técnicas de cifrado para proteger las claves?
Si (X) **No ( )**
Observación:
Se graban las llaves en la base de datos.

140. ¿Se verifica que el empleado tenga autorización de gerencia para el uso del sistema antes de asignarle una clave?
Si (X) **No ( )**
Observación:

Se verifica que tenga autorización del jefe de su área.

141. ¿Las claves se asignan por grupo de usuarios o por cada usuario?
Por usuario

142. ¿Los permisos (lectura, escritura, ejecución, eliminación, todos los anteriores) son asignados de acuerdo a las funciones del usuario?
Si (X) **No** ( )

143. ¿Se lleva un registro de los cambios de privilegios en el sistema actualizados en el caso de que el usuario cambie de función dentro de la organización?
Si ( ) **No** (X)

144. ¿Se bloquea el equipo después de un número limitado de ingresos de claves incorrectas?
Si ( ) **No** (X)

145. ¿Cuánto intentos fallidos permite el sistema antes de bloquear el equipo?
Es indefinido el número de intentos

146. ¿El equipo espera un tiempo para mostrar nuevamente la ventana de ingreso de contraseña?
Si ( ) **No** (X)

147. ¿Existen registros de los intentos de aceptación y rechazo de claves de usuario en el sistema?
Si ( ) **No** (X)

148. ¿Existe un registro que indique la hora, fecha y aplicación que utilizo el usuario?
Si (X) **No** ( )

149. ¿Se realizan seguimientos a los registros de accesos no autorizados, autorizados y fallidos?
Si ( ) **No** (X)

150. ¿Existen registros de errores al ingresar datos por cada aplicación?
Si (X) **No** ( )

151. ¿Es limitado el tiempo de conexión a la red al horario de oficina?

Si ( ) **No** (X)

152. **¿Existen procedimientos para la eliminación de claves?**
Si (X) **No ( )**

153. **¿Se llevan registros de las claves eliminadas?**
Si ( ) **No** (X)

154. **¿Estos procedimientos se realizan inmediatamente que el empleado sea retirado de la organización?**
Si (X) **No ( )**

155. **¿Qué procedimientos siguen en caso de que el usuario se encuentre dentro de alguna de estas condiciones:**
a. Vacaciones o Ausencia temporal
Ninguno
b. Olvido o Revelación de la clave
Se inicializa la clave y se obliga al usuario a cambiarla de inmediato
c. Claves sin usar
Se eliminan

156. **¿Se llevan registros de estos procedimientos?**
Si ( ) **No** (X)

Firma del Entrevistador Ma. Gabriela Hernández	Firma del Entrevistado Ing. Milton Parrales

ANEXO 14

EVALUACIÓN SEGURIDAD LÓGICA

DEPARTAMENTO DE SISTEMAS

Empresa: Agropec S.A.
Persona entrevistada: Camilo Reyes (Dato ficticio)
Cargo: Asistente de sistemas

157. **¿Cuentan con una política documentada para la gestión de las claves de acceso?**
Si (X) **No ( )**

158. **¿Quién es la persona encargada de administrar las claves?**
Jefe de sistemas

159. **¿Como están conformadas las claves de acceso?**
Nombre de usuario y una clave secreta.

160. **¿Qué características debe tener el passwords?**
Tienen caracteres alfanuméricos y mínimo de seis caracteres.

161. **¿Qué método emplean para generar las claves?**
Software (X) **Elegida por el usuario ( )**
Observación:
Se crea la misma del usuario y luego el sistema le pide cambiarla

162. **¿Con qué periodicidad se actualizan las claves?**
Cada vez que se lo programe o que el usuario cambie de puesto de trabajo.

163. **¿Son utilizadas técnicas de cifrado para proteger las claves?**
Si (X) **No ( )**

164. **¿Se verifica que el empleado tenga autorización de gerencia para el uso del sistema antes de asignarle una clave?**
Si (X) **No ( )**

165. **¿Las claves se asignan por grupo de usuarios o por cada usuario?**
Por usuario

166. **¿Los permisos (lectura, escritura, ejecución, eliminación, todos los anteriores) son asignados de acuerdo a las funciones del usuario?**
Si (X) **No** ( )

167. **¿Se lleva un registro de los cambios de privilegios en el sistema actualizados en el caso de que el usuario cambie de función dentro de la organización?**
Si ( ) **No** (X)

168. **¿Se bloquea el equipo después de un número limitado de ingresos de claves incorrectas?**
Si ( ) **No** (X)

169. **¿Cuánto intentos fallidos permite el sistema antes de bloquear el equipo?**
No tiene límite.

170. **¿El equipo espera un tiempo para mostrar nuevamente la ventana de ingreso de contraseña?**
Si ( ) **No** (X)

171. **¿Existen registros de los intentos de aceptación y rechazo de claves de usuario en el sistema?**
Si ( ) **No** (X)

172. **¿Existe un registro que indique la hora, fecha y aplicación que utilizo el usuario?**
Si (X) **No** ( )

173. **¿Se realizan seguimientos a los registros de accesos no autorizados, autorizados y fallidos?**
Si ( ) **No** (X)

174. **¿Existen registros de errores al ingresar datos por cada aplicación?**
Si ( ) **No** (X)

175. **¿Es limitado el tiempo de conexión a la red al horario de oficina?**
Si ( ) **No** (X)

176. **¿Existen procedimientos para la eliminación de claves?**
Si (X) **No** ( )

177. ¿Se llevan registros de las claves eliminadas?
Si ( ) **No** (X)

178. ¿Estos procedimientos se realizan inmediatamente que el empleado sea retirado de la organización?
Si (X) **No ( )**

179. ¿Qué procedimientos siguen en caso de que el usuario se encuentre dentro de alguna de estas condiciones:

a. Vacaciones o Ausencia temporal
Ninguna, se deja su clave y usuario como los dejo.

b. Olvido o Revelación de la clave
Petición por mail de cambio de clave dirigida al jefe de sistemas.

c. Claves sin usar
Se las mantiene hasta eliminarlas.

180. ¿Se llevan registros de estos procedimientos?
Si ( ) **No** (X)

Firma del Entrevistador
Ma. Gabriela Hernández

Firma del Entrevistado
Camilo Reyes

ANEXO 15

EVALUACIÓN SEGURIDAD DEL SISTEMA APLICATIVO
DEPARTAMENTO DE SISTEMAS

Empresa: Agropec S.A.
Persona entrevistada: Ing. Milton Parrales (Dato ficticio)
Cargo: Jefe del departamento

1. **¿Existe un mapa orgánico de los puestos y funciones del departamento que administra el sistema?**
   Si (X) **No** ( )

2. **¿Existe un manual de sistemas y procedimientos para las actividades de la empresa?**
   Si (X) **No** ( )

3. **¿Está documentado?**
   Si (X) **No** ( )

4. **¿Está actualizado?**
   Si ( ) **No** (X)

5. **¿Existe un manual documentado de usuario del sistema?**
   Si (X) **No** ( )
   Observación:
   Está desactualizado

6. **¿Han existido evaluaciones de la seguridad anteriores del sistema?**
   Si ( ) **No** (X)

7. **¿Existe un manual de los procedimientos para la configuración del sistema?**
   Si (X) **No** ( )

8. **¿Está documentado?**
   Si ( ) **No** (X)

9. **¿El diagrama entidad-relación del sistema está debidamente actualizado y documentado?**
   Si ( ) **No** (X)

10. **¿Está documentado el diccionario de datos del sistema?**

Si ( ) **No** (X)

11. **¿Existe un plan para cambios futuros que se vayan a hacer al sistema??**
    Si (X) **No** ( )

12. **Si existe ¿Está documentado?**
    Si (X) **No** ( )

13. **¿Existen manuales de los procedimientos para realizar los cambios en las aplicaciones y generación de reportes del sistema?**
    Si (X) **No** ( )

14. **¿Están documentados?**
    Si ( ) **No** (X)

15. **¿Existen procedimientos para autorizar y aprobar los cambios en el sistema?**
    Si (X) **No** ( )

16. **¿Existen registros de cambios en el sistema con las fechas de vigencia?**
    Si (X) **No** ( )

17. **¿Se documentan estos registros de cambios?**
    Si ( ) **No** (X)

18. **¿Existen cambios recientes en algún modulo del sistema?**
    Si (X) **No** ( )

19. **¿Se realiza un seguimiento de seguridad a está aplicación?**
    Si ( ) **No** (X)

20. **¿Existen registros de los errores que ocurren en el sistema de aplicativo?**
    Si (X) **No** ( )

21. **¿Son documentados?**
    Si ( ) **No** (X)

22. **¿Son revisados periódicamente estos registros de errores?**
    Si (X) **No** ( )

Firma del Entrevistador
Ma. Gabriela Hernández

Firma del Entrevistado
Ing. Milton Parrales

ANEXO 16

EVALUACIÓN SEGURIDAD DEL SISTEMA APLICATIVO

DEPARTAMENTO DE SISTEMAS

Empresa: Agropec S.A.
Persona entrevistada: Camilo Reyes (Dato ficticio)
Cargo: Asistente de sistemas

23. **¿Existe un mapa orgánico de los puestos y funciones del departamento que administra el sistema?**
    Si (X) **No** ( )

24. **¿Existe un manual de sistemas y procedimientos para las actividades de la empresa?**
    Si (X) **No** ( )

25. **¿Está documentado?**
    Si (X) **No** ( )

26. **¿Está actualizado?**
    Si ( ) **No** (X)

27. **¿Existe un manual documentado de usuario del sistema?**
    Si (X) **No** ( )

28. **¿Han existido evaluaciones de la seguridad anteriores del sistema?**
    Si ( ) **No** (X)

29. **¿Existe un manual de los procedimientos para la configuración del sistema?**
    Si (X) **No** ( )

30. **¿Está documentado?**
    Si ( ) **No** (X)

31. **¿El diagrama entidad-relación del sistema está debidamente actualizado y documentado?**
    Si (X) **No** ( )

32. **¿Está documentado el diccionario de datos del sistema?**
    Si ( ) **No** (X)

33. ¿Existe un plan de desarrollo, de mejora o modificación del sistema?
Si (X) **No** ( )

34. Si existe ¿Está documentado?
Si ( ) **No** (X)

35. ¿Existen manuales de los procedimientos para realizar los cambios en las aplicaciones y generación de reportes del sistema?
Si (X) **No** ( )

36. ¿Están documentados?
Si ( ) **No** (X)

37. ¿Existen procedimientos para autorizar y aprobar los cambios en el sistema?
Si ( ) **No** (X)

38. ¿Existen registros de cambios en el sistema con las fechas de vigencia?
Si (X) **No** ( )

39. ¿Se documentan estos registros de cambios?
Si ( ) **No** (X)

40. ¿Existen cambios recientes en algún modulo del sistema?
Si (X) **No** ( )

41. ¿Se realiza un seguimiento de seguridad a está aplicación?
Si ( ) **No** (X)

42. ¿Existen registros de los errores que ocurren en el sistema de aplicativo?
Si (X) **No** ( )

43. ¿Son documentados?
Si ( ) **No** (X)

44. ¿Son revisados periódicamente estos registros de errores?
Si (X) **No** ( )

Firma del Entrevistador	Firma del Entrevistado
Ma. Gabriela Hernández	Camilo Reyes

ANEXO 17

EVALUACIÓN SEGURIDAD EN REDES
DEPARTAMENTO DE SISTEMAS

Empresa: Agropec S.A.
Persona entrevistada: Ing. Milton Parrales (Dato ficticio)

Cargo: Jefe del departamento

181. **¿Existen adecuados y eficaces controles operacionales como por ejemplo: el separar la administración del sistema y de la red?**
Si (X) **No** ( )
Observación:
Hay seguridades a nivel de aplicación y de sistema operativo

FIREWALL

1. **¿Qué controles de acceso tiene el firewall?**
Controles sobre los equipos que tienen acceso a internet

2. **¿Se examinan los servicios de internet que los usuarios necesitan para darles el respectivo acceso?**
Si (X) **No** ( )
Observación:
Los gerentes tienen acceso total y el resto de personal tiene acceso solo a correo electrónico y páginas específicas como bancos, SRI, entre otros

3. **¿Se permiten sólo los servicios que se comprenden o se tiene experiencia, que se pueden proporcionar con seguridad y para los cuales existen una necesidad legítima?**
Si (X) **No** ( )

Observación:
A las páginas de instituciones pública y bancos.

4. **¿Se generan registros de los intentos de accesos no autorizados?**
Si ( ) **No** (X)

5. **¿Es lo suficientemente rápido para que no demore a los usuarios en sus intentos por acceder a la red?**
Si (X) **No** ( )

ANTIVIRUS

1. **¿Existen controles contra el uso de software malicioso (virus)?**
Si (X) **No** ( )

2. **¿Todo el tráfico originado por una red no confiable es chequeada por el antivirus dentro de la organización? Ejemplo: Comprobar si hay virus en el email, los archivos adjuntos del email y en la web?**
   Si (X) **No ( )**
   Observación:
   En ciertos equipos

3. **¿Hay un antivirus instalado en cada equipo (incluidos los servidores) o hay un solo antivirus en toda la red?**
   En cada equipo existen antivirus instalados

4. **¿El software antivirus está instalado en los equipos para que cheque, aislé o remueva cualquier virus de la computadora o medios de almacenamiento?**
   Si (X) **No ( )**

5. **¿Qué procedimiento siguen en el caso de una infección con un virus?**
   Se trata de eliminar el virus, de no lograrse esto, se formatea el disco duro del equipo infectado.

6. **¿El escaneo de las máquinas se realiza por cuenta de cada usuario o lo realiza el encargado de sistemas?**
   Encargado de sistemas.

7. **¿Cada cuánto tiempo se hace un escaneo total de virus en los servidores y en los equipos de los usuarios?**
   Trimestralmente

8. **¿Quién se encarga?**
   Asistente de sistemas.

9. **¿Se hacen chequeos ocasionales para ver si se han actualizado los antivirus?**
   Si (X) **No ( )**

Firma del Entrevistador	Firma del Entrevistado
Ma. Gabriela Hernández	Ing. Milton Parrales

ANEXO 18

EVALUACIÓN SEGURIDAD EN REDES
DEPARTAMENTO DE SISTEMAS

Empresa:	Agropec S.A.
Persona entrevistada:	Camilo Reyes (Dato ficticio)
Cargo:	Asistente de sistemas

182. ¿Existen adecuados y eficaces controles operacionales como por ejemplo: el separar la administración del sistema y de la red?

Si (X) **No** ( )

FIREWALL

1. **¿Qué controles de acceso tiene el firewall?**
   Se tienen controlado el acceso de los usuarios a ciertas páginas.

2. **¿Se examinan los servicios de internet que los usuarios necesitan para darles el respectivo acceso?**
   Si (X) **No** ( )

3. **¿Se permiten sólo los servicios que se comprenden o se tiene experiencia, que se pueden proporcionar con seguridad y para los cuales existen una necesidad legítima?**
   Si (X) **No** ( )

4. **¿Se generan registros de los intentos de accesos no autorizados?**
   Si ( ) **No** (X)

5. **¿Es lo suficientemente rápido para que no demore a los usuarios en sus intentos por acceder a la red?**
   Si ( ) **No** (X)

ANTIVIRUS

1. **¿Existen controles contra el uso de software malicioso (virus)?**
   Si (X) **No** ( )

2. **¿Todo el tráfico originado por una red no confiable es chequeada por el antivirus dentro de la organización? Ejemplo: Comprobar si hay virus en el email, los archivos adjuntos del email y en la web?**
   Si (X) **No** ( )

3. **¿Hay un antivirus instalado en cada equipo (incluidos los servidores) o hay un solo antivirus en toda la red?**
   Hay un antivirus en cada equipo pero no en el servidor.

4. **¿El software antivirus está instalado en los equipos para que cheque, aislé o remueva cualquier virus de la computadora o medios de almacenamiento?**
   Si (X) **No** ( )

5. **¿Qué procedimiento siguen en el caso de una infección con un virus?**

Se reconoce e investiga en internet el virus, se actualiza y ejecuta el antivirus sin conectarse a red y se trata de eliminarlo normalmente y si no es posible se respalda la información y se formatea.

6. **¿El escaneo de las máquinas se realiza por cuenta de cada usuario o lo realiza el encargado de sistemas?**
   El encargado de sistemas.

7. **¿Cada cuánto tiempo se hace un escaneo total de virus en los servidores y en los equipos de los usuarios?**
   Trimestralmente.

8. **¿Quién se encarga?**
   Asistente de sistemas.

9. **¿Se hacen chequeos ocasionales para ver si se han actualizado los antivirus?**
   Si (X) **No** ( )

Firma del Entrevistador	Firma del Entrevistado
Ma. Gabriela Hernández	Camilo Reyes

ANEXO 19

EVALUACIÓN SEGURIDAD EN LOS RECURSOS HUMANOS
DEPARTAMENTO DE RECURSOS HUMANOS

Empresa: Agropec S.A.
Persona Entrevistada: Francisco Murillo (Dato ficticio)
Cargo: Jefe de recursos Humanos

183. **¿Se verifican los antecedentes del posible empleado antes de ser contratado?**
   Si (X) **No** ( )

   Observación:

Los aspirantes normalmente son enviados por la tercerizadora, en la cual los evalúan y verifican los datos, los jefes inmediatos del candidato se encargan de hacer las entrevistas previas y pasan a la Gerencia Financiera que se encarga de aprobar o no al candidato.

184. ¿Existe una cláusula de confidencialidad en el contrato de trabajo para los empleados, especialmente si son postulantes para algún cargo en el departamento de sistemas?

Si ( ) **No** (X)

185. ¿Este contrato es firmado y leído por el empleado antes de que ingrese a laborar en la empresa?

Si (X) **No** ( )

186. ¿Todos los empleados de la organización reciben el entrenamiento apropiado en materia de seguridad de la información y actualizaciones regulares en políticas y procedimientos de la organización?

	Si	**No**
• **Al iniciar su labor en la organización**	(X)	( )
• **Durante su vida laboral en la empresa**	( )	(X)

187. ¿Se evalúa periódicamente el comportamiento del personal, especialmente si estos tienen privilegios dentro de la organización?

Si ( ) **No** (X)

188. ¿Existe una adecuada separación de funciones de los empleados dentro de la organización, especialmente de los que forman el departamento de sistemas?

Si ( ) **No** (X)

189. ¿Existe un adecuado procedimiento para dar de baja a los empleados cuando estos se ausentan definitivamente de la empresa?

Si (X) **No** ( )

Observación:

Existe un control de asistencia y puntualidad, el mismo que es pasado semanalmente a la Gerencia Financiera Administrativa que es la que se encarga de la toma de decisiones.

190. ¿Comunican inmediatamente al departamento de sistemas que dicho empleado no labora más en la empresa para que esta área elimine su clave del sistema y no correr riesgos?

Si (X) **No** ( )

Observación:
Normalmente se lo hace, pero debido a las múltiples ocupaciones en el departamento de RRHH a veces no se pasa esta información por vía escrita, sino que se la hace de manera verbal.

Firma del Entrevistador Ma. Gabriela Hernández	Firma del Entrevistado Francisco Murillo

ANEXO 20

EVALUACIÓN SEGURIDAD EN EL OUTSOURCING DEPARTAMENTO DE SISTEMAS

Empresa: Agropec S.A.
Persona entrevistada: Ing. Milton Parrales (Dato ficticio)
Cargo: Jefe del departamento

191. ¿Se tienen en cuenta los riesgos que implica este tipo de contrato?
Si ( ) **No** (X)

192. ¿El contrato de outsourcing que tienen con la empresa de mantenimiento posee cláusulas que protejan la seguridad de los equipos y de la información de la empresa?
Si ( ) **No** (X)

193. ¿Se asegura de los antecedentes que los terceros (empresa de outsourcing) tienen por su trabajo realizado en otras organizaciones?

Si (X) **No** ( )

194. ¿Existen medidas de control para los empleados de la empresa que ofrece el servicio de mantenimiento?

Si (X) **No** ( )

Observación:

Cuando vienen a realizar el mantenimiento que es cada tres meses los acompaña el asistente de sistemas durante todo el tiempo.

Nota:

Está evaluación se realizó al Jefe del área de Sistemas por ser el encargado de lo que respecta al mantenimiento de los equipos

Firma del Entrevistador Ma. Gabriela Hernández	Firma del Entrevistado Ing. Milton Parrales

ANEXO 21
VULNERABILIDADES QUE DAN ORIGEN A LOS FACTORES DE RIESGO

SISTEMA DE CONTROL
No existen políticas de seguridad.
Falta de revisiones periódicas y control de las cuentas de los usuarios.
Falta de registro de accesos al sistema.
Falta de registro de accesos al área de sistemas.
Falta de separación de las áreas de desarrollo y producción.
Desactualización del manual de usuario del sistema.
Falta de mantenimiento para los equipos.
Inadecuada segregación de funciones.
Falta de medidas contra incendio
No se siguen los tiempos de mantenimiento para los equipos que indica el proveedor.

NIVEL DE SENSIBILIDAD
Mala ubicación del área de sistemas.
Mala ubicación del servidor de producción.

No se bloquea el equipo por ingresar una clave incorrecta.
No hay procedimientos para dar de bajas claves de usuarios por ausencia temporal o definitiva.
No hay un límite de intentos fallidos en el sistema al ingresar una clave errónea.
No se limita el tiempo de conexión a la red.
Falta de separación de las áreas de desarrollo y producción.
No se siguen los tiempos de mantenimiento para los equipos que indica el proveedor.
Falta de seguridad para los respaldos.
Desactualización del manual de usuario del sistema.
Falta de protección en los cables de la red.

COMPLEJIDAD
Mala ubicación de los equipos.
Falta de seguridad para los respaldos.
Mala ubicación del área de sistemas.
Falta de registros de acceso al área de sistemas.
Falta de separación de las áreas de desarrollo y producción.
Desactualización del manual de usuario del sistema.
Falta de restricciones en el horario para ingresar al sistema
No hay un límite de intentos fallidos en el sistema al ingresar una clave errónea.
No se registran los intentos de ingresos a páginas de internet no permitidas.
No se bloquea el equipo por ingresar una clave incorrecta.
No hay procedimientos para dar de bajas claves de usuarios por ausencia temporal o definitiva.
Falta de protección en los cables de la red.
No se siguen los tiempos de mantenimiento para los equipos que indica el proveedor.

ANEXO 21
(CONTINUACIÓN)

VULNERABILIDADES QUE DAN ORIGEN A LOS FACTORES DE RIESGO

MATERIALIDAD
No existe un manual de políticas y procedimientos de seguridad.
Falta de registros de acceso al área de sistemas.
Mala ubicación del área de sistemas.
Mala ubicación del servidor de producción.
Falta de protección especial para los equipos.
Falta de medidas contra incendio.
Falta de seguridad para los respaldos.
Falta de restricciones en el horario para ingresar al sistema.
No se lleva a cabo ninguna revisión periódica ni control sobre el buen funcionamiento de las cuentas de los usuarios, ni sobre los permisos que tienen asignados.
No hay un límite de intentos fallidos en el sistema al ingresar una clave errónea.

No se registran los intentos de ingresos a páginas de internet no permitidas.
Falta de verificación de los antecedentes de los empleados de la empresa por parte de Recursos Humanos.
Falta de comunicación formal inmediata entre el departamentos de Recursos Humanos y Sistemas cuando se ausenta un empleado temporalmente o definitivamente.
Falta de equipos de respaldo en caso de contingencia.
Falta de separación de las áreas de desarrollo y producción.

IMAGEN
Falta de evaluaciones a la seguridad informática de la empresa.
No existe un manual de políticas y procedimientos de seguridad.
Falta de restricciones en el horario para ingresar al sistema.
Falta de verificación de antecedentes de los empleados.
Falta de seguridad para los respaldos.
Falta de equipos de respaldo en caso de contingencia.
Falta de separación de las áreas de desarrollo y producción.
Desactualización del manual de usuario del sistema.

AUDITORÍAS ANTERIORES
No se han realizado anteriormente auditorias a la seguridad informática.

PLAN DE CONTIGENCIAS
No cuentan con un Plan de Contingencias.

ANEXO 22

FACTORES DE RIESGO

FACTOR DE RIESGO	PARÁMETROS O INDICADORES
Sistema de Control	Refleja la opinión del sistema de control interno en el área de informática. * Políticas de seguridad informática. * Nivel de cumplimiento de normas y procedimientos de seguridad.
Nivel de Sensibilidad	Grado de sensibilidad de los sistemas y equipos considerados recursos informáticos en cuanto a su importancia para que la empresa logre sus objetivos * Sensibilidad de los equipos y del sistema a daños y fallas.

Complejidad	Evalúa el nivel potencial de daños que se pueden producir como consecuencia de las variables interactuantes. * Mantenimiento del sistema y equipos. * Entorno funcional y tecnológico. * Ubicación de equipos. * Respaldos de la información. * Ubicación y protección del Departamento. * Accesos al sistema. * Accesos en Internet.
Materialidad	Refleja la importancia de los sistemas y equipos en términos monetarios y que es vital para la empresa. A mayor materialidad, mayor riesgo
Imagen	Refleja el nivel de seguridad que maneja el área informática. La seguridad permite que la información confidencial como datos de clientes y de la propia empresa no sea divulgada, alterada ni mal empleada.
Auditorias previas	Específica el último periodo auditado indicando el grado de monitoreo y evaluación aplicado
Respuesta ante fallas (Plan de Contingencia)	Posibilidad de recuperación de los procesos y equipos de la organización ante contingencias * Existencia de un plan.

ANEXO 23

PONDERACIÓN DE FACTORES DE RIESGO

Las ponderaciones de los factores de riesgo fueron asignados de acuerdo al criterio de importancia que los integrantes del área de sistemas dan a cada factor de riesgo. Considerando que la ponderación total de importancia es del 100%.

Nº	FACTOR DE RIESGO	POND.
1	Sistema de Control	12%
2	Nivel de Sensibilidad	12%
3	Complejidad	15%

4	Materialidad	15%
5	Imagen	30%
6	Tiempo de realización de Auditorías previas	8%
7	Respuesta ante fallas (Plan de Contingencia)	8%
	TOTAL	100%

ANEXO 24

METRICAS DE FACTORES DE RIESGO

Escala de riesgos: 1 (Bajo**); 2 (**Medio Bajo**); 3 (**Medio Alto**); 4 (**Alto**)**

Nº	Factor de Riesgo	Métricas	Puntaje
1	Sistema de control	Esquema de control implantado y documentado	1
		Procedimientos de control descritos	2
		No existe esquema de control	3
2	Nivel de sensibilidad	Ningún impacto de daños y fallas	1
		Bajo impacto de daños y fallas	2
		Alto impacto de daños y fallas	3

3	Complejidad	Simple Moderadamente complejo Complejo	1 2 3
4	Materialidad	Materialidad Baja Materialidad Media Materialidad Alta	1 2 3
5	Imagen	Seguridad Baja Seguridad Media Seguridad Alta	1 2 3
6	Tiempo de realización de Auditorias previas	Hace 1 año Entre más de 1 y 2 años Hace más de 2 años No se ejecutaron auditorias	1 2 3 4
7	Respuesta ante fallas (Plan de contingencia)	Existe plan de contingencia No existe plan de contingencia	1 2

ANEXO 25

MATRIZ DESCRIPTIVA

DE

FACTORES DE RIESGO Y VALORACIONES ASOCIADOS A LOS RECURSOS INFORMÁTICOS

Cada recurso informático tiene un puntaje asignado de acuerdo a los criterios en la tabla de métricas de factores de riesgos.

No.	Recursos Informáticos	Sistema de Control	Nivel de Sensibilidad	Complejidad	Materialidad	Imagen	Tiempo de realización de Auditorias previas	Respuesta ante fallas (Planes de contingencia)
1	Servidor de Aplicaciones	3	3	3	3	1	4	1
2	Sistema Contable (software)	2	3	3	3	1	4	2
3	Control de Comunicación (Software)	2	2	1	1	1	4	2
4	Equipo de Comunicación	3	1	2	2	1	4	2
5	Sistema de Correo Electrónico	2	2	1	1	1	4	2

ANEXO 26

MATRIZ PONDERADA

DE

FACTORES DE RIESGO Y VALORACIONES ASOCIADOS A LOS RECURSOS INFORMÁTICOS

	PONDERACIÓN	12%	12%	15%	15%	30%	8%	8%	100%
No.	**RECURSOS INFORMÁTICOS**	**Sistema de Control**	**Nivel de Sensibilidad**	**Complejidad**	**Materialidad**	**Imagen**	**Tiempo de realización de Auditorias previas**	**Respuesta ante fallas (Planes de contingencia)**	**TOTAL**
1	Servidor de Aplicaciones	3	3	3	3	1	4	1	232
2	Sistema Contable (software)	2	3	3	3	1	4	2	228
3	Control de Comunicación (Software)	2	2	1	1	1	4	2	156
4	Equipo de Comunicación	3	1	2	2	1	4	2	186
5	Sistema de Correo Electrónico	2	2	1	1	1	4	2	156

ANEXO 27

MATRIZ CATEGORIZADA

Rango para la escala de riesgo = 232 – 156 =76 → Este valor nos ayuda para obtener el tamaño del intervalo

Tamaño del intervalo para la escala de riesgo = 76 / 3 = 25.33 = 25

Escala de Riesgo:

Riesgo Bajo: 156 – 179

Riesgo Medio: 180 – 205

Riesgo Alto: 206 – 231

	PONDERACIÓN	12%	12%	15%	15%	30%	8%	8%	100%
No.	**RECURSOS INFORMÁTICOS**	**Sistema de Control**	**Nivel de Sensibilidad**	**Complejidad**	**Materialidad**	**Imagen**	**Tiempo de realización de Auditorias previas**	**Respuesta ante fallas (Planes de contingencia)**	**TOTAL**
1	Servidor de Aplicaciones	3	3	3	3	1	4	1	232
2	Sistema Contable (software)	2	3	3	3	1	4	2	228
3	Equipo de Comunicación	3	1	2	2	1	4	2	186
4	Control de Comunicación (Software)	2	2	1	1	1	4	2	156
5	Sistema de Correo Electrónico	2	2	1	1	1	4	2	156

ANEXO 28

AGROPEC S.A.

POLÍTICAS DE SEGURIDAD INFORMÁTICA

1. Justificación
2. Generalidades
3. Seguridad física
4. Seguridad lógica
5. Seguridad en redes
6. Seguridad en los recursos humanos
7. Seguridad en el Outsourcing
8. Planificación de seguridad informática
9. Planificación de contingencia y recuperación de desastres.

1. Justificación

Los activos de información y los equipos informáticos son recursos importantes y vitales de toda compañía. Sin ellos se quedarían rápidamente fuera del negocio y por tal razón la Gerencia tiene el deber de preservarlos, utilizarlos y mejorarlos. Esto significa que se deben tomar las acciones apropiadas para asegurar que la información y los sistemas informáticos estén apropiadamente protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales.

La información perteneciente a la compañía debe protegerse de acuerdo a su valor e importancia. Deben emplearse medidas de seguridad sin importar cómo la información se guarda (en papel o en forma electrónica), o como se procesa (PC`s, servidores, etc.), o cómo se transmite (correo electrónico, conversación telefónica). Tal protección incluye restricciones de acceso a los usuarios de acuerdo a su cargo.

Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos.

2. Generalidades

Está política debe ser comunicada a todos los usuarios de la organización, de una forma apropiada, accesible y entendible para el lector.

Objetivo

La compañía debe tener vigente una política de seguridad informática que le permita establecer un marco para la implantación de seguridad y control extensivo a todas las áreas.

Alcance

Está política se aplica a toda la organización, rige para todos los empleados de sistemas y el personal externo.

Responsabilidades

Los siguientes entes son responsables, en distintos grados, de la seguridad en la compañía:

1. **Comité de Informática.-** Será conformado por el Gerente, el Jefe de Seguridad y el Jefe de Sistemas. Este comité será responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con la Gerencia. También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados

con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

2. **Jefe de Seguridad.-** Es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes.

3. **Jefe de Sistemas.-** Es responsable de establecer los controles de acceso apropiados para cada usuario, la creación de nuevos usuarios, supervisar el uso de los recursos informáticos, administrar la red, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra. El Jefe de Sistemas también es responsable de informar al Jefe de Seguridad y a sus superiores sobre toda actividad sospechosa o evento insólito. Cuando no exista un Jefe de Seguridad, el Jefe de Sistemas realizará sus funciones.

4. **Usuarios.-** Son responsables de cumplir con todas las políticas de la compañía relativas a la seguridad informática y en particular:

   - Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.

   - No divulgar información confidencial de la compañía a personas no autorizadas.

   - No permitir y no facilitar el uso de los sistemas informáticos de la compañía a personas no autorizadas.
   - No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras

actividades que no estén directamente relacionadas con el trabajo en la compañía.

- Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.

- Seleccionar una contraseña fuerte que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.

- Reportar inmediatamente a su jefe inmediato a un funcionario del Departamento de Sistemas cualquier evento que pueda comprometer la seguridad de la compañía y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

- No dejar información confidencial en los escritorios al alcance de todos.

Incumplimiento o violación de las políticas

Si se llegase a incumplir o violar una de estas políticas por parte del personal, el área de sistemas o seguridad informática si existiere, realizará un informe detallado al gerente. Este informe describirá la circunstancia y la gravedad del hecho y el gerente deberá tomar las medidas necesarias sobre la persona implicada.

Estructura de la política

Está política se divide en las siguientes secciones:

- Seguridad física
- Seguridad lógica
- Seguridad en redes
- Seguridad en los recursos humanos
- Seguridad en el Outsourcing
- Planificación de seguridad informática
- Planificación de contingencia y recuperación de desastres.

Cada sección se divide en tres partes:

Propósito: Define la intensión de cada sección

Alcance: Define el ámbito de aplicación

Controles generales: define los objetivos para cada sección.

POLÍTICA DE SEGURIDAD FÍSICA

Propósito

El propósito de esta política preservar la seguridad de los recursos informáticos y garantizar la integridad y disponibilidad de los mismos.

Alcance

Estás políticas son aplicables a todos los recursos informáticos de la compañía entendiendo por ellos datos, hardware, software, personal e instalaciones.

Controles generales

1. Los computadores de la compañía sólo deben usarse en un ambiente seguro. Se considera que las oficinas de la empresa son un ambiente seguro porque en ellas se han implantado las medidas de control apropiadas para proteger datos, hardware, software, personal e instalaciones.

2. Toda persona debe portar credenciales de identificación.

3. Todas las personas ajenas a la organización deberán llevar un formulario de datos personales antes de ingresar a la empresa.

4. El personal de vigilancia debe controlar el ingreso y egreso de vehículos llevando una planilla con los datos personales de los ocupantes, la marca, número de placa y la hora de entrada y salida del mismo.

5. Se deben mantener registros de entrada al centro de cómputo.

6. Se debe instalar videocámaras en el centro de cómputo a fin de identificar personas ajenas a la organización.

7. El área de desarrollo deberá estar separada del área de producción.

8. La temperatura de los equipos de aire acondicionado que abastecen a toda la organización deberá estar entre los 18-19ºC.

9. En caso de que el equipo de aire acondicionado falle se deben contar con alternativas para solucionar este problema como equipos de respaldo o ventiladores de pedestales a fin de refrescar los equipos.

10. Debe respetarse y no modificar la configuración de hardware y software establecida por el Departamento de Sistemas, pues este cambio puede poner en riesgo la integridad y disponibilidad del equipo.

11. No se permite fumar, comer o beber mientras se está usando un computador.

12. La organización debe contar con señalización de salidas de emergencia, prohibiciones de comer, fumar, beber alrededor de los equipos.

13. El área de sistemas debe contar con una libreta donde se encuentren teléfonos de emergencia, para cualquier contingencia.

14. Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).

15. La temperatura de las oficinas con computadoras debe estar comprendida entre 18 y 21 grados centígrados y la humedad relativa del aire debe estar entre 45% y el 65%.

16. Deben existir conexiones independientes para los equipos de cómputo.

17. Los cables eléctricos deben ser puestos en paneles y canales resistentes al fuego.

18. Deben usarse reguladores de voltaje, equipos de protección como fuentes de poder ininterrumpibles (UPS).

19. Se debe contar con equipos de suministro de energía alternos en caso de fallas.

20. Instalarse alarmas en el centro de cómputo así como detectores de humo como esquemas correctivos ante incendios.

21. Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

22. Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de llaves.

23. Los servidores no pueden estar sobre pisos falsos.

24. Los servidores de red y los equipos de comunicación (modems, routers, etc) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso

25. Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.

26. No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la compañía se requiere una autorización escrita.

27. La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

28. Se debe llevar un registro de entrada y salida de los equipos de las instalaciones de la empresa.

29. Los usuarios deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad.

30. El usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina.

31. No está permitido llevar al sitio de trabajo computadoras portátiles (laptops) o cualquier equipo personal, y en caso de ser necesario se requiere solicitar la autorización correspondiente.

32. Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.

33. A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la compañía está protegido por derechos de autor y cuenta con licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

34. Los usuarios no deben copiar a un medio removible (como un diskette), el software o los datos residentes en las computadoras de la compañía, sin la aprobación previa de la Gerencia General o Jefe de Sistemas.

35. Se deben desactivar las unidades de disquete de las estaciones de trabajo.

36. No pueden extraerse datos fuera de la sede de la compañía sin la aprobación previa de la gerencia.

37. Siempre que sea posible, debe eliminarse información confidencial de los computadores y unidades de disco duro antes de que se les envíe a reparación.

38. No deben dejarse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial de la compañía.

39. No se permite bajo ninguna circunstancia el uso de cualquiera de las computadoras con propósitos de ocio o lucro.

40. Se dará mantenimiento a los equipos de acuerdo a las especificaciones del proveedor.

41. Sólo el personal de mantenimiento debidamente autorizado debería realizar la reparación y servicio de los equipos.

42. Se deben mantener registros de los mantenimientos preventivos y correctivos, además de sospechas de falla y fallas reales.

43. Todos los equipos deben estar cubiertos por un seguro.

44. El administrador del sistema es el responsable de realizar respaldos de la información.

45. Cada treinta días deberá efectuarse un respaldo completo del sistema y cada día deberán ser respaldados todos los archivos que fueron modificados o creados.

46. La información respaldada deberá ser almacenada en un lugar seguro y distante del sitio de trabajo.

47. Los respaldos deben estar debidamente etiquetados, está etiqueta deberá indicar fecha y contenido del mismo.

48. Deberá mantenerse siempre una versión reciente impresa de los archivos más importantes del sistema.

49. En el momento en que la información respaldada deje de ser útil a la organización, dicha información deberá ser borrada antes de deshacerse del medio.

50. Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.

51. Las impresoras, faxes, copiadoras deben estar situados en lugares de acceso restringido.

52. Los empleados deben archivar inmediatamente documentos que ya no van a utilizar y no dejarlos sobre sus escritorios.

53. Se deben emplear trituradoras de papel para eliminar documentos que ya no son de uso en la oficina.

POLÍTICA DE SEGURIDAD LOGICA

Propósito

Tiene como propósito controlar el acceso a la información y los procesos del negocio.

Alcance

Estás políticas son aplicables para todos los sistemas de información, datos de la compañía. Así mismo es aplicable a todos los miembros de la entidad que hacen uso de los sistemas de información.

Controles generales

Cuentas

1. Se debe crear un documento en donde el empleado declare conocer las políticas y procedimientos de seguridad y se haga responsable del uso de su cuenta de usuario

2. El usuario al recibir una nueva cuenta, debe firmar un documento de responsabilidad con el uso que le de a su cuenta.

3. La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada por el

respectivo Jefe de área, Jefe de Recursos Humanos y la Gerencia.

4. Las cuentas deben ser otorgadas exclusivamente a usuarios legítimos.

5. Una cuenta deberá estar conformada por un nombre de usuario y su respectiva contraseña.

6. El nombre de usuario de una cuenta deberá estar conformado por la primera letra de su nombre y su apellido paterno.

7. Los privilegios de lectura, escritura, creación, eliminación y modificación de datos deben definirse de una manera consistente con las funciones que desempeña cada usuario.

8. Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses.

9. Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.

10. Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.

11. Cuando un empleado es despedido, renuncia o sale de vacaciones de la compañía, debe desactivarse su cuenta antes de que deje el cargo.

12. La cuenta de un usuario es personal e intransferible, por lo cual no se permite que este comparta su cuenta ni su contraseña con persona alguna, aún si ésta acreditada la confianza del usuario.

Contraseñas

1. La longitud de una contraseña deberá siempre ser verificada de manera automática al ser construida por el usuario. Todas las contraseñas deberán contar con al menos siete caracteres.

2. La longitud de la contraseña serán de mínimo 8 caracteres y máximo 10.

3. Todas las contraseñas elegidas por los usuarios deben ser difíciles de adivinar.

4. No deben ser utilizadas como claves palabras que aparezcan en el diccionario, secuencias conocidas de caracteres, datos personales ni acrónimos.

5. Está prohibido que los usuarios construyan contraseñas compuestas de algunos caracteres constantes y otros que cambien de manera predecible y sean fáciles de adivinar.

6. Los usuarios no deben construir contraseñas idénticas o muy parecidas a contraseñas anteriores.

7. El usuario no debe guardar su contraseña en una forma legible en archivos, disco y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada.

8. Nunca debe compartirse la contraseña o revelarla a otros.

9. Las contraseñas deben ser encriptadas para imposibilitar su identificación.

Control de acceso

1. Todos los usuarios deberán acceder al sistema contable utilizando algún programa que permita una comunicación segura y encriptada.

2. Al momento de ingresar al sistema contable y al sistema operativo, cada usuario deberá ser notificado de la fecha, hora y dirección desde la que se conectó al sistema por última vez.

3. Para prevenir ataques, cuando el software del sistema contable lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema.

4. Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo específicamente 10 a 15 minutos, el sistema debe automáticamente borrar la pantalla y suspender la sesión.

5. Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la compañía, pudiendo ser causal de despido.

6. Se deben establecer días y horas de trabajo para los usuarios dentro del sistema contable.

Aplicaciones

1. Está estrictamente prohibido hacer uso de programas que explotan alguna vulnerabilidad de un sistema para proporcionar privilegios no otorgados explícitamente por el administrador.

2. Está estrictamente prohibido hacer uso de herramientas propias de delincuentes informáticos, tales como programas que rastrean vulnerabilidades en sistemas de cómputo propios o ajenos.

3. Se deben generar registros del uso de las aplicaciones que contengan:
   - El identificador del usuario
   - Fecha y hora de conexión y desconexión
   - Identificación del terminal
   - Registro de intentos aceptados y rechazados de acceso al sistema.
   - Registro de los intentos aceptados y rechazados de acceso a datos y otros recursos.

4. Los archivos de bitácora (logs) y los registros de auditoria que graban los eventos relevantes sobre la seguridad de los sistemas informáticos, deben revisarse cada semana y guardarse durante un tiempo prudencial de por lo menos tres meses.

5. Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo

abuso, fraude u otro acceso que ponga en riesgo a los sistemas informáticos.

6. Está terminantemente prohibido instalar programas de uso personal.

Problemas de seguridad lógica

1. Se debe implementar un sistema de manejo de problema de seguridad lógica en el que se registren y den seguimiento a todos los incidentes de seguridad lógica, inclusive las causas que lo provocaron.

2. El software de desarrollo y de producción deberán funcionar en servidores distintos.

3. Las tareas de desarrollo y producción deben estar separadas.

4. Los servicios del sistema no deben ser accesibles desde los sistemas de producción.

5. Se deben tener claves diferentes para el sistema de producción y el de desarrollo.

POLÍTICA DE SEGURIDAD EN REDES

Propósito

El propósito de esta política es establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de la compañía al estar conectada a redes de computadoras.

Alcance

Esta política se aplica a todos los empleados, y personal temporal de la compañía.

Controles generales

Correo electrónico, Internet e Intranet.

1. Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Jefe de Sistemas y poner la computadora en cuarentena hasta que el problema sea resuelto.

2. Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos. Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otros departamentos de la compañía.

3. No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que este haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Departamento de Sistemas.

4. No deben usarse diskettes u otros medios de almacenamiento en cualquier computadora de la compañía a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.

5. El usuario es la única persona autorizada para leer su propio correo, a menos que él sistema autorice explícitamente a otra persona para hacerlo, o bien, que su cuenta esté involucrada en un incidente de seguridad de cómputo.

6. Está estrictamente prohibido usar la cuenta de correo electrónico proporcionada por la organización para propósitos ajenos a sus actividades laborales.

7. No se permite el uso de la cuenta de correo electrónico para suscribirse a listas electrónicas de discusión de interés personal.

8. El firewall será programado para dar acceso sólo a páginas que cada usuario por sus funciones tendrá permitido acceder.

POLÍTICA DE SEGURIDAD
EN LOS RECURSOS HUMANOS

Propósito

El propósito de esta política es establecer las directrices, los procedimientos y los requisitos para reducir los riesgos de error humano, robo, fraude o uso inadecuado de las instalaciones.

Alcance

Esta política se aplica a todos los empleados, y personal temporal de la compañía.

Controles generales

1. Se deben verificar las recomendaciones y antecedentes de los postulantes a ingresar a la empresa.

2. Se deben firmar con los empleados acuerdos de confidencialidad o no divulgación de la información.

3. En los términos y condiciones del contrato se debe indicar la responsabilidad que el empleado tiene en cuanto a la seguridad de la información.

4. Todos los empleados deben tener conocimientos de las políticas de seguridad de información de la empresa.

5. Los empleados deben informar a sus superiores de los incidentes que afecten a la seguridad de la información.

6. La capacitación de los usuarios debe ser orientada a incrementar la conciencia de la necesidad de proteger los recursos informáticos.

7. Debe existir una adecuada separación funciones entre los empleados, especialmente los integrantes del área de sistemas.

8. El Departamento de Recursos Humanos deberá comunicar inmediatamente al área de informática la separación del empleado de la empresa.

9. El Departamento de Sistemas será el encargado de dar de baja los accesos del empleado separado de la organización.

POLÍTICA DE SEGURIDAD EN EL OUTSOURCING

Propósito

Tiene como propósito proteger los recursos informáticos de la organización.

Alcance

Estás políticas son aplicables para todo tipo de servicio externo que la empresa solicite.

Controles generales

1. Deberá realizarse un concurso de méritos para seleccionar al proveedor del servicio tercerizado.

2. Se deberá definir claramente la duración del contrato.

3. Se definirán las condiciones previstas para la resolución del contrato con anterioridad a la fecha de su finalización.

4. Se detallaran minuciosamente todos y cada uno de los compromisos concretos que van a ser contraídos por la organización y la empresa de outsourcing.

5. Se establecerá en el contrato el plan de pagos en que se remunerará el servicio.

6. Establecer en el contrato de outsourcing que su personal deberá regirse por la política de seguridad de información de la organización contratista.

7. Establecer en el contrato con la empresa de outsourcing la responsabilidad que tiene de mantener segura la información de la empresa contratante.

8. El contrato de outsourcing deberá prever las cláusulas necesarias en caso de terminación anticipada del contrato.

9. Se debe seguir los lineamientos de todo contrato con la ayuda de un abogado.

POLÍTICA DE PLANIFICACIÓN DE SEGURIDAD INFORMÁTICA

Propósito

El propósito de está política es definir los lineamientos para diseñar e implantar un modelo de seguridad en la compañía que proteja la información y los activos de la organización.

Alcance

Esta política se aplica a toda la organización.

Controles generales

1. El Comité de Seguridad en conjunto con la Gerencia deberán elaborar e implantar un plan estratégico de seguridad informática, el cual deberá estar alineado con el plan y el presupuesto de la organización. Para la elaboración de dicho plan se deben considerar, evaluar y priorizar los requerimientos de seguridad de los recursos informáticos.

2. El plan de seguridad informática debe ser aprobado por la Gerencia de la organización considerando, para cada uno de los objetivos involucrados, la razonabilidad de los plazos, beneficios a obtener y costos asociados.

3. El plan de seguridad informática debe mantenerse actualizado.

4. El comité de seguridad debe elaborar un presupuesto asociado a la ejecución del plan de seguridad informática, el cual debe ser evaluado y aprobado por la Gerencia, e incorporado al presupuesto anual de la organización.

5. La Gerencia de la organización debe controlar en forma periódica, el grado de avance del plan de seguridad informática, a efectos de detectar y evitar desvíos en los plazos, costos y metas previstas.

6. Las adquisiciones de hardware, software u otros servicios informáticos, deben responder a los objetivos incluidos en el plan de seguridad informática de la organización. Las situaciones de excepción deben ser autorizadas por la Gerencia de la organización.

POLÍTICA DE PLANIFICACIÓN DE CONTINGENCIA Y RECUPERACIÓN DE DESASTRES

Propósito

Garantizar la continuidad de las operaciones de negocio de la compañía y limitar el impacto económico/financiero e intangible en el negocio en caso que se detecte un evento inesperado que ocasione la interrupción de las operaciones de la compañía.

Alcance

Esta política se aplica a todos los sistemas de información y datos de la compañía.

Controles generales

1. El plan de contingencia debe ser realizado y sometido a prueba por el Jefe de seguridad, Jefe de sistemas y junto a la ayuda del personal seleccionado para el plan. Este plan deberá ser aprobada toda su ejecución por la Gerencia.

2. Deben proveerse procedimientos de contingencia para los sistemas del negocio que incluyan niveles definidos y documentados de recuperación en el caso de desastres o fallas de sistemas.

3. Se debe proteger primero al personal como recurso fundamental en cualquier contingencia.

4. Deben ponerse a prueba tales planes en un intervalo de seis meses. Las actividades de planificación de contingencia deben ser coordinadas y administradas en forma centralizada.

5. Se deben identificar los registros esenciales y hacer los arreglos adecuados para mantener copias de tales registros en las sedes alternativas donde se trabajará en caso de eventos inesperados.

6. Las sedes alternativas no deben estar ubicadas en el mismo lugar donde se encuentre el centro de cómputo.

7. Debe disponerse de una copia completa de la documentación requerida, el software de base, software de aplicaciones y datos en producción, así como los registros (logs) de transacciones que permitan restaurar los datos o información en caso de pérdidas o daños.

8. Las copias de resguardo de los sistemas principales, los datos de registros esenciales y la documentación de Tecnología Informática, deben ser almacenadas teniendo en cuenta las políticas de seguridad física.

9. Deben registrarse y resguardarse los registros históricos que contabilicen los medios de almacenamiento de copias de resguardos que se mantienen en las sedes remotas de almacenamiento.

10. Se deben establecer planes de contingencias detallados que definan las acciones que han de tomarse y el personal requerido, para realizar la recuperación de los sistemas del negocio.

11. En el plan debe definirse quién es el responsable de su ejecución y detallar las funciones que las personas involucradas en el plan deben tener.

12. El plan de contingencia deberá ser conocido por toda la organización.

13. Dichos planes deben ser revisados y actualizados cada seis meses.

ANEXO 29

AGROPEC S.A.

PLAN ESTRATEGICO DE SEGURIDAD INFORMÁTICA 2006-2007

INTRODUCCIÓN

El presente plan estratégico tiene como finalidad establecer objetivos mínimos de seguridad para la organización.

Este Plan consta de dos partes, la primera parte la constituyen: una breve presentación, descripción del objetivo del Plan, el alcance del mismo y un resumen de resultados del análisis de riesgo; en la segunda parte se describe cada uno de los objetivos del plan:

1. Elaborar Políticas de seguridad informática.
2. Implementar seguridades físicas
3. Mejorar la seguridad lógica
4. Establecer seguridades en redes
5. Fortalecer la seguridad en los Recursos Humanos
6. Implantar medidas de seguridad en el outsourcing
7. Implementar estrategias de continuidad.
8. Revisar el cumplimiento de las políticas de seguridad informática.

PRIMERA PARTE

PRESENTACIÓN

El Plan Estratégico de Seguridad Informática de la empresa AGROPEC S.A. 2006 – 2007 responde a los siguientes principios que definen la seguridad informática.

- √ **Confidencialidad.** Proporcionando acceso a la información solamente a los usuarios autorizados
- √ **Integridad.** Garantizando que la información sobre la cual la empresa tomara decisiones no haya sufrido manipulación alguna antes, durante y después de su procesamiento.
- √ **Disponibilidad.** Permitiendo acceder a la información o utilizar algún servicio informático siempre que sea necesitado

OBJETIVO GENERAL

El objetivo del presente Plan Estratégico de Seguridad Informática es proporcionar los lineamientos para promover la planeación, el diseño e implantación de un modelo de seguridad en la organización.

ALCANCE

Este documento se aplica para todos los empleados de la empresa AGROPEC S.A, así como a personal externo que desempeñen labores o le proporcionen algún tipo de servicio o producto a la entidad.

RESUMEN DE RESULTADOS DEL ANÁLISIS DE RIESGO

La identificación de riesgos en la organización dio como resultados los siguientes factores de riesgo: Sistema de Control, Nivel de Sensibilidad, Complejidad, Materialidad, Imagen, Tiempo de realización de Auditorías previas, Respuesta ante fallas (Planes de Contingencia) los cuales fueron analizados mediante una confrontación con los recursos informáticos de la empresa.

De este análisis se determino que el Servidor de aplicaciones y el Sistema Contable están categorizados con un riesgo alto; el Equipo de comunicación está en la categoría de riesgo medio y el software de control de comunicaciones y el sistema de correo electrónico tienen un riesgo bajo. Tomando como fundamento estos resultados se procedió a la elaboración de este Plan Estratégico.

SEGUNDA PARTE

OBJETIVOS DE IMPLEMENTACIÓN DEL PLAN

Para el desarrollo del plan he establecido 8 objetivos en común acuerdo con la Gerencia quienes en conjunto con quién redacta este plan trabajamos por espacio de un mes en determinar el alcance del plan y lo primero que se debe hacer en el corto, mediano y largo plazo.

El primero y segundo objetivo se desarrollarán en los meses de Julio y Agosto; el tercero y cuarto objetivo se llevarán a cabo en el mes de Septiembre; el séptimo objetivo se efectuará en el mes de Octubre; el quinto y sexto objetivo se llevarán cabo en Noviembre y el cumplimiento del octavo objetivo será cada seis meses a partir de la ejecución de este plan.

OBJETIVO 1
ELABORAR POLÍTICAS DE SEGURIDAD INFORMÁTICA

Tareas

1. Se deben relevar los riesgos de la organización siguiendo una metodología de riesgo
2. Se debe valorar los riesgos determinando objetos y factores de riesgos.
3. Se elabora la matriz de ponderación
4. Se determinan los principales aspectos de control que deben documentarse en la política.
5. Se documenta la política, alineada con los objetivos generales de la organización y basada en directrices y modelos de tecnología de información.
6. Se implementa la política.
7. Se capacita a todo el personal en materia de seguridad y en la política.

Responsables

El Jefe de Seguridad y la Gerencia serán los encargados del cumplimiento de este objetivo que será ejecutado por toda la organización.

Fecha de Realización

Mes de Julio y Agosto.

OBJETIVO 2
IMPLEMENTAR SEGURIDADES FÍSICA

Tareas

1. Establecer un sistema de registro de acceso al centro de cómputo.
2. Se comprarán equipos de seguridad definidos con la Gerencia (extintores, detectores de humo, alarmas contra robo, etc)
3. Se adquirirá equipos de aire acondicionado que actúen como respaldo en caso de que se averíe alguno y así mantener el ambiente correcto en que deben trabajar los equipos
4. Se controlará periódicamente si el ambiente en que trabajan los equipos es el correcto
5. Se verificará que los usuarios configuren el protector de pantalla en sus equipos y lo activen siempre que se ausenten de la oficina.
6. Se llevarán registros del mantenimiento preventivo y correctivo que se realice a los equipos de computación.
7. El Departamento de Sistemas se encargará de presentar a la Gerencia reportes que indiquen el estado físico de los equipos.
8. Se definirá con la Gerencia la compra de trituradoras de papel para la eliminación de documentos ya no utilizados y así proteger la confidencialidad de los datos.
9. La Gerencia recibirá asesoramiento de Sistemas para que la póliza de seguros de los equipos cubra todo tipo de riesgos.
10. Se capacitará al personal en las medidas de seguridad física.

Responsables

El Jefe de Seguridad, la Gerencia y el Jefe de Compras serán los encargados de la ejecución de este objetivo el cual se llevará a cabo en toda la organización.

Fecha de Realización

Mes de Julio y Agosto.

OBJETIVO 3
MEJORAR LA SEGURIDAD LÓGICA

Tareas

1. Implantar un sistema de análisis periódico de riesgos, a fin de que identifiquen, se midan, se comuniquen y se establezcan controles lógicos.
2. Se definirán objetivos de control.
3. Se aplicarán esquemas de seguridad como:
   a. Revisiones periódicas de los derechos de acceso de los usuarios dentro del sistema.
   b. Establecer que el tiempo de conexión a la red se límite al horario normal de oficina.
   c. Hacer de conocimiento de los usuarios los requisitos de seguridad y los procedimientos que deben seguir para proteger sus datos, entre éstos puede ser asegurarse que se desconectó debidamente de la red.
   d. Llevar una bitácora de eventos que incluya:
      - El identificador del usuario.
      - Fecha y hora de conexión y desconexión.
      - Registro de los intentos aceptados y rechazados de acceso al sistema.
      - Registro de los intentos aceptados y rechazados de acceso a datos y otros recursos.

Responsables

Igual que el anterior el Jefe de Seguridad y la Gerencia serán los encargados de la ejecución de este objetivo en el software de la empresa.

Fecha de Realización

Mes de Septiembre.

OBJETIVO 4

ESTABLECER SEGURIDADES EN REDES

Tareas

1. Capacitar a los usuarios en el uso de software antivirus y en las precauciones adecuadas en el uso del correo electrónico.
2. Realizar periódicamente escaneos de virus a los equipos.
3. Actualizar el antivirus en los computadores ya sea como control preventivo o como rutina básica de seguridad.
4. Programar el firewall para dar accesos de acuerdo a las funciones y direcciones IP de los usuarios.
5. Implementar medidas de control en el acceso remoto a la red mediante usuarios y contraseñas previamente definidos.

Responsables

El Jefe de Sistemas será el responsable de la ejecución de este objetivo en toda la empresa.

Fecha de Realización

Mes de Septiembre.

OBJETIVO 5
FORTALECER LA SEGURIDAD EN LOS RECURSOS HUMANOS

Tareas

1. Investigar los antecedentes de los candidatos a ser empleados de la empresa.
2. Incluir cláusulas de confidencialidad en los contratos de trabajo.
3. Capacitar a los empleados periódicamente brindándoles información actualizada sobre la seguridad y el uso apropiado de las computadoras.
4. Establecer procedimientos para informar acerca de incidentes de seguridad.
5. Controlar que exista una adecuada segregación de funciones en cada una de las áreas de la organización.
6. Mantener informada al Área de Sistemas oportunamente de los despidos o renuncias de los empleados.
7. Establecer procedimientos disciplinarios para los empleados que violen las políticas de seguridad.

Responsables

El Jefe de Seguridad, la Gerencia y el Jefe de Recursos Humanos serán los responsables de ejecutar este objetivo en toda la empresa.

Fecha de Realización

Mes de Noviembre.

OBJETIVO 6
IMPLEMENTAR MEDIDAS DE SEGURIDAD EN EL OUTSOURCING

Tareas

1. Realizar concurso de méritos para seleccionar a las empresas que nos brinden servicios, ya sean éstos de mantenimiento preventivo, detectivo o correctivo de recursos informáticos.
2. Constatar las referencias de los servicios prestados por la empresa seleccionada a sus clientes.
3. Establecer en los contratos acuerdos y requerimientos de seguridad, establecidos en la política de seguridad informática.
4. Efectuar revisiones periódicas del cumplimiento de la política de seguridad informática por parte del personal tercerizado.
5. Hacer cumplir estos acuerdos y requerimientos.

Responsables

La Gerencia y el Jefe del Departamento Legal serán los responsables de ejecutar este objetivo en toda la empresa.

Fecha de Realización

Mes de Noviembre.

OBJETIVO 7
IMPLEMENTAR ESTRATEGIAS DE CONTINUIDAD

Tareas

1. Se identificarán las necesidades de la estrategia de continuidad de negocio.
2. Evaluar la idoneidad de las estrategias alternativas consideradas, a la vista de los resultados del análisis de impacto realizado.
3. Preparar un análisis costo beneficio de las estrategias de recuperación y presentar las conclusiones a la Dirección.
4. Seleccionar un centro alternativo y almacenamiento externo.
5. Definir y seleccionar un acuerdo contractual para los servicios de continuidad de negocio.
6. Se realizarán respaldos diarios de la información de la Base de Datos.
7. La Gerencia junto con el Jefe de Seguridad, determinarán el lugar donde se guardarán los respaldos fuera de la empresa.

Responsables

El Jefe de Sistemas y la Gerencia serán los responsables de llevar a cabo este objetivo en toda la empresa.

Fecha de Realización

Mes de Octubre.

OBJETIVO 8
REVISAR EL CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE INFORMACIÓN

Tareas

1. Los sistemas de información serán revisados para la conformidad con los estándares de implementación de seguridad.
2. Los Jefes de Área se asegurarán de que se cumplen correctamente los procedimientos de seguridad dentro de su área de responsabilidad.
3. Todas las áreas de la organización serán consideradas para las revisiones regulares del cumplimiento de las políticas de seguridad.

Responsables

El Jefe de Seguridad y la Gerencia serán los encargados de hacer cumplir este objetivo en toda la empresa.

Fecha de Realización

Cada seis meses a partir del inicio de la ejecución de este plan.