

BONNADOR

AUDITORÍA INFORMÁTICA

OBJETIVOS DE CONTROL

**CONTROLES EN UN ENTORNO INFORMATIZADO:
OBJETIVOS, DIRECTIVAS Y
PROCEDIMIENTOS DE AUDITORÍA.**

BELDEN MENKUS, CISA, CSP
EDITOR

ZELLA G. RUTHBERG, CSP
ASSISTANT EDITOR

Traducción Autorizada y Exclusiva en Español,
por Manuel Palao, CISA.

THE EDP AUDITORS FOUNDATION, INC.
Carol Stream, Illinois, Estados Unidos.
THE INFORMATION SYSTEMS CONTROL FOUNDATION.

La información contenida en esta publicación pretende reflejar una concepción del diseño, desarrollo, operación, mantenimiento, y auditoría de sistemas de información –tanto en una configuración convencional centralizada cuanto en un entorno informático de los denominados distribuidos. Ciertas prácticas y procedimientos contenidos en esta publicación pueden no ser aplicables a todos los sistemas de proceso de datos. En consecuencia, el incumplimiento de alguna práctica o procedimiento específico contenido en esta publicación no debiera ser utilizado para imputar a la dirección un fallo en el uso de la prudencia o de la precaución en el cumplimiento de sus obligaciones.

La **EDP Auditors Foundation** es una corporación no lucrativa de beneficios mutuos de California, con capítulos en todo el mundo. Su propósito y objetivo es dedicarse a la formación e investigación en el campo de la Auditoría de Sistemas de Información. Se entiende que ni la EDP Auditors Foundation ni sus autores están prestando aquí servicio legal, contable o profesional alguno y en consecuencia rechazan explícitamente cualquier responsabilidad resultante del seguimiento de cualesquiera de las informaciones, prácticas o procedimientos contenidos en esta publicación. Esta publicación no toma en consideración ningún requisito legal o gubernamental que afecte a las prácticas de auditoría y a los controles en los diversos países.

Esta publicación se preparó bajo la dirección de los siguientes miembros de la Junta de la **EDPAA/EDPAF** de 1.989-1.990:

International President	John A. Kuyers, CPA, CISA, CSP Ernst & Young
Executive Vice-President	Deepak Sarup, ACA Deloitte Ross Tohmatsu International
Administrative Vice-President	Arnold Dito, CISA Fireman's Fund Insurance Co.
Vice-President of Research	Michael Donahue, CISA, CSP Price Waterhouse.

Reconocemos también con agradecimiento la asistencia de Joann Menkus en la corrección y composición iniciales y la de Steven Arbitman por agilizar las artes finales de este documento.

© **Copyright**, 1990 por la **EDP Auditors Foundation Inc.** Carol Stream, Illinois Estados Unidos) Reservados todos los derechos. Ninguna parte de esta publicación puede ser reproducida en forma alguna sin el permiso escrito de la Fundación.

© **Copyright**, 1990 del original en inglés: **EDPAF**.

Traducción al castellano por **Manuel Palao**, CISA, vice-Presidente de la Organización de Auditoría Informática, Capítulo Español de la EDPAF; bajo permiso de y mediante acuerdo con la EDPAF, editora del original inglés, y que retiene todos sus derechos.

© **Copyright**, 1991 de la traducción al castellano: **Manuel Palao**.

Esta traducción ha sido supervisada por Miguel Ángel Ramos, CISA miembro del Comité Directivo y ex-Presidente de la Organización de Auditoría Informática, Capítulo Español de la EDPAF, y por Peggy S. Whobrey, Traductora e Intérprete certificada por los Tribunales Federales de los EEUU; y ha sido sometida a consulta a los miembros del Comité Directivo de la Organización de Auditoría Informática.

La EDPAF declina toda responsabilidad que pudiera sobrevenirle por esta traducción. Manuel Palao asume la plena responsabilidad de que su versión es, a su leal saber y entender, una traducción fiel y cierta del original.

. . .

CONTENIDO

PREÁMBULO	I
1. La naturaleza de "Control"	I
2. Estructura de esta publicación	II
3. Terminología empleada en esta publicación	IV
NOTA DEL TRADUCTOR	VI

PARTE I: CONTROLES GENERALES Y DE APLICACIONES

1	CONTROLES DE GESTIÓN	I-1-1
	1.1 PLANIFICACIÓN DEL DEPARTAMENTO DE INFORMÁTICA	I-1-1
	1.1.1 Planificación a largo plazo de la organización	I-1-1
	1.1.2 El Comité de Planificación o de Dirección del Departamento de Informática	I-1-1
	1.1.3 Planificación a largo plazo del Departamento de Informática	I-1-2
	1.1.4 Planificación a corto plazo de la organización y del Departamento de Informática	I-1-3
	1.1.5 Revisión de la planificación de la organización y del Departamento de Informática	I-1-3
	1.2 POLÍTICAS, ESTÁNDARES Y PROCEDIMIENTOS	I-1-4
	1.2.1 Políticas	I-1-4
	1.2.2 Estándares	I-1-4
	1.2.3 Procedimientos	I-1-4
	1.3 RESPONSABILIDADES ORGANIZATIVAS Y GESTIÓN DE PERSONAL .	I-1-5
	1.3.1 La ubicación del Departamento de Informática en la organización.	I-1-5
	1.3.2 Descripción de responsabilidades dentro del Departamento de Informática.	I-1-5
	1.3.3 Separación de funciones	I-1-6
	1.3.4 Descripción de puestos del Departamento de Informática	I-1-6
	1.3.5 Selección de personal	I-1-7
	1.3.6 Procedimientos de acreditación de seguridad del personal.	I-1-7
	1.3.7 Procedimientos de baja del personal.	I-1-8
	1.3.8 Formación del personal.	I-1-9

OBJETIVOS DE CONTROL, 1990.

	1.3.9 Evaluación de la ejecutoria del empleado en el puesto.	I-1-9
1.4	GARANTÍA DE CALIDAD DEL DEPARTAMENTO DE INFORMÁTICA.	I-1-10
	1.4.1 Responsabilidad de la garantía de calidad (G.C.)	I-1-10
	1.4.2 Aspectos organizativos de la función de garantía de calidad. (GC).	I-1-10
	1.4.3 Cualificación del personal de garantía de calidad. (GC).	I-1-11
	1.4.4 Plan de revisión de la garantía de calidad. (GC).	I-1-11
	1.4.5 Revisión por garantía de calidad (GC) del logro de los objetivos del Departamento de Informática.	I-1-12
	1.4.6 Revisión por garantía de calidad (GC), del cumplimiento de los estándares y procedimientos del Departamento de Informática.	I-1-13
	1.4.7 Revisión por garantía de calidad (GC) de los controles de sistemas	I-1-13
	1.4.8 Revisión por garantía de calidad (GC) de otros aspectos de las funciones del Departamento de Informática	I-1-13
	1.4.9 Informes de las revisiones de garantía de calidad (GC).	I-1-14
1.5	LA FUNCIÓN DE AUDITORÍA INTERNA.	I-1-14
	1.5.1 El estatuto de auditoría interna	I-1-14
	1.5.2 Competencia técnica del personal de auditoría interna.	I-1-15
	1.5.3 Formación continuada del personal de auditoría interna.	I-1-16
	1.5.4 Rendimiento del trabajo de auditoría interna.	I-1-16
	1.5.5 Informes de la función de auditoría interna.	I-1-16
1.6	ESPECIFICACIONES DE ORIGEN EXTERNO.	I-1-17
2	CONTROLES DE DESARROLLO, ADQUISICIÓN Y MANTENIMIENTO DE SISTEMAS INFORMÁTICOS.	I-2-1
	2.1 METODOLOGÍA Y RESPONSABILIDAD DEL CICLO DE VIDA DEL DESARROLLO DE SISTEMAS.	I-2-1
	2.1.1 Metodología de ciclo de vida del desarrollo de sistemas.	I-2-1
	2.1.2 Papeles y responsabilidades.	I-2-2
	2.1.3 Actualización del ciclo de vida del nuevo sistema.	I-2-2
	2.2 INICIACIÓN DEL PROYECTO.	I-2-3
	2.2.1 Definición del proyecto.	I-2-3
	2.2.2 Participación del departamento usuario en la iniciación del proyecto.	I-2-4

2.2.3	Composición y responsabilidades del equipo de proyecto.	I-2-4
2.2.4	Definición de las necesidades de información.	I-2-5
2.2.5	Aprobación del proyecto.	I-2-5
2.3	ESTUDIO DE VIABILIDAD	I-2-6
2.3.1	Formulación de cursos de acción alternativos.	I-2-6
2.3.2	Estudio de viabilidad tecnológica	I-2-7
2.3.3	Estudio de viabilidad económica	I-2-8
2.3.5	Aprobación del proyecto.	I-2-9
2.3.6	Plan director del proyecto.	I-2-9
2.3.7	Control de costes.	I-2-10
2.4	FASE DE DISEÑO.	I-2-10
2.4.1	Metodología de diseño	I-2-10
2.4.2	Definición y documentación de las especificaciones de salida.	I-2-10
2.4.3	Documentación y definición de especificaciones de entrada.	I-2-11
2.4.4	Definición y documentación de especificaciones de ficheros.	I-2-11
2.4.5	Documentación y definición de especificaciones de proceso.	I-2-12
2.4.6	Especificaciones de programas.	I-2-12
2.4.7	Diseño de la recogida de datos fuente.	I-2-13
2.4.8	Diseño de controles y seguridad.	I-2-13
2.4.9	Diseño de pistas de auditoría.	I-2-14
2.4.10	Aprobación del diseño.	I-2-15
2.4.11	Estándares de documentación de programas.	I-2-15
2.4.12	Plan de validación, verificación y pruebas.	I-2-16
2.5	DÉSARROLLO E IMPLANTACIÓN.	I-2-16
2.5.1	Objetivos de programación.	I-2-17
2.5.2	Descripción de la narrativa del programa.	I-2-17
2.5.3	Paquetes de logical de aplicación.	I-2-18
2.5.4	Contratación de programas de aplicación a medida.	I-2-18
2.5.5	Manual de operaciones y mantenimiento.	I-2-19
2.5.6	Manual de usuario.	I-2-20
2.5.7	Plan de Formación.	I-2-21
2.5.8	Estándares de prueba de programas.	I-2-21
2.5.9	Estándares de prueba de sistemas.	I-2-21
2.5.11	Evaluación de los resultados de las pruebas.	I-2-23
2.5.12	Plan de Conversión.	I-2-23
2.5.13	Pruebas en Paralelo	I-2-24
2.5.14	Prueba de aceptación final.	I-2-24

OBJETIVOS DE CONTROL, 1990.

2.6	EXPLOTACIÓN Y MANTENIMIENTO.	I-2-25
	2.6.1 Procedimientos de control de explotación.	I-2-25
	2.6.2 Control de costes.	I-2-25
	2.6.3 Modificaciones al sistema.	I-2-26
	2.6.4 Re-evaluación de las especificaciones de usuario.	I-2-26
2.7	REVISIÓN POST-IMPLANTACIÓN.	I-2-26
	2.7.1 Plan de revisión post-implantación.	I-2-27
	2.7.2 Evaluación de resultados.	I-2-27
	2.7.3 Evaluación del cumplimiento de las especificaciones de usuario.	I-2-28
	2.7.4 Análisis de evaluación coste-beneficio.	I-2-28
	2.7.5 Evaluación del cumplimiento de los estándares de desarrollo.	I-2-28
	2.7.6 Informe sobre los hallazgos de la revisión post-implantación.	I-2-29
3	CONTROLES DE EXPLOTACIÓN DE SISTEMAS DE INFORMACIÓN.	I-3-1
	3.1 PLANIFICACIÓN Y GESTIÓN DE RECURSOS DEL DEPARTAMENTO DE INFORMÁTICA.	I-3-1
	3.1.1 Presupuesto operativo anual del Departamento de Informática.	I-3-1
	3.1.2 Plan de Adquisición de Equipos.	I-3-1
	3.1.3 Gestión de capacidad de los equipos.	I-3-2
	3.2 EXPLOTACIÓN.	I-3-2
	3.2.1 Calendario de carga de trabajo.	I-3-2
	3.2.2 Programación del personal.	I-3-3
	3.2.3 Mantenimiento Preventivo del Material.	I-3-4
	3.2.4 Gestión de Problemas.	I-3-5
	3.2.5 Gestión de Cambios.	I-3-6
	3.2.6 Contabilidad de Costes de Trabajos.	I-3-7
	3.2.7 Procedimiento de Facturación a Usuarios.	I-3-8
	3.2.8 Responsabilidades de Gestión de la Biblioteca de Soportes Magnéticos.	I-3-8
	3.2.9 Sistema de Gestión de la Biblioteca de Soportes.	I-3-9
	3.2.10 Identificación Externa y Control de Soportes Magnéticos.	I-3-10
	3.2.11 Procedimientos de Explotación.	I-3-10
3.3	LOGICAL DE SISTEMA OPERATIVO.	I-3-10
	3.3.1 Selección de Logical de Sistema.	I-3-11

OBJETIVOS DE CONTROL, 1990.

3.3.2	Análisis Coste-Beneficio del Logical de Sistema	I-3-11
3.3.3	Instalación de Cambios en el Logical de Sistema	I-3-11
3.3.4	Mantenimiento del Logical de Sistema	I-3-12
3.3.5	Control de Cambios en el Logical de Sistema	I-3-12
3.3.6	Gestión de Problemas con el Logical de Sistema	I-3-13
3.3.7	Seguridad del Logical de Sistema	I-3-13
3.4	SEGURIDAD LÓGICA Y FÍSICA	I-3-14
3.4.1	Responsabilidad de la Seguridad Lógica y Física	I-3-14
3.4.2	Acceso a las Instalaciones de Ordenadores	I-3-14
3.4.3	Acompañamiento de Visitas	I-3-15
3.4.4	Administración de Palabras de Paso	I-3-15
3.4.5	Informes de Violaciones y Actividad de Seguridad	I-3-16
3.4.6	Restricciones de Acceso Lógico	I-3-16
3.4.7	Seguridad del Acceso a Datos En Línea	I-3-17
3.4.8	Identificación Limitada del Centro de Cálculo	I-3-17
3.4.10	Formación y Concienciación en Procedimientos de Seguridad	I-3-18
3.5	PLANIFICACIÓN ANTE CONTINGENCIAS	I-3-18
3.5.1	Plan de Recuperación de Desastres	I-3-19
3.5.2	Seguridad del Personal y Formación en Procedimientos de Emergencia	I-3-19
3.5.3	Aplicaciones críticas de tratamiento de datos	I-3-19
3.5.4	Recursos de Ordenador Críticos	I-3-20
3.5.5	Restauración de Servicios de Telecomunicación	I-3-21
3.5.6	Respaldo: Del Centro de Cálculo y de los Equipos	I-3-21
3.5.7	Plantilla de Programación para Operaciones de Respaldo	I-3-22
3.5.8	Procedimientos de Recuperación de Ficheros	I-3-22
3.5.9	Consumibles para Recuperación de Desastres	I-3-23
3.5.10	Pruebas del Plan de Recuperación de Desastres	I-3-23
3.5.11	Reconstrucción del Centro de Cálculo del Departamento de Informática	I-3-23
3.5.12	Procedimientos de Respaldo Manual de los Departamentos Usuarios	I-3-24

4. CONTROLES DE APLICACIONES

4.1	CONTROL DE CREACIÓN DE DATOS.	I-4-1
4.1.1	Procedimientos de preparación de datos.	I-4-1
4.1.2	Diseño de documentos fuente.	I-4-1
4.1.3	Control de documentos fuente.	I-4-2
4.1.4	Procedimiento de autorización de entrada de datos. ..	I-4-2
4.1.5	Retención de documentos fuente.	I-4-3

OBJETIVOS DE CONTROL, 1990.

4.2	CONTROL DE ENTRADA DE DATOS.	I-4-4
4.2.1	Procedimientos de conversión y entrada de datos.	I-4-4
4.2.2	Procedimientos de conversión y entrada de datos en línea.	I-4-5
4.2.3	Validación y corrección de datos.	I-4-6
4.3	CONTROLES DE TRATAMIENTOS DE DATOS	I-4-8
4.3.1	Integridad del Tratamiento de Datos	I-4-8
4.3.2	Disposiciones acerca de la integridad del tratamiento de los datos en el logical de aplicación.	I-4-9
4.3.3	Validación y Corrección del Tratamiento de Datos.	I-4-10
4.3.4	Manejo de Errores de Proceso de Datos.	I-4-11
4.4	CONTROL DE SALIDAS DE DATOS	I-4-11
4.4.1	Revisión de salidas	I-4-12
4.4.2	Cuadre y Reconciliación de Salidas	I-4-12
4.4.3	Distribución de salidas.	I-4-13
4.4.4	Gestión de errores en las salidas.	I-4-14
4.4.5	Manejo y retención de las salidas	I-4-15
4.4.6	Disposiciones de seguridad sobre los informes de salida ..	I-4-16

PARTE II: CONTROLES ESPECÍFICOS DE CIERTAS TECNOLOGÍAS

1	CONTROLES EN SISTEMAS INFORMÁTICOS EN ENTORNOS DE BASES DE DATOS	II-1-1
1.1	SISTEMAS DE GESTIÓN DE BASES DE DATOS	II-1-1
1.2	ADMINISTRACIÓN DE DATOS	II-1-2
1.3	RESPONSABILIDAD DE LA ADMINISTRACIÓN DE LAS BASES DE DATOS	II-1-2
1.4	DESCRIPCIÓN DE DATOS Y CAMBIOS DE DATOS	II-1-3
1.5	CONTROL DE ACCESO A DATOS Y DE CONCURRENCIA	II-1-3
1.6	RECUPERACIÓN DEL CONTENIDO DE LAS BASES DE DATOS	II-1-4
1.7	INTEGRIDAD DE LAS BASES DE DATOS	II-1-5
1.8	DISPONIBILIDAD DE LAS BASES DE DATOS	II-1-5
2.-	CONTROLES DE EXPLOTACIÓN EN INFORMÁTICA DISTRIBUIDA Y REDES	II-2-1
2.1	COMPRESIÓN DE LOS OBJETIVOS DE LA DIRECCIÓN	II-2-1
2.2	PLAN DE IMPLANTACIÓN	II-2-1
2.3	ESTANDÁRES DE CONTROL PARA LA RED	II-2-2
2.4	OPCIONES DE CONTROL DEL MATERIAL Y LOGICAL	II-2-3
2.5	DISTRIBUCIÓN DE BASES DE DATOS	II-2-3

OBJETIVOS DE CONTROL, 1990.

2.6 ESTÁNDARES DE DATOS PARA LA RED	II-2-4
2.7 ACCESO A DATOS DE LA RED	II-2-5
2.8 MECANISMO DE REVISIÓN DE DATOS DE LA RED	II-2-5
2.9 DISPOSICIONES SOBRE RESPALDO DE MATERIAL Y LOGICAL	II-2-6
2.10 EXPLOTACIÓN DE LA RED	II-2-7
2.11 LOGICAL DE COMUNICACIONES	II-2-8
2.12 ACCESO AL LOGICAL DE SISTEMA OPERATIVO DE LA RED	II-2-8
2.13 ACCESO A LAS INSTALACIONES DE EXPLOTACIÓN DE LA RED	II-2-9
2.14 CIFRA (CRIPTOGRAFÍA) DE DATOS	II-2-10
2.15 SEGURIDAD DE LA RED	II-2-10
2.16 REVISIONES DE SEGURIDAD DE LA RED	II-2-11
2.17 DOCUMENTACIÓN Y FORMACIÓN DEL PERSONAL DE OPERACIÓN DE LA RED	II-2-12
2.18 REVISIÓN POST-IMPLANTACIÓN DE LA RED	II-2-12
2.19 CONTROL DE FUNCIONAMIENTO DE LA RED	II-2-13
2.20 PLANES DE CONTINGENCIA DE EXPLOTACIÓN DE LA RED	II-2-14
3 CONTROLES SOBRE EL INTERCAMBIO ELECTRÓNICO DE DATOS	II-3-1
3.1 OBJETIVOS DE GESTIÓN	II-3-1
3.2 ANÁLISIS COSTE-BENEFICIO	II-3-1
3.3 SELECCIÓN DE SUMINISTRADORES DE SERVICIOS	II-3-2
3.4 TÉRMINOS CONTRACTUALES	II-3-2
3.5 IDENTIFICACIÓN Y VERIFICACIÓN DE USUARIOS	II-3-4
3.6 CONTROLES DE PROTECCIÓN DE PROGRAMAS	II-3-5
3.7 CONTROLES SOBRE EL LOGICAL DE APLICACIÓN	II-3-5
3.8 MANUAL DE USUARIO	II-3-6
3.9 FACTURAS POR EL SERVICIO	II-4-1
4 CONTROLES EN LAS OPERACIONES EN LAS OFICINAS DE SERVICIOS	II-4-1
4.1 EL CONTRATO CON LA OFICINA DE SERVICIOS	II-4-1
4.2 MANUALES DE USUARIO	II-4-1
4.3 REVISIÓN POR TERCEROS	II-4-1
4.4 ESTABILIDAD FINANCIERA DE LA OFICINA DE SERVICIOS	II-4-2
4.5 EL PLAN DE RECUPERACIÓN DE DESASTRES INFORMÁTICOS DE LOS USUARIOS	II-4-2
5 CONTROLES SOBRE ORDENADORES PERSONALES	II-5-1
5.1 POLÍTICAS DE DIRECCIÓN	II-5-1
5.2 CRITERIOS de ADQUISICIÓN DE ORDENADORES PERSONALES	II-5-2
5.3 DESARROLLO Y ADQUISICIÓN DE LOGICAL DE APLICACIÓN	II-5-3
5.4 DOCUMENTACIÓN DE LOS PROGRAMAS	II-5-4

5.5 BIBLIOTECA DE PROGRAMAS APLICACIÓN OBTENIDOS BAJO LICENCIA	II-5-5
5.6 FICHEROS DE DATOS	II-5-6
5.7 FICHEROS DE TRANSACCIONES	II-5-7
5.8 ACCESO A RECURSOS DE ORDENADORES PERSONALES.	II-5-7
5.9 DOCUMENTACIÓN DE LOS PROCESOS	II-5-8
5.10 CARACTERÍSTICAS DE CONTROL	II-5-8
5.11 TRANSMISIÓN DE DATOS CON ORDENADORES PERSONALES	II-5-8
5.12 RESPALDO Y SEGURIDAD DE PROGRAMAS Y DATOS	II-5-9
5.13 SEGURIDAD FÍSICA DE LOS EQUIPOS	II-5-9
5.14 OPERACIÓN DE LOS ORDENADORES PERSONALES	II-5-10
5.15 REVISIÓN POR LA DIRECCIÓN	II-5-11
6 CONTROLES SOBRE REDES DE ÁREA LOCAL	II-6-1
6.1 POLÍTICAS SOBRE GESTIÓN DE REDES	II-6-1
6.2 SEGURIDAD LÓGICA DE LA RED	II-6-1
6.3 SEGURIDAD FÍSICA LA RED	II-6-2
6.4 SOPORTE Y GESTIÓN LA RED	II-6-2
6.5 CONTROL DE CAMBIOS EN LA RED	II-6-3
7.1 SELECCIÓN DE LA APLICACIÓN	II-7-1
7.2 DISEÑO	II-7-1
7.3 ADQUISICIÓN DEL CONOCIMIENTO	II-7-2
7.4 PRUEBAS	II-7-2
7.5 MANTENIMIENTO	II-7-2
7.6 FORMACIÓN Y SUPERVISIÓN LOS USUARIOS	II-7-3
7.7 ACCESO	II-7-3

APÉNDICES

ÍNDICE ANALÍTICO

APÉNDICE A: CONTRIBUYENTES A ESTA PUBLICACIÓN

APÉNDICE B: GLOSARIO INGLÉS - ESPAÑOL UTILIZADO

. . .

PREÁMBULO

**El Papel del Auditor Informático
en el desarrollo y revisión de controles
para sistemas informatizados.**

Esta publicación es el resultado del análisis, la revisión, y la ampliación profundos de una publicación editada en 1.983 bajo el título **Control Objectives: Controls In A Computer Environment: Objectives, Guidelines, and Audit Procedures (Objetivos de Control: Controles en un Entorno Informatizado: Objetivos, Directivas y Procedimientos de Auditoría)**. Esta edición de 1.990 desarrolla la concepción de la versión de 1.983 ampliando su cobertura a una variedad de tecnologías informáticas y sus correspondientes controles. Esta publicación está concebida para ofrecer a la alta dirección, a los miembros de consejos de administración, a la dirección de sus Departamentos de Informática y a sus Auditores Informáticos una guía actualizada y completa referente a lo que pudiera denominarse la buena práctica en la creación, operación, verificación y evaluación de controles en un entorno informatizado. Debiera resultar también útil a otras personas con un interés continuado en evaluar la calidad y eficacia general de tales controles. Dichos grupos adicionales incluyen -sin quedar limitados a-- reguladores, legisladores, aseguradores de siniestros y responsabilidades, investigadores y formadores en este campo, y el gran público. El objetivo de quienes han contribuido a la organización y presentación de este material es crear un estándar con el que puedan medirse los esfuerzos para establecer y mantener el control de sistemas informatizados.

1. La naturaleza de "Control"

En un entorno informatizado, se define el control para que abarque las políticas, procedimientos, prácticas, y estructuras organizativas que aseguren la adecuación de la gestión de los activos informáticos y la fiabilidad de las actividades de sistemas de información. Cuando el control es efectivo, todas las partes interesadas en -- o afectadas por -- la operación de los sistemas de información en cuestión debieran tener una confianza razonable en que se satisfacen las expectativas de la dirección, técnicos, profesionales y público respecto del proceso de datos en el entorno en cuestión. Especificar la naturaleza y ámbito del control en todos los aspectos de sus actividades -- incluyendo los sistemas de información -- es cometido de la alta dirección de una organización. El Auditor Informático tiene que contestar dos preguntas fundamentales en el entorno informático:

- * ¿Es realista la especificación del control?
- * ¿Cuán efectivas son las medidas de control?

El control es, por su propia naturaleza, relativo más que absoluto. En algunos casos está limitado por las expectativas de la alta dirección de una organización y por otras partes interesadas. También puede estar limitado por el coste de mantener un

control en particular cuando se compara con el daño que puede ocasionarse -- o la pérdida en que puede incurrirse -- bien por un fallo al implantar el control, bien por el fallo de dicho control en funcionar adecuadamente. Muy rara vez una medida de control específica resultará eficaz por sí misma. La eficacia del control, en un entorno informático específico, o para un sistema o actividad informáticos en concreto, es, en última instancia, función de la eficacia de todos los controles pertinentes a dicho sistema o actividad.

El papel de la alta dirección de una organización es ejercer un juicio razonable y prudente para definir buenas prácticas de control en un entorno de sistemas informáticos, para evaluar la eficacia del modo en que tales medidas se han aplicado, y para remediar cualesquiera deficiencias que se identifiquen, bien en su estructura, bien en la forma en que han sido aplicadas. (El incumplimiento de alguna práctica o procedimiento específico contenidos en esta publicación no debiera utilizarse para imputar a la dirección un fallo en el uso de la prudencia o de la precaución en el cumplimiento de sus obligaciones. Antes bien el auditor informático debiera reconocer que un control específico que puede ser generalmente considerado aconsejable implantar en un entorno informático, en ocasiones puede no ser aconsejable establecerlo en un entorno organizativo específico).

El papel del auditor informático, en esta situación, es actuar como un delegado de la alta dirección para examinar las prácticas de control y evaluar su eficacia. Es también función del auditor informar --en base a lo que ha corroborado mediante su examen-- sobre las conclusiones alcanzadas en el proceso de evaluación del control, y recomendar medidas adecuadas para corregir cualesquiera deficiencias que pudieran haber sido descubiertas durante este examen y evaluación. Con total independencia de esta actividad de revisión de controles, es también apropiado que el auditor informático aconseje a la alta dirección de la organización respecto de la necesidad de ciertos controles en el desarrollo o revisión de los sistemas de información existentes y de los procedimientos de tratamiento de la información. Es también apropiado que el Auditor Informático evalúe cuán bien se han materializado dichas recomendaciones en el sistema o procedimiento acabado y que informe a la alta dirección sobre las conclusiones alcanzadas como resultado de esta evaluación. En ninguno de esos casos puede suponerse que la independencia del auditor se haya comprometido en medida alguna por estas actividades.

2. Estructura de esta publicación

La generación de información en una organización viene dictada por las necesidades de sus diversos departamentos y unidades y se lleva a cabo mediante el establecimiento de distintas concepciones o visiones de los datos para sus departamentos y unidades. En este documento, la revisión de los controles sobre esta información se ha dividido en varias secciones, para permitir al auditor revisar la eficiencia y eficacia de tales controles desde diversas perspectivas, y no todas ellas serán útiles en una revisión en concreto. Las secciones están organizadas en dos partes. La Parte I cubre controles generales y de aplicación. Estas áreas de control están interrelacionadas y versan sobre aquellas funciones de control que son comunes a cualquier entorno informático. La parte II complementa a la parte I y

versa sobre aquellos aspectos del control que son propios de aplicaciones específicas de la tecnología de los sistemas de información. Habida cuenta de que uno de los propósitos de este documento era que cada sección fuera autocontenida, con un mínimo de referencias cruzadas a material presentado en otras partes del documento, entre las diversas secciones tienen lugar ciertas pequeñas duplicidades y solapamientos. Se suministra, sin embargo, un índice del contenido de esta publicación para ayudar al lector a determinar cuándo diversos temas se tratan en sus diferentes secciones. Este índice señalará también las áreas de solapamiento.

Los contenidos de esta publicación están organizados con un formato estructurado. Cada una de las secciones se presenta como una serie de Objetivos de Control y declaraciones de Directivas de Auditoría. En los primeros, el verbo "debería" identifica una acción que la dirección debiera razonablemente emprender o exigir de otros. En el segundo tipo de declaraciones el verbo "debe" identifica una acción que se espera emprenda un Auditor Informático. Cada Directiva de Auditoría se complementa con una secuencia de procedimientos de auditoría (denominados también pasos), que el auditor informático debiera seguir para identificar la existencia y eficacia de los Objetivos de Control significativos. Los verbos que describen acciones del auditor en estos procedimientos o pasos han sido impresos en *itálicas negritas* para agilizar la utilización de dichos pasos por el auditor. El seguir tales pasos solamente, sin embargo, no excluye la necesidad de que el Auditor Informático desarrolle programas de trabajo de auditoría exhaustivos para cada examen o revisión emprendidos. Se reconoce que en muchos entornos de auditoría no es posible examinar cada centro de cálculo, cada departamento usuario, o cada aplicación informática. Así pues, en esta publicación se sugiere que cuando sea significativo, el auditor seleccione una muestra de la población más amplia a examinar. Para que una Directiva de Auditoría específica sea aplicable, deben de estar implantados los Objetivos de Control pertinentes. Cuando esa condición no se da, el Auditor Informático debiera considerar recomendar a la alta dirección de la organización que se implante dicho control.

El material contenido en esta publicación puede citarse en informes u otros documentos de la siguiente forma: Parte/Sección/Punto. Así, por ejemplo, la Parte 1/Sección 2/Punto 2.5, se referirá a todos los objetivos de control, directivas de auditoría y procedimientos de auditoría relacionados con el examen por el Auditor Informático del papel y de la responsabilidad de los individuos implicados en el Desarrollo e Implantación de una aplicación informática en una organización, empleando la metodología de ciclo de vida del desarrollo de sistemas propia de la organización.

Esta versión de Objetivos de Control se publica en formato de hojas cambiables, para facilitar el proceso continuado de revisión y ampliación de este documento. Téngase presente que Objetivos de Control está disponible en varios idiomas.

3. Terminología empleada en esta publicación

En esta publicación se emplean de una forma particular un cierto número de términos.

* **Logical ("software") de programas de aplicación.**

Se refiere a aplicaciones informáticas y se emplea indistintamente para programas de aplicación y para logical de aplicación.

* **Intercambio electrónico de datos.**

Se refiere a una transmisión organizada, ordenador a ordenador, de datos especificados, utilizando estructuras de mensajes y formatos acordados entre socios comerciales, o agencias gubernativas a través de una red de comunicación pública o privada, a efectos de contabilidad, administración, comercio, transporte y fiscalidad.

* **Sistema experto.**

Se refiere a una aplicación informática que se usa como una guía para la ejecución de rutinas de trabajo complejas o como una ayuda a la toma de decisiones. Un sistema experto puede ser parte integral de otra aplicación o puede operar independientemente. Un sistema experto tiene dos componentes: una base de conocimientos y un motor de inferencia, o concha. La base de conocimientos contiene reglas generales o ejemplos usados por expertos humanos en la toma de decisiones. La concha es un programa de ordenador que brinda a los usuarios del sistema experto decisiones sobre circunstancias específicas, basadas en la información contenida en la base de conocimientos del sistema experto.

* **Departamento de Informática.**

Se refiere a la unidad dentro de una organización que suministra -- o coordina el uso de -- diversos servicios de tratamiento de la información. El término concreto utilizado para identificar a esta unidad variará de una organización otra.

* **Ordenador Personal (Microordenador).**

Identifica un dispositivo que, en general, opera de modo independiente y que consta de un teclado u otra unidad de entrada autocontenida, algún tipo de memoria interna, una unidad central de proceso, una pantalla y una impresora de salida. Un ordenador personal es normalmente capaz de procesar por sí mismo cantidades significativas de datos. Puede usarse, en algunos casos, para comunicar directamente con otros ordenadores personales y para compartir datos y tareas con ellos. En

otras ocasiones un ordenador personal puede emplearse como un terminal para comunicar con un ordenador central que tenga capacidad de tratamiento de datos compatible.

* **Organización.**

Se refiere a cualquier entidad empresarial o pública --tanto si tiene fines lucrativos como si se trata de una agencia o institución no lucrativa.

* **Alta dirección.**

Se refiere a aquellos ejecutivos de la organización que pueden formular especificaciones generales de políticas y procedimientos que definen la forma en que ciertas actividades serán desarrolladas por la organización y sus componentes. Los títulos usados para identificar a los individuos que pertenecen a esta categoría varían de una organización a otra.

* **Sistema o sistema de información.**

Se refiere a una colección interrelacionada de programas de proceso de datos, datos, procedimientos de tratamiento de la información, así como a los documentos y registros asociados con su uso.

* **Ciclo de vida del desarrollo de sistemas.**

Se refiere a un método estructurado a ser seguido para el diseño, creación, y operación de un sistema de información. Las fases definidas para esta metodología varían de una organización a otra, pero en esta publicación se supone que consisten en una iniciación del proyecto, un estudio de viabilidad, el propio proceso de diseño, el desarrollo e implantación del diseño del sistema, su operación y mantenimiento, y una post-implantación del sistema, ya en la fase concluyente del ciclo.

* **Departamento usuario.**

Se refiere a una de las secciones de la organización que utiliza informática en su trabajo y al que el Departamento de Informática proporciona alguna forma de servicio de tratamiento de datos.

Michael Donahue
Vice President, Research
The EDP Auditors Foundation

Beldon Menkus
Editor

Zella G. Ruthberg
Assistant Editor

NOTA DEL TRADUCTOR

La terminología informática en castellano - como otra mucha terminología técnica - está muy marcada por el inglés y - en muchos casos - los términos varían mucho de unos a otros entornos. (Piénsese, por ejemplo, en el caso de *interficie*, el término homologado en el ámbito oficial de la Comunidad Europea, para referirse a *interfaz* o *interfase* o *interface*).

En toda la traducción se ha hecho un esfuerzo considerable para lograr la máxima uniformidad en el vertido de palabras y expresiones, y en la elección de términos generalizados en castellano. El Apéndice B recoge el Glosario Inglés - Español con las correspondencias de términos que hemos utilizado.

* * *

PARTE I: CONTROLES GENERALES Y DE APLICACIONES

CONTROLES DE GESTIÓN

CONTENIDO

1	CONTROLES DE GESTIÓN	I-1-1
1.1	PLANIFICACIÓN DEL DEPARTAMENTO DE INFORMÁTICA	I-1-1
1.1.1	Planificación a largo plazo de la organización	I-1-1
1.1.2	El Comité de Planificación o de Dirección del Departamento de Informática	I-1-1
1.1.3	Planificación a largo plazo del Departamento de Informática	I-1-2
1.1.4	Planificación a corto plazo de la organización y del Departamento de Informática	I-1-3
1.1.5	Revisión de la planificación de la organización y del Departamento de Informática	I-1-3
1.2	POLÍTICAS, ESTÁNDARES Y PROCEDIMIENTOS	I-1-4
1.2.1	Políticas	I-1-4
1.2.2	Estándares	I-1-4
1.2.3	Procedimientos	I-1-4
1.3	RESPONSABILIDADES ORGANIZATIVAS Y GESTIÓN DE PERSONAL	I-1-5
1.3.1	La ubicación del Departamento de Informática en la organización.	I-1-5
1.3.2	Descripción de responsabilidades dentro del Departamento de Informática.	I-1-5
1.3.3	Separación de funciones	I-1-6
1.3.4	Descripción de puestos del Departamento de Informática	I-1-6
1.3.5	Selección de personal	I-1-7
1.3.6	Procedimientos de acreditación de seguridad del personal.	I-1-7
1.3.7	Procedimientos de baja del personal.	I-1-8
1.3.8	Formación del personal.	I-1-9
1.3.9	Evaluación de la ejecutoria del empleado en el puesto.	I-1-9
1.4	GARANTÍA DE CALIDAD DEL DEPARTAMENTO DE INFORMÁTICA.	I-1-10
1.4.1	Responsabilidad de la garantía de calidad (G.C.)	I-1-10
1.4.2	Aspectos organizativos de la función de garantía de calidad. (GC).	I-1-10

PARTE I - 1. CONTROLES DE GESTION.

1.4.3	Cualificación del personal de garantía de calidad (GC).	I-1-11
1.4.4	Plan de revisión de la garantía de calidad (GC).	I-1-11
1.4.5	Revisión por garantía de calidad (GC) del logro de los objetivos del Departamento de Informática.	I-1-12
1.4.6	Revisión por garantía de calidad (GC), del cumplimiento de los estándares y procedimientos del Departamento de Informática.	I-1-13
1.4.7	Revisión por garantía de calidad (GC) de los controles de sistemas	I-1-13
1.4.8	Revisión por garantía de calidad (GC) de otros aspectos de las funciones del Departamento de Informática	I-1-13
1.4.9	Informes de las revisiones de garantía de calidad (GC).	I-1-14
1.5	LA FUNCIÓN DE AUDITORÍA INTERNA.	I-1-14
1.5.1	El estatuto de auditoría interna	I-1-14
1.5.2	Competencia técnica del personal de auditoría interna.	I-1-15
1.5.3	Formación continuada del personal de auditoría interna.	I-1-16
1.5.4	Rendimiento del trabajo de auditoría interna.	I-1-16
1.5.5	Informes de la función de auditoría interna.	I-1-16
1.6	ESPECIFICACIONES DE ORIGEN EXTERNO.	I-1-17

* * *

1 CONTROLES DE GESTIÓN

1.1 PLANIFICACIÓN DEL DEPARTAMENTO DE INFORMÁTICA

El Departamento de Informática debería tener planes a corto y largo plazo, a fin de asegurar su contribución al éxito en el logro de los objetivos generales de la organización. Dichos planes deberían ser congruentes con los planes más generales de la organización para lograr sus propios objetivos.

1.1.1 Planificación a largo plazo de la organización

• **Objetivo de Control.**

Los planes a largo plazo del Departamento de Informática deberían cubrir aspectos relacionados con su contribución al logro de los objetivos a largo plazo de la organización. La dirección de la organización, al más alto nivel, debería participar en el desarrollo del plan a largo plazo del Departamento de Informática. La participación de la alta dirección debería asegurar que el plan del Departamento está integrado en el plan general de la organización.

• **Directiva de Auditoría.**

Debe revisarse el plan a largo plazo de la organización. Debe prestarse especial consideración a cuán bien integrada está en el plan general la parte relativa al Departamento de Informática. Deben **evaluarse** la eficiencia y eficacia de la contribución del Departamento de Informática.

1. **Revisar** el proceso de planificación de la organización para **determinar** el nivel de implicación en el mismo de la alta dirección.

2 **Revisar** partes significativas de las actas de las reuniones del Consejo de Administración, del Comité Ejecutivo, del

Comité de Dirección o del Comité de Política de Empresa de la organización, para **identificar** los objetivos a largo plazo de la organización.

3. **Entrevistar** a los directivos significativos en cuanto a la fijación de políticas de la organización, a fin de **identificar** y comentar las estrategias a largo plazo relacionadas con los objetivos del Departamento de Informática.

4. **Revisar** los planes a largo plazo documentados y los objetivos del Departamento de Informática para **determinar** su compatibilidad con los objetivos generales de la organización.

5. **Entrevistar** a las principales unidades usuarias para **determinar** la consistencia de las estrategias a largo plazo de la organización y del usuario, en lo que se refiera a los objetivos del Departamento de Informática.

6. **Determinar** la eficiencia y eficacia del plan a largo plazo del Departamento de Informática.

1.1.2 El Comité de Planificación o de Dirección del Departamento de Informática

• **Objetivo de Control.**

La alta dirección de la organización debería designar un comité de planificación o de dirección que supervise las actividades del Departamento de Informática. Entre los miembros del comité debería haber representantes de la alta dirección, del Departamento de Informática y de la dirección de los departamentos usuarios.

• **Directiva de Auditoría.**

Debe verificarse la existencia de un comité de planificación o de dirección

PARTE I - 1. CONTROLES DE GESTION.

del Departamento de Informática, y debe **revisarse** su composición. Debe **dejarse establecido** que incluye a directivos de departamentos usuarios.

1 **Determinar** la existencia de un comité de planificación o de dirección del Departamento de Informática, y **revisar** su estatuto.

2 **Identificar** la composición del comité y **verificar** que la dirección de los departamentos usuarios está representada en el mismo.

3 **Revisar** la definición de responsabilidades y funciones del comité.

4 **Revisar** las actas de las reuniones del comité, así como sus planes documentados, para **determinar** la naturaleza y extensión de su papel en el proceso de planificación del Departamento de Informática.

5 **Determinar** si los objetivos del Departamento de Informática y del comité son consistentes con el - y contribuyen al - logro de los planes y objetivos generales de la organización.

1.1.3 Planificación a largo plazo del Departamento de Informática

* Objetivo de Control.

Los planes a largo plazo para el Departamento de Informática deberían ser congruentes con - y estar integrados en - los planes a largo plazo de la alta dirección. Deberían identificar los objetivos de la organización, los cambios de la misma, los avances tecnológicos, y las disposiciones reglamentarias.

* Directiva de Auditoría.

Deben revisarse los planes a largo plazo para el Departamento de Informática y compararse con los planes a largo plazo de la alta dirección, a fin de determinar su congruencia, así como su compatibilidad con los cambios organizativos, avances tecnológicos y disposiciones reglamentarias previstos.

1 **Revisar** los planes a largo plazo del Departamento de Informática para **determinar** su congruencia con los objetivos generales de la organización y proyecciones de crecimiento relacionadas con éstos.

2 **Revisar** las fuentes de documentación usadas para el desarrollo de los planes a largo plazo y previsiones del Departamento de Informática, y **verificar** que la base de esas proyecciones es razonable.

3 **Entrevistar** a los directivos clave del Departamento de Informática para lograr una comprensión de su conocimiento tanto de los objetivos del Departamento cuanto de los generales de la organización.

4 **Explorar** la comprensión, por parte de los directivos clave del Departamento de Informática, de los avances tecnológicos potenciales, y de los cambios probables en disposiciones reglamentarias aplicables, y las necesidades de conocimientos / pericia del personal, y **evaluar** su preparación para reaccionar a tales cambios, en caso de que se produjeran.

5 **Determinar** si se han distribuido a otras unidades de la organización copias de los planes del Departamento de Informática y **evaluar** el grado de aceptación de los mismos por dichas unidades.

6 **Revisar** los organigramas y descripciones de puestos vigentes en el Departamento de Informática para **determinar** su conformidad general con los planes a largo plazo del Departamento.

7 **Identificar** avances tecnológicos específicos y **determinar** si han sido incorporados a los planes a largo plazo del Departamento de Informática.

8 **Determinar** que se han identificado y localizado en el organigrama del Departamento de Informática los nuevos conocimientos / pericia exigidos por los avances tecnológicos previstos.

9. **Identificar** las disposiciones reglamentarias de importancia para la organización en general y **asegurar** que los planes del Departamento de Informática son congruentes con esas disposiciones.

10. **Evaluar** el nivel de eficiencia y eficacia con que se han integrado en el plan a largo plazo del Departamento de Informática los avances tecnológicos, los cambios en las disposiciones reglamentarias y las necesidades de conocimientos / pericia.

1.1.4 Planificación a corto plazo de la organización y del Departamento de Informática

- **Objetivo de Control.**

Los planes a corto plazo de la alta dirección para la organización deberían asegurar que los recursos adecuados del Departamento de Informática se asignan de forma congruente con los planes a corto plazo generales de la organización.

- **Directiva de Auditoría.**

Deben revisarse los planes a corto plazo preparados por la alta dirección de la organización. Debe evaluarse la adecuación de los recursos asignados al Departamento de Informática, así como la congruencia y compatibilidad de los planes a corto plazo del Departamento con los correspondientes planes a largo plazo.

1. **Revisar** los planes a corto plazo de la alta dirección e **identificar** los recursos que se asignan a corto plazo al Departamento de Informática.

2. **Evaluar** la adecuación de los recursos asignados al Departamento de Informática a corto plazo.

3. **Asegurar** la congruencia entre los planes a corto plazo y los planes a largo plazo del Departamento de Informática.

1.1.5 Revisión de la planificación de la organización y del Departamento de Informática

- **Objetivo de Control.**

Deberían suministrarse informes a la alta dirección que les permitieran revisar el progreso de la organización hacia los objetivos identificados.

- **Directiva de Auditoría.**

Deben revisarse los informes de gestión para obtener pruebas de que la alta dirección y el comité de planificación o de dirección del Departamento de Informática revisan y coordinan las actividades del Departamento.

1. **Determinar** la fecha y naturaleza de la última revisión por la dirección de los planes a largo y corto plazo.

2. **Inspeccionar** los informes de progreso de la dirección, en busca de pruebas de logro de objetivos.

3. **Revisar** la frecuencia y precisión de los informes sobre proyectos relacionados con los planes a largo y corto plazo.

4. **Comparar** los gastos reales con los presupuestados para **identificar** diferencias significativas.

5. **Entrevistar** a usuarios y dirección para **determinar** si se han alcanzado como se deseaba los objetivos específicos. **Revisar**, si procede, los informes de gestión específicos y las respuestas a los mismos relativas a aquellas áreas en que no se han alcanzado los objetivos.

6. **Determinar**, en ausencia de informes formales, si hay una comunicación informal adecuada de las actividades del Departamento de Informática a la alta dirección.

PARTE I - 1. CONTROLES DE GESTION.

1.2 POLÍTICAS, ESTÁNDARES Y PROCEDIMIENTOS

Debería haber políticas, estándares y procedimientos, que sirvieran de base para la planificación, control y evaluación por la dirección de las actividades del Departamento de Informática.

1.2.1 Políticas

- **Objetivo de Control.**

La alta dirección debería desarrollar, y comunicar a todos los afectados, directivas de política que definiesen la relación entre el Departamento de Informática y los departamentos usuarios.

- **Directiva de Auditoría.** Determinar la existencia y adecuación de declaraciones de política por parte de la alta dirección, y confirmar que han sido comunicadas a los departamentos pertinentes.

1. **Revisar** las declaraciones de política de la alta dirección, y **determinar** que están actualizadas.

2. **Determinar** que las declaraciones de política de la alta dirección se han comunicado a las direcciones tanto del Departamento de Informática cuanto de los departamentos usuarios.

3. **Revisar** y **evaluar** la integración de las directivas de política de la alta dirección en el estatuto del Departamento de Informática y de los principales departamentos usuarios.

1.2.2 Estándares

- **Objetivo de Control.**

Deben definirse, coordinarse, mantenerse, y comunicarse a todo el personal afectado, estándares que regulen la adquisición de recursos, el diseño, desarrollo y modificación y explotación de

sistemas del Departamento de Informática.

- **Directiva de Auditoría.**

Deben revisarse los estándares que regulen la adquisición de recursos, el diseño, desarrollo y modificación y explotación de sistemas del Departamento de Informática.

1. **Evaluar** el proceso de desarrollo, aprobación, distribución y actualización de los estándares aplicables al Departamento de Informática.

2. **Revisar** los estándares aprobados, para **evaluar** la extensión de su documentación formal, su calidad, vigencia y cuán completos son.

3. **Revisar** los manuales de operaciones y procedimientos aplicables para **determinar** que los procedimientos relativos a la adquisición de recursos del Departamento de Informática cumplen los estándares que regulan dichas adquisiciones.

4. **Revisar** los manuales de operaciones y procedimientos tanto en el Departamento de Informática cuanto en los departamentos usuarios para **determinar** su cumplimiento de los estándares relativos al diseño, desarrollo y modificación de sistemas de información.

5. **Revisar** los manuales de operaciones y procedimientos del Departamento de Informática para **determinar** que las declaraciones de procedimiento relativas a la operación de dicho Departamento cumplen los estándares que regulan dicha operación.

1.2.3 Procedimientos

- **Objetivo de Control.**

Deben establecerse, coordinarse, mantenerse y comunicarse a todos los departamentos afectados, procedimientos que describan la forma y las responsabilidades de ejecutoria para regular las relaciones entre el Departamento de

Informática y los departamentos usuarios.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos operativos relativos a las responsabilidades de ejecutoria en las relaciones entre departamentos usuarios y el Departamento de Informática.

1. **Evaluar** el proceso por el que se desarrollan, aprueban, distribuyen y actualizan las declaraciones de procedimientos.

2. **Revisar** los manuales de operaciones y procedimientos del Departamento de Informática para **apreciar** la extensión de la documentación formal, del Departamento, su calidad, grado de vigencia y cuán completa es. **Evaluar** la adecuación de las instrucciones escritas que se refieren a las actividades del Departamento de Informática.

3. **Revisar** los manuales de operaciones y procedimientos de los departamentos usuarios para **apreciar** la extensión de su documentación formal su calidad, grado de vigencia y cuán completa es. **Evaluar** la adecuación de las instrucciones escritas que cubren las relaciones de este departamento con el Departamento de Informática.

4. **Entrevistar** al personal tanto del Departamento de Informática cuanto de los departamentos usuarios para **apreciar** su comprensión de los procedimientos aprobados.

1.3 RESPONSABILIDADES ORGANIZATIVAS Y GESTIÓN DE PERSONAL

El Departamento de Informática debería ser lo bastante importante en la jerarquía de la organización para permitirle lograr sus objetivos generales establecidos y promover su independencia operativa de los departamentos usuarios. Para promover la utilización efectiva de los

recursos humanos del Departamento, y para facilitar la evaluación del desempeño dentro de la función Informática, deberían emplearse técnicas de gestión de personal sólidas.

1.3.1 La ubicación del Departamento de Informática en la organización.

• **Objetivo de Control.**

La alta dirección debería colocar el Departamento de Informática lo bastante alto en la estructura organizativa como para asegurar su independencia de los departamentos usuarios.

• **Directiva de Auditoría.**

Apreciar lo adecuado de la ubicación del Departamento de Informática en la estructura de la organización y evaluar el grado de independencia del Departamento respecto de los departamentos usuarios.

1. **Revisar** la ubicación del Departamento de Informática en la jerarquía de la organización y **apreciar** su independencia de los departamentos usuarios.

2. **Entrevistar** al Director del Departamento de Informática para **determinar** su apreciación de la independencia del Departamento respecto de los departamentos usuarios.

1.3.2 Descripción de responsabilidades dentro del Departamento de Informática.

• **Objetivo de Control.**

Deberían estar descritas las principales unidades organizativas que constituyen el Departamento de Informática, así como perfiladas y documentadas sus responsabilidades.

• **Directiva de Auditoría.**

Revisar las descripciones de las principales unidades organizativas que constituyen el Departamento de Informática y

PARTE I - 1. CONTROLES DE GESTION.

apreciar la adecuación de dicha documentación.

1. **Identificar** las principales unidades organizativas que constituyen el Departamento de Informática examinando los organigramas pertinentes.

2. **Revisar** los manuales de procedimientos pertinentes para **determinar** que las responsabilidades asignadas a cada una de las principales unidades organizativas están enunciadas adecuadamente, y que los procedimientos de evaluación de su ejecutoria están adecuadamente presentados.

3. **Entrevistar** al personal supervisor de cada una de las principales unidades organizativas del Departamento para **determinar**:

a. que su comprensión de las responsabilidades asignadas a la unidad, el desempeño esperado y los procedimientos de evaluación se corresponden con los descritos en los manuales

b. que su responsabilidad para la introducción y uso de nueva tecnología ha sido definida claramente dentro del Departamento de Informática (por ejemplo, la distinción entre el grupo de apoyo a usuarios finales y grupo de desarrollo de sistemas) y entre el Departamento y los departamentos usuarios.

1.3.3 Separación de funciones

* **Objetivo de Control.**

La alta dirección debe establecer una separación de funciones dentro del Departamento de Informática, por ejemplo entre desarrollo de sistemas y explotación, entre explotación y control de datos, y entre administración de bases de datos y desarrollo de sistemas.

* **Directiva de Auditoría.**

Hay que apreciar la adecuación de la separación de funciones dentro del Departamento de Informática.

1. **Examinar** los organigramas y descripciones de puestos pertinentes para **determinar** que en el Departamento de Informática existe la adecuada separación de funciones, incluyendo la separación entre los siguientes pares de unidades organizativas principales:

a. desarrollo de sistemas y explotación

b. explotación y control de datos

c. administración de bases de datos y desarrollo de sistemas.

2. **Revisar** las descripciones de tareas u otra documentación referente a las tareas para **determinar** que se mantiene la separación de funciones deseada.

3. **Observar** las actividades del personal del Departamento de Informática para **confirmar** la naturaleza y extensión del cumplimiento de esta separación de funciones deseada.

4. **Revisar** las asignaciones significativas de suplencias o apoyos para **asegurar** que se mantiene la adecuada separación de funciones.

1.3.4 Descripción de puestos del Departamento de Informática

* **Objetivo de Control.**

Las descripciones de puestos del Departamento de Informática deben mantenerse por escrito y perfilar claramente tanto la autoridad cuanto la responsabilidad. Las descripciones deberían incluir definiciones de los conocimientos / pericia técnicos requeridos para las posiciones relevantes y deberían ser adecuadas para ser empleadas en evaluaciones de ejecutoria.

* **Directiva de Auditoría.**

Deben revisarse las descripciones de puestos del Departamento de Informática.

tica en cuanto a su adecuación y claridad, a la inclusión de las descripciones de los conocimientos /pericia técnicos y en cuanto a su utilidad como una base para evaluar las ejecutorias.

1. **Obtener y revisar** las descripciones de puestos empleadas dentro del Departamento de Informática para **apreciar** su adecuación y claridad.
2. **Comparar** dichas descripciones con las responsabilidades en vigor de quienes ocupan tales posiciones, para **determinar** la precisión de las declaraciones.
3. **Determinar**, mediante entrevistas y análisis, que la línea directa de autoridad asociada con la posición es conmensurable con las responsabilidades del interesado.
4. **Apreciar** los cambios significativos en la organización y en la descripción de puestos en cuanto a su adecuación y precisión en el contexto de los objetivos y políticas actuales del Departamento de Informática.
5. **Entrevistar** al personal del Departamento de Informática para **determinar** que las descripciones de sus puestos les han sido adecuadamente comunicadas y que el interesado las entiende.
6. **Revisar** las fechas de validez de las descripciones de puestos, para **asegurar** que están en vigor.
7. **Determinar** que las descripciones de puestos incluyen descripciones de conocimientos / pericia técnicos. **Evaluar** cuán adecuadas son esas descripciones.
8. **Determinar** que, en las descripciones de puestos, los textos que describen los conocimientos / pericia técnicos del interesado están en vigor.

1.3.5 Selección de personal

• **Objetivo de Control.**

Las prácticas de contratación y promoción del personal deberían basarse en

criterios objetivos y deberían contemplar la formación, la experiencia y la responsabilidad.

• **Directiva de Auditoría.**

Debe apreciarse la adecuación del proceso de selección de personal en lo que respecta al Departamento de Informática.

1. **Identificar y evaluar** los métodos empleados para cubrir vacantes, tales como el uso de promociones internas, firmas externas de selección de personal, u otros métodos apropiados.

2. **Evaluar** la adecuación de los criterios empleados para reclutar y seleccionar miembros de la plantilla del Departamento de Informática, y para ello:

a. **entrevistar** a la dirección del Departamento en lo que respecta a estos criterios

b. **revisar** los documentos apropiados, como descripciones de puestos, en cuanto a si son claros y completos.

3. **Revisar** la adecuación de las políticas de selección empleadas por el Departamento de Relaciones Laborales y por el Departamento de Informática.

1.3.6 Procedimientos de acreditación de seguridad del personal.

• **Objetivo de Control.**

El personal del Departamento de Informática, antes de ser contratado, debería ser objeto de una acreditación de seguridad.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos relativos a la acreditación de seguridad del

PARTE I - 1. CONTROLES DE GESTION.

personal del Departamento de Informático.

1. **Revisar** los documentos relativos a la política de contratación de personal de la organización para **determinar** que se han establecidos procedimientos de acreditación de seguridad.

2. **Entrevistar** a los responsables de contratar al personal del Departamento de Informática para **determinar** que hay implantados procedimientos adicionales de acreditación de seguridad.

3. **Revisar** las fichas del personal del Departamento de Informática para **determinar** que:

a. se han seguido los procedimientos de investigación de seguridad asociados con la contratación del nuevo personal, de conformidad con los estándares de la organización

b. se han seguido procedimientos periódicos de investigación de seguridad del personal.

4. **Determinar** que los procedimientos de investigación de seguridad seguidos son congruentes con las leyes aplicables relativas a la protección de la intimidad.

1.3.7 Procedimientos de baja del personal.

* Objetivo de Control.

Deberían establecerse procedimientos pertinentes para la baja del personal del Departamento de Informática y para asegurar la protección de los recursos constituidos por los ordenadores y los ficheros de la organización.

* Directiva de Auditoría.

Debe revisarse la adecuación de los procedimientos de baja del personal del Departamento de Informática para asegurar la protección de los recursos

constituidos por los ordenadores y los ficheros de la organización.

1. **Revisar** los procedimientos escritos relativos al personal para **determinar** que los procedimientos de baja de empleados aplicables al personal del Departamento de Informática son, generalmente, conformes con:

a. al personal del Departamento de Informática que causa baja, se le paga, en lugar de permitirle que trabaje durante el período hasta que la baja sea plenamente efectiva

b. a los empleados que causan baja se les requiere para que retornen todos los documentos y tarjetas de identificación suministrados por la organización; en concreto aquéllos que pudieran ser empleados para lograr un acceso no autorizado, después de la baja, a instalaciones o datos que tienen asignado algún nivel de seguridad

c. al personal del Departamento de Informática al que se comunica la baja, se le acompaña hasta el exterior de los locales de la organización de forma inmediata y sin darle la oportunidad de dañar las instalaciones informáticas o los ficheros de la organización

d. después de la baja del empleado concreto, se cambian inmediatamente las palabras de paso u otros dispositivos de control empleados para lograr acceso a los recursos informáticos.

2. Determinar que estos procedimientos son seguidos de forma congruente, procediendo a:

a. **entrevistar** a la dirección del Departamento de Informática

b. **revisar** las fichas de personal referentes a empleados que hayan causado baja recientemente

c. **revisar** los registros de los sistemas de seguridad de accesos físicos y de control de accesos al ordenador para **comprobar** que los accesos de los empleados que han causado baja se han desactivado adecuadamente.

1.3.8 Formación del personal.

*** Objetivo de Control.**

Debería darse orientación a los empleados, desde su contratación, y también formación continuada para mantener sus conocimientos / pericia.

*** Directiva de Auditoría.**

Deben evaluarse los procedimientos de orientación y formación al personal de plantilla del Departamento de Informática.

1. **Revisar** el manual del empleado para **determinar** que a los nuevos empleados se les brindan programas de orientación que cubren los requisitos de seguridad y control.

2. **Asegurar** que a los nuevos empleados, durante las sesiones de orientación, se les hace tomar plena conciencia de los objetivos de la organización y del Departamento.

3. **Determinar** que los programas de formación de la organización son congruentes con los requisitos mínimos sugeridos por las organizaciones profesionales para el Departamento de Informática.

4. **Entrevistar** a miembros de la plantilla del Departamento de Informática para determinar que están informados tanto de los programas de informática patrocinados por la organización como de los requisitos de formación continua de las organizaciones profesionales, en áreas relacionadas con las del Departamento, de las cuales son miembros o a través de las cuales reciben certificaciones u homologaciones profesionales.

5. **Revisar** los calendarios de formación, las descripciones de los cursos, los métodos y técnicas de formación, para **determinar** que tales programas son adecuados para mantener las necesidades actuales y a largo plazo, tanto de la organización cuanto de los empleados.

6. **Determinar** que en el programa de formación se incluyen cursos específicamente orientados a aumentar la comprensión de los objetivos de control del Departamento de Informática respecto a la gestión, las aplicaciones, y la explotación (u operación).

7. **Entrevistar** a miembros de la plantilla del Departamento de Informática para **determinar** la eficacia de la formación que se les ha brindado.

8. **Comparar** las fichas de formación de los miembros de la plantilla del Departamento de Informática con sus exigencias de conocimientos / pericia, para **evaluar** cuán adecuada y actualizada es la formación que están recibiendo.

1.3.9 Evaluación de la ejecutoria del empleado en el puesto.

*** Objetivo de Control.**

Debería evaluarse, de forma periódica, la ejecutoria del empleado en comparación con estándares establecidos y con responsabilidades específicas del puesto.

*** Directiva de Auditoría.**

Deben de evaluarse los métodos de evaluación del desempeño de los miembros de la plantilla del Departamento de Informática.

1. **Revisar** los procedimientos establecidos para **determinar** que se efectúan evaluaciones periódicas del desempeño del empleado de conformidad con dichos procedimientos.

2. **Entrevistar** a la dirección del Departamento de Informática para **determinar** tanto su comprensión cuanto su uso de los métodos de evaluación del desem-

PARTE I - 1. CONTROLES DE GESTION.

peño de los empleados establecidos por la organización.

3. **Entrevistar** a miembros escogidos de la plantilla del Departamento de Informática, para **determinar**:

- a. su comprensión de los estándares de rendimiento establecidos
- b. su comprensión de las responsabilidades singulares de su puesto
- c. que los resultados de las evaluaciones han sido comunicados a los empleados de forma congruente con los procedimientos establecidos.

1.4 GARANTÍA DE CALIDAD DEL DEPARTAMENTO DE INFORMÁTICA.

Debería asegurarse la calidad de los servicios prestados por el Departamento de Informática mediante el establecimiento de una función independiente dentro del Departamento dedicada a mantener estándares de calidad establecidos.

1.4.1 Responsabilidad de la garantía de calidad (G.C.)

* **Objetivo de Control.**

La responsabilidad de llevar a cabo la función de GC debería asignarse a miembros de la plantilla del Departamento de Informática. Cuando sea adecuado, debería establecerse un grupo independiente de GC, dentro del Departamento. La única responsabilidad de dicho grupo debería ser el realizar funciones de GC.

* **Directiva de Auditoría.**

Debe realizarse un análisis para determinar la necesidad de establecer un grupo formal de GC.

1. **Evaluar** el nivel general de satisfacción de los usuarios con el servicio brindado por el Departamento de Informática.

2. **Revisar** los registros existentes de problemas, peticiones de programas, sistemas y de servicios, pendientes de cumplimentar. **Determinar** la presteza con que el Departamento de Informática responde a tales peticiones.

3. **Determinar** si las necesidades de los departamentos usuarios se han satisfecho de forma general, mediante la introducción de nuevos equipos, comunicaciones, programas de sistemas y programas de aplicación en los últimos años.

4. **Determinar** si se cumplen de forma congruente los estándares y procedimientos del Departamento de Informática.

5. **Apreciar**, basándose en la extensión de los hallazgos negativos de los pasos 1,2,3 y 4 anteriores, si debería establecerse un grupo independiente de GC en el Departamento de Informática.

1.4.2 Aspectos organizativos de la función de garantía de calidad. (GC).

* **Objetivo de Control.**

Cuando exista un grupo independiente de GC en el Departamento de Informática, dicho grupo debería tener un estatuto escrito aprobado por un nivel de dirección adecuado. La función de este grupo debería ser apoyada por la dirección tanto del Departamento de Informática cuanto de los departamentos usuarios. Si lo adecuado es que sean sólo una o dos personas las que hayan de desarrollar la función de GC, debería existir una documentación clara de sus responsabilidades, aprobada por la dirección. Aun así, es necesario el apoyo tanto de la dirección del Departamento de Informática cuanto de la de los departamentos usuarios.

* **Directiva de Auditoría.**

Deben revisarse los aspectos organizativos de la función de GC del Departamento de Informática.

1. **Determinar** que se ha publicado un estatuto debidamente aprobado del grupo de GC o un documento describiendo las responsabilidades de la actividad de GC de una o dos personas y que describe los deberes, responsabilidades, autoridad e imputabilidad del grupo o de la persona o personas.
2. **Determinar** que el estatuto o documento está complementado por descripciones de tareas actualizadas que incluyen una descripción de responsabilidades.
3. **Verificar** que a la función de garantía de calidad no se le ha asignado ninguna de las responsabilidades operativas del Departamento de Informática.
4. **Verificar** que la función de GC informa a un nivel de dirección adecuado que asegurará que las recomendaciones se lleven a cabo.
5. **Determinar** que la función de GC recibe adecuado apoyo económico para completar eficazmente sus responsabilidades.
6. **Revisar** documentación seleccionada recabada al personal de GC para **apreciar** la amplitud y profundidad de su cobertura de las actividades del Departamento de Informática.
7. **Entrevistar** a la dirección tanto de los usuarios cuanto del Departamento de Informática para **determinar** que brindan apoyo a la misión y al trabajo del personal de GC y **obtener** pruebas para documentar sus afirmaciones.

1.4.3 Cualificación del personal de garantía de calidad. (GC).

• **Objetivo de Control.**

En la función GC del Departamento de Informática debería haber pericia adecuada en los temas de sistemas, controles y comunicaciones.

• **Directiva de Auditoría.**

Deben revisarse las cualificaciones del personal de GC del Departamento de Informática.

1. **Determinar** que el personal adscrito a la función GC del Departamento de Informática tiene un conocimiento adecuado de la explotación del sistema y de lenguajes de programación.
2. **Verificar** que el personal asignado a la función GC del Departamento de Informática tiene un amplio conocimiento de las operaciones empresariales, de los conceptos de control interno y de los controles de proceso de las aplicaciones.
3. **Determinar** que usuarios clave forman parte del equipo de GC o que son consultados periódicamente durante el proceso de GC.
4. **Determinar** que el personal asignado a la función GC del Departamento de Informática recibe entrenamiento y formación adecuados, de forma continua.
5. **Asegurar** que el supervisor de la función GC del Departamento de Informática tiene pericia adecuadas de supervisión, comunicación y gestión de proyectos.
6. **Determinar** que la función GC del Departamento de Informática ha sido adecuadamente dotada de plantilla, en base a los resultados de los pasos 1,2,3,4, y 5 anteriores, señalando cualquier deficiencia y su impacto en la eficacia de la función GC.

1.4.4 Plan de revisión de la garantía de calidad. (GC).

• **Objetivo de Control.**

Deberían desarrollarse, mantenerse y estandarizarse planes generales de garantía de calidad, calendarios y procedimientos, dentro del Departamento de Informática, para fijar criterios para el trabajo del personal de GC del departa-

PARTE I - 1. CONTROLES DE GESTION.

mento. Tales planes, calendarios y procedimientos deberían usarse para establecer la congruencia de los resultados alcanzados por dicho personal y para brindar una base para la gestión de las funciones de GC del departamento.

- **Directiva de Auditoría.**

Debe apreciarse lo apropiado de los planes de revisión de GC en el Departamento de Informática.

1. **Evaluar** los planes de revisión de GC existentes en el Departamento de Informática, así como los calendarios y procedimientos. **Apreciar** su aplicabilidad y oportunidad comparándolos con las revisiones realmente llevadas a cabo.
2. **Determinar** que las revisiones de GC del Departamento de Informática han sido programadas de conformidad con las prioridades establecidas por la dirección del Departamento.
3. **Determinar** que el personal de GC del Departamento de Informática usa programas especiales de auditoría para las funciones de investigación que pueden ser fácilmente automatizadas.
4. **Verificar** que, tras cada revisión principal de GC, los planes de revisión pertinentes y los procedimientos se evalúan y mejoran, en la medida que proceda, para **contribuir** a la mejora de la eficacia de futuras revisiones.
5. **Verificar** que inmediatamente después de la terminación de cada revisión de GC, los requisitos de nivel de pericia y experiencia para llevar a cabo la siguiente revisión se incorporan a los planes de GC del Departamento de Informática.

1.4.5 Revisión por garantía de calidad (GC) del logro de los objetivos del Departamento de Informática.

- **Objetivo de Control.**

Las responsabilidades de GC deberían incluir una revisión de cómo sistemas y aplicaciones concretos han jugado un papel en el logro de los objetivos del Departamento.

- **Directiva de Auditoría.**

Debe evaluarse la documentación relacionada con las revisiones por el personal de GC de cómo sistemas y aplicaciones concretos han jugado un papel en el logro de los objetivos del Departamento.

1. **Revisar** los resultados de la revisión por el personal de GC de las aplicaciones. **Entrevistar** al personal de GC que llevó a cabo la revisión y **determinar** que las especificaciones originales del usuario sirvieron como base fundamental para la evaluación de la aplicación que se revisó.
2. **Verificar** que esta revisión incluyó la ejecución de pruebas de calidad tanto del diseño de sistemas pertinentes cuanto de las actividades de programación y que las especificaciones de diseños pertinentes se cumplieron.

1.4.6 Revisión por garantía de calidad (GC), del cumplimiento de los estándares y procedimientos del Departamento de Informática.

• **Objetivo de Control.**

Las responsabilidades asignadas al personal de GC deberían incluir una revisión del cumplimiento general de los estándares y procedimientos del Departamento.

• **Directiva de Auditoría.**

Debe revisarse la documentación relacionada con la revisión por el personal de GC, del cumplimiento general de los estándares y procedimientos del Departamento.

1. **Determinar** que el personal de GC ha desarrollado una metodología para revisar y documentar el cumplimiento de los estándares y procedimientos del Departamento.

2. **Asegurar** que el personal de GC emplea consistentemente esta metodología u otros procedimientos estándar.

3. **Verificar** que los informes del personal de GC describen de forma específica el cumplimiento de los estándares y procedimientos del Departamento.

1.4.7 Revisión por garantía de calidad (GC) de los controles de sistemas

• **Objetivo de Control.**

Las responsabilidades asignadas al personal afecto a GC deberían incluir una revisión de los controles generales del sistema.

• **Directiva de Auditoría.**

Debe revisarse la documentación relacionada con los análisis de los controles generales del sistema por el personal de GC.

1. **Identificar** los controles de sistemas que fueron seleccionados para las revisiones de GC y **apreciar** que tales revisiones eran razonables y completas.

2. **Verificar** que los informes suministrados por el personal de GC incluyen específicamente los resultados de los hallazgos en las revisiones de control.

1.4.8 Revisión por garantía de calidad (GC) de otros aspectos de las funciones del Departamento de Informática

• **Objetivo de Control.**

Las responsabilidades asignadas al personal de GC deberían incluir una revisión de otros aspectos de las funciones del Departamento que merezcan la atención de la dirección.

• **Directiva de Auditoría.**

Deben revisarse las directivas relativas a las responsabilidades del personal de GC en la revisión de otros aspectos de las funciones del Departamento de Informática.

1. **Determinar** que las responsabilidades asignadas al personal de GC incluyen una revisión de lo siguiente:

- a. especificaciones reglamentarias y legales
- b. la calidad de diseño del sistema
- c. la calidad de la programación y las operaciones
- d. la adecuación de las pruebas de sistemas y programas
- e. los conocimientos y pericia del personal del Departamento
- f. la extensión y naturaleza de la participación de los usuarios en las actividades de desarrollo y mantenimiento de sistemas del departamento
- g. la calidad de la documentación de sistemas y programas

PARTE I - 1. CONTROLES DE GESTION.

h. la calidad de los datos y de la información.

2. **Seleccionar** informes producidos por el personal de GC relativos a las áreas enumeradas en el paso 1 de la sección 1.4.8 anterior y **apreciar** la calidad del trabajo llevado a cabo en las revisiones.

1.4.9 Informes de las revisiones de garantía de calidad (GC).

• **Objetivo de Control.**

Deberían elaborarse y presentarse a la dirección de los usuarios y del Departamento de Informática, informes de las revisiones de garantía de calidad.

• **Directiva de Auditoría.**

Debe evaluarse la calidad y utilidad de los informes preparados por el personal de GC del Departamento de Informática.

1. **Seleccionar** informes relativos a distintos tipos de revisiones de GC y asegurar que los mismos:

- a. comunican eficazmente los hallazgos significativos de la revisión
- b. están escritos claramente y con una estructura orientada a la gestión
- c. incluyen un resumen para la dirección con una breve introducción, los objetivos generales, el informe general, los hallazgos significativos y su impacto en el negocio
- d. incluyen una sección de apoyo, detallada, que contiene recomendaciones.

2. **Entrevistar** al personal de GC que llevó a cabo las revisiones y **determinar** su apreciación de los resultados. **Comparar** su apreciación con los contenidos de los informes pertinentes.

3. **Verificar** que la dirección de los departamentos usuarios y del Depar-

tamento de Informática recibieron en un plazo adecuado copias de los informes de GC. **Determinar** su apreciación del valor de los informes.

1.5 LA FUNCIÓN DE AUDITORÍA INTERNA.

Debería establecerse, de forma complementaria a otros elementos de los controles de gestión, una función de auditoría interna, con suficiente competencia técnica, independencia, y autoridad para efectuar revisiones objetivas de los controles de los sistemas de información y para preparar y presentar informes de sus hallazgos y recomendaciones de mejora en todas las áreas funcionales del entorno de sistemas de informática de la organización.

1.5.1 El estatuto de auditoría interna

• **Objetivo de Control.**

La alta dirección de la organización debería establecer un estatuto de la función de auditoría interna. Este documento debería esbozar la responsabilidad, autoridad e imputabilidad de la función de auditoría interna. Debería revisarse periódicamente el estatuto para asegurar que se mantienen la independencia, autoridad e imputabilidad de la función de auditoría interna.

• **Directiva de Auditoría.**

Debe efectuarse una revisión periódica del estatuto de la función de auditoría interna de la organización.

1. **Determinar** que la función de auditoría interna ha sido asignada a una unidad separada dentro de la organización, basándose en sus responsabilidades según las establezca el Estatuto de auditoría.

2. **Revisar** dicho estatuto para **asegurar** que a la función de auditoría interna se le ha asignado independencia en la de-

terminación de las áreas en las cuales emprender revisiones de auditoría.

3. **Determinar** que este estatuto brinda una estructura para informar de los hallazgos de auditoría y de las recomendaciones en una línea de comunicación directa con la alta dirección.

4. **Asegurar** que el estatuto de la función de auditoría interna de la organización incluye declaraciones que establecen su autoridad para obtener acceso ilimitado a registros manuales y automáticos, a activos y al personal necesario para llevar a cabo sus revisiones.

5. **Asegurar** que las responsabilidades asignadas a la función de auditoría interna de la organización incluyen la revisión periódica de todos los aspectos de las actividades del Departamento de Informática, y en concreto:

- a. gestión y administración
- b. desarrollo y mantenimiento de sistemas
- c. explotación de proceso de datos y apoyo a explotación
- d. servicios técnicos.

1.5.2 Competencia técnica del personal de auditoría interna.

- **Objetivo de Control.**

Los auditores responsables de la revisión de las actividades del Departamento de Informática de la organización deberían ser técnicamente competentes y poseer los conocimientos/pericia necesarios para efectuar eficaz y eficientemente tales revisiones.

- **Directiva de Auditoría.**

Deben revisarse las actividades de gestión de la función de auditoría interna de la organización, a fin de asegurar la competencia técnica de los auditores asignados a revisiones de actividades del Departamento de Informática y apli-

caciones informatizadas que se procesan en el entorno de sistemas de información.

1. **Asegurar** que los auditores asignados a la revisión de actividades del Departamento de Informática y a las aplicaciones informatizadas tienen suficiente preparación o conocimiento de las áreas que se revisan para **asegurar** la independencia tanto de sus trabajos cuanto de sus hallazgos.

2. Si el personal disponible de auditoría interna carece de la competencia técnica suficiente para asegurar la independencia de sus trabajos y de sus hallazgos, **determinar** que la dirección de la función de auditoría interna de la organización contrata a consultores internos que poseen competencia suficiente para efectuar revisiones de las actividades y de las aplicaciones en ordenador del Departamento de Informática.

PARTE I: CONTROLES GENERALES Y DE APLICACIONES

CONTROLES DE DESARROLLO, ADQUISICIÓN Y
MANTENIMIENTO DE SISTEMAS INFORMÁTICOS

CONTENIDO

2	CONTROLES DE DESARROLLO, ADQUISICIÓN Y MANTENIMIENTO DE SISTEMAS INFORMÁTICOS.	I-2-1
2.1	METODOLOGÍA Y RESPONSABILIDAD DEL CICLO DE VIDA DEL DESARROLLO DE SISTEMAS.	I-2-1
2.1.1	Metodología de ciclo de vida del desarrollo de sistemas.	I-2-1
2.1.2	Papeles y responsabilidades.	I-2-2
2.1.3	Actualización del ciclo de vida del nuevo sistema.	I-2-2
2.2	INICIACIÓN DEL PROYECTO.	I-2-3
2.2.1	Definición del proyecto.	I-2-3
2.2.2	Participación del departamento usuario en la iniciación del proyecto.	I-2-4
2.2.3	Composición y responsabilidades del equipo de proyecto. ..	I-2-4
2.2.4	Definición de las necesidades de información.	I-2-5
2.2.5	Aprobación del proyecto.	I-2-5
2.3	ESTUDIO DE VIABILIDAD	I-2-6
2.3.1	Formulación de cursos de acción alternativos.	I-2-6
2.3.2	Estudio de viabilidad tecnológica	I-2-6
2.3.3	Estudio de viabilidad económica	I-2-7
2.3.5	Aprobación del proyecto.	I-2-8
2.3.6	Plan director del proyecto.	I-2-9
2.3.7	Control de costes.	I-2-9
2.4	FASE DE DISEÑO.	I-2-10
2.4.1	Metodología de diseño	I-2-10
2.4.2	Definición y documentación de las especificaciones de salida.	I-2-10
2.4.3	Documentación y definición de especificaciones de entrada.	I-2-11
2.4.4	Definición y documentación de especificaciones de ficheros.	I-2-11
2.4.5	Documentación y definición de especificaciones de proceso.	I-2-12
2.4.6	Especificaciones de programas.	I-2-12
2.4.7	Diseño de la recogida de datos fuente.	I-2-13
2.4.8	Diseño de controles y seguridad.	I-2-13
2.4.9	Diseño de pistas de auditoría.	I-2-13
2.4.10	Aprobación del diseño.	I-2-14
2.4.11	Estándares de documentación de programas.	I-2-15
2.4.12	Plan de validación, verificación y pruebas.	I-2-16
2.5	DESARROLLO E IMPLANTACIÓN.	I-2-16
2.5.1	Objetivos de programación.	I-2-17
2.5.2	Descripción de la narrativa del programa.	I-2-17
2.5.3	Paquetes de logical de aplicación.	I-2-18

PARTE I - 2. CONTROLES DE DESARROLLO, ADQUISICION Y MANTENIMIENTO

2.5.4	Contratación de programas de aplicación a medida.	I-2-18
2.5.5	Manual de operaciones y mantenimiento.	I-2-19
2.5.6	Manual de usuario.	I-2-20
2.5.7	Plan de Formación.	I-2-21
2.5.8	Estándares de prueba de programas.	I-2-21
2.5.9	Estándares de prueba de sistemas.	I-2-23
2.5.11	Evaluación de los resultados de las pruebas.	I-2-23
2.5.12	Plan de Conversión.	I-2-24
2.5.13	Pruebas en Paralelo.	I-2-24
2.5.14	Prueba de aceptación final.	I-2-24
2.6	EXPLOTACIÓN Y MANTENIMIENTO.	I-2-25
2.6.1	Procedimientos de control de explotación.	I-2-25
2.6.2	Control de costes.	I-2-25
2.6.3	Modificaciones al sistema.	I-2-26
2.6.4	Re-evaluación de las especificaciones de usuario.	I-2-26
2.7	REVISIÓN POST-IMPLANTACIÓN.	I-2-26
2.7.1	Plan de revisión post-implantación.	I-2-27
2.7.2	Evaluación de resultados.	I-2-27
2.7.3	Evaluación del cumplimiento de las especificaciones de usuario.	I-2-28
2.7.4	Análisis de evaluación coste-beneficio.	I-2-28
2.7.5	Evaluación del cumplimiento de los estándares de desarrollo.	I-2-28
2.7.6	Informe sobre los hallazgos de la revisión post-implantación. .	I-2-29

* * *

2 CONTROLES DE DESARROLLO, ADQUISICIÓN Y MANTENIMIENTO DE SISTEMAS INFORMÁTICOS.

2.1 METODOLOGÍA Y RESPONSABILIDAD DEL CICLO DE VIDA DEL DESARROLLO DE SISTEMAS.

El proceso que la organización sigue para el desarrollo, adquisición y mantenimiento de sistemas de información debería intentar alcanzar la eficacia del sistema, economía y eficiencia, integridad de los datos, protección de los recursos y cumplimiento con las leyes y regulaciones. El empleo de una metodología eficaz de ciclo de vida del desarrollo de sistemas debería brindar a la alta dirección de la organización una garantía razonable de que dichos objetivos serán alcanzados.

2.1.1 Metodología de ciclo de vida del desarrollo de sistemas.

* **Objetivo de Control.**

La alta dirección de la organización debería publicar una declaración escrita de política estableciendo una metodología de ciclo de vida del desarrollo de sistemas, como medio para estructurar y controlar el proceso de desarrollo o adquisición de sistemas informatizados.

* **Directiva de Auditoría.**

Debe revisarse la metodología de ciclo de vida del desarrollo de sistemas de la organización.

1. **Revisar** el ciclo de vida del desarrollo de sistemas actualmente en uso en la organización y determinar si se usa un enfoque estructurado congruente con conceptos y prácticas generalmente aceptadas en el sector informático.

2. **Evaluar** si cada fase de la metodología de ciclo de vida del desarrollo de sistemas en la organización tiene como resultado un producto acabado medible que es sometida a una revisión adecuada y aprobación antes de que el pro-

yecto pase a la fase siguiente. Determinar si las especificaciones de planificación de cada fase dentro de la metodología están claramente identificadas.

3. **Determinar** si la metodología de ciclo de vida del desarrollo de sistemas en la organización brinda un mecanismo para controlar los cambios que pueden tener lugar a lo largo de la vida del proyecto. Revisar la metodología para determinar la importancia que en ella se concede a la seguridad y a los controles internos.

4. **Determinar** la familiaridad, grado de formación y experiencia que las plantillas tanto del Departamento de Informática cuanto de los departamentos usuarios tienen en el uso de la metodología de ciclo de vida del desarrollo de sistemas de la organización.

5. **Determinar** si los requisitos de la metodología de ciclo de vida del desarrollo de sistemas de la organización son obligatorios u orientativos y aprecian la flexibilidad del uso de la metodología bajo condiciones, cambios tales como por ejemplo en proyectos grandes y pequeños. Determinar si se permiten desviaciones de la metodología, bajo que circunstancias puede esto ocurrir y si tales desviaciones han de ser documentadas y probadas.

6. **Determinar** si la metodología de ciclo de vida del desarrollo de sistemas de la organización incluye especificaciones de programación y documentación y estándares para usuarios, programadores, personal de desarrollo de sistemas, y para la plantilla de operaciones del Departamento de Informática.

7. **Cerciorarse** de si la metodología de ciclo de vida del desarrollo de sistemas contempla la aplicación de tecnología de bases de datos, el impacto de las telecomunicaciones, informática de "usuario final", y el empleo de lenguajes de Cuarta Generación y de prototipos, así como la selección e instalación de productos de logical comerciales.

8. **Determinar** si la metodología de ciclo de vida del desarrollo de sistemas de la organización está siendo realmente utilizada en el desarrollo del logical. Aprender la adecuación, actualización y adaptabilidad a cambios tecnológicos de la metodología, para determinar el grado de riesgo que pueda existir en el logical desarrollado con adhesión a la misma.

2.1.2 Papeles y responsabilidades.

• **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas adoptada por la organización debería establecer los papeles, y responsabilidades del Departamento de Informática, de los departamentos usuarios, y de otros, en cuanto a planificación, desarrollo, revisión, implantación y auditoría del producto final del proceso de desarrollo del sistema.

• **Directiva de Auditoría.**

Debe revisarse la asignación de papeles y responsabilidades en los diversas fases de la metodología de ciclo de vida del desarrollo de sistemas de la organización.

1. **Determinar** si la alta dirección de la organización ha publicado un estatuto o una declaración escrita de política que defina los papeles y responsabilidades en el proceso de desarrollo de sistemas. Los papeles definidos deberían incluir los de comité de planificación o dirección, los del departamento usuario, el equipo de proyecto, el grupo de garantía interna y el personal de operaciones del Departamento de Informática.

2. **Evaluar** si cada fase de la metodología del ciclo de vida del desarrollo de sistemas de la organización permite a los grupos que participan en el proceso de desarrollo decidir a pasar a la fase siguiente o a modificar los objetivos o dirección del esfuerzo de desarrollo o a dar por terminado el proyecto.

3. **Determinar** si los papeles y responsabilidades de equipo de proyecto están claramente enunciados en la metodología del ciclo de vida del desarrollo de sistemas de la organización. **Apreciar** la extensión con la cual el director del proyecto puede tomar decisiones sobre el empleo de plantilla y otros recursos, la programación de las actividades, las técnicas del desarrollo del sistema.

4. **Determinar** cómo han de ser seleccionados los representantes de los departamentos usuarios en los equipos de proyecto y la extensión de la participación prevista de los departamentos usuarios en el proyecto de desarrollo. **Verificar** que las responsabilidades que les asigna son congruentes con sus necesidades.

5. **Determinar** la extensión, bajo la metodología de desarrollo de sistema de la organización de la participación prevista del grupo de garantía de calidad del Departamento de Informática y del personal de Auditoría Interna de la dirección en el proceso de desarrollo del sistema.

6. **Revisar** las disposiciones contenidas en la metodología del ciclo de vida del desarrollo de sistemas de la organización en cuanto a cosas tales como el conservar una separación de funciones, evitar conflictos de interés, y asegurar adecuados controles de supervisión.

2.1.3 Actualización del ciclo de vida del nuevo sistema.

• **Objetivo de Control.**

La metodología del ciclo de vida del desarrollo de sistemas usada por la organización debería revisarse periódicamente por la alta dirección de la organización para asegurar que sus disposiciones reflejan técnicas generalmente aceptadas hoy en día y procedimientos.

• **Directiva de Auditoría.**

Deben examinarse los mecanismos de la organización para revisar la urgencia y adecuación de las disposiciones de su

metodología de ciclo de vida del desarrollo de sistemas.

1. **Determinar** si existe un mecanismo para revisar periódicamente la adecuación y vigencia de la metodología de ciclo de vida del desarrollo de sistemas de la organización y examinar evaluaciones anteriores de dicha metodología.
2. **Determinar** si se conserva un registro escrito de las modificaciones o revisiones de las disposiciones contenidas en la metodología de ciclo de vida del desarrollo de sistemas de la organización.
3. **Determinar**, mediante entrevistas a los representantes de departamentos de sistemas, si están satisfechos con la forma en que la metodología se usa actualmente.

2.2 INICIACIÓN DEL PROYECTO.

La metodología de ciclo de vida del desarrollo de sistemas debería permitir la participación de los departamentos usuarios en la identificación de la naturaleza y ámbito generales de un proyecto de desarrollo de sistemas. Las especificaciones de información a cumplir por el sistema nuevo o modificado deberían definirse cuidadosamente por escrito y el desarrollo de un sistema propuesto debería aprobarse antes de que comience el proceso de desarrollo.

2.2.1 Definición del proyecto.

• Objetivo de Control.

La metodología de ciclo de vida del desarrollo de sistemas de la organización establecen la creación de una definición claramente enunciada por escrito de la naturaleza y ámbito de cada proyecto de desarrollo de sistema antes de que comience el trabajo en el proyecto.

• Directiva de Auditoría.

Deben examinarse las disposiciones establecidas en la metodología de ciclo de vida del desarrollo de sistemas de la or-

ganización para establecer por escrito el ámbito y propósito de un desarrollo de sistema antes de que comience el trabajo en el mismo.

1. **Determinar** que la metodología de ciclo de vida del desarrollo de sistemas de la organización establece la presentación por escrito de una solicitud de proyecto y que la misma incluye informaciones tales como:

- a. razones para abordar el proyecto, incluyendo: (1) enunciado del problema a resolver), (2) una expresión de la necesidad de un sistema de información nuevo o modificado en términos de la mejora de la capacidad de la organización para alcanzar sus objetivos), (3) un análisis de las deficiencias en los sistemas actuales aplicables), (4) las oportunidades que se obtendrían por un aumento de la economía o de la eficiencia de la operación), y (5) la necesidad de control interno o de seguridad que sería satisfecha por el proyecto
- b. el entorno del proyecto
- c. el ámbito del proyecto
- d. las restricciones al proyecto
- e. los beneficios a obtener mediante el proyecto
- f. quién es el patrocinador o usuario del proyecto.

2. **Determinar** que la metodología de ciclo de vida del desarrollo de sistemas de la organización establece que las peticiones de proyecto sean revisadas en cuanto a su congruencia con la planificación aprobada del Departamento de Informática o con el plan para el año en curso del comité de dirección.

3. **Determinar**, revisando los registros referentes a proyectos de desarrollo de sistemas de información, selección, que las peticiones se prepararon, se revisaron, y aprobaron de conformidad con la

PARTE I - 2. CONTROLES DE DESARROLLO, ADQUISICION Y MANTENIMIENTO

metodología de ciclo de vida del desarrollo de sistemas.

2.2.2 Participación del departamento usuario en la iniciación del proyecto.

* **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debería establecer la participación por parte de la dirección del departamento usuario afectado en la definición y autorización de un proyecto de desarrollo o modificación de un sistema de información.

* **Directiva de Auditoría.**

Deben revisarse las disposiciones en la metodología de ciclo de vida del desarrollo de sistemas de la organización en cuanto a la participación por la dirección y del departamento usuario afectado en la definición y autorización de una modificación o desarrollo de sistemas de informática.

1. **Revisar** las actas del comité de planificación o de dirección del Departamento de Informática y los planes relativos a proyectos escogidos para determinar la extensión de la participación de los departamentos usuarios en el trabajo de los comités y en general en el proceso de definir y autorizar el desarrollo o modificaciones de sistemas informáticos.

2. **Revisar** los presupuestos de departamentos usuarios seleccionados para identificar la asignación de tiempo por miembros de la plantilla del departamento a los proyectos de modificación o desarrollo de sistemas significativos del Departamento de Informática.

2.2.3 Composición y responsabilidades del equipo de proyecto.

* **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debería especificar las bases para asignar a individuos de la plantilla como

miembros del equipo de proyecto y definir las responsabilidades de los distintos miembros del proyecto.

* **Directiva de Auditoría.**

Deben revisarse las disposiciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización para asignar a individuos como miembros de equipos de proyectos y definir sus responsabilidades.

1. **Identificar**, para proyectos seleccionados de desarrollo o modificación de sistemas de información, la persona a cargo del proyecto, los nombres de todos los miembros del equipo de proyecto y sus responsabilidades.

2. **Evaluar** los antecedentes y las cualificaciones de estos individuos como una medida de la adecuación de su asignación a tareas específicas de proyectos bajo la metodología de ciclo de vida del desarrollo de sistemas de la organización.

3. **Determinar** si la dirección de los departamentos usuarios implicados en el desarrollo o modificaciones de proyectos significativos de sistemas informáticos ha nombrado a individuos de sus departamentos para participar en los equipos pertinentes del proyecto y evaluar si tales personas tienen:

a. una comprensión profunda de las necesidades de información del departamento a ser satisfechas por el producto final planificado en este esfuerzo

b. la habilidad para trabajar con los otros miembros del equipo de proyecto

c. la misma comprensión del ámbito y objetivos del proyecto que tienen los demás miembros del equipo.

2.2.4 Definición de las necesidades de información.

* **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debería establecer que las necesidades de información a ser satisfechas por el sistema actual o el nuevo o modificado deberían ser claramente definidas antes de que se apruebe un proyecto de desarrollo o modificación.

* **Directiva de Auditoría.**

Deben revisarse las disposiciones de la metodología de ciclo de vida del desarrollo de sistemas que requieren que las necesidades de informática a ser satisfechas por el sistema actual o el propuesto o modificado sean definidas antes de que se apruebe un proyecto de desarrollo o modificación.

1. **Cerciorarse**, para proyectos seleccionados de desarrollo o modificación de sistemas de información de que se han cumplidos los requisitos de la metodología de ciclo de vida del desarrollo de sistemas de la organización, respecto a documentación. En particular, **asegurar** que:

- a. las descripciones del sistema actual son adecuadas para servir de base para el estudio de las necesidades del sistema propuesto, nuevo o modificado
- b. que se han identificado claramente aquellos aspectos del sistema actual que serían cambiados por el serían cambiados por el sistema propuesto
- c. que el Departamento de Informática ha evaluado, en cuanto a cuan completo son, a su congruencia, y a la viabilidad del tratamiento de la información dichas especificaciones de información
- d. que esas especificaciones de información han sido revisadas y aprobadas por la dirección de los departa-

mentos usuarios implicados en el proyecto de desarrollo.

2.2.5 Aprobación del proyecto.

* **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debería contener disposiciones para la aprobación por miembros asignados de la dirección del trabajo llevado a cabo en cada fase del ciclo antes de que comience el trabajo en la fase siguiente.

* **Directiva de Auditoría.**

Debe revisarse lo dispuesto por la metodología de ciclo de vida del desarrollo de sistemas de la organización en cuanto a la aprobación por miembros designados de la dirección del trabajo ejecutado en cada fase del ciclo antes de que comience el trabajo en la fase siguiente.

1. **Determinar**, mediante una revisión de los registros referentes a proyectos de desarrollo o modificación de sistemas informáticos seleccionados, que el equipo de proyecto ha preparado un informe escrito cubriendo los aspectos enunciados en la propuesta el proyecto y definiendo las especificaciones de informática a ser satisfechas por el productor final del proyecto.

2. **Verificar** para proyectos de desarrollo o modificación de sistema de informática seleccionados, que la dirección del Departamento de Informática y de los departamentos usuarios han revisado los informes de los equipos de proyecto relativos a las especificaciones de información a ser satisfechas por los productos finales de estos proyectos. Además, verificar que ambos han dado aprobación escrita para que comience el trabajo en la siguiente fase del proyecto.

2.3 ESTUDIO DE VIABILIDAD

Una metodología de ciclo de vida del desarrollo de sistemas en cualquier organización debería establecer, para cada proyecto o propuesta, que se elabore un estudio tecnológico de viabilidad en el cual se formulen formas alternativas de alcanzar los objetivos del proyecto acompañadas de un análisis de coste - beneficio - de cada alternativa contemplada (entre los temas a considerar está la posibilidad de una alternativa nula y la viabilidad de una decisión alternativa entre desarrollar o comprar). Cuando se toma la decisión de seguir adelante en el trabajo con el tema propuesto, debe producirse un plan director del proyecto, por escrito.

2.3.1 Formulación de cursos de acción alternativos.

- **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debería determinar que se analicen cursos de acción alternativos que satisfagan las especificaciones de información establecidas para el sistema propuesto, nuevo o modificado.

- **Directiva de Auditoría.**

Deben revisarse las disposiciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización que exigen que se analicen cursos de acción alternativos que satisfagan las especificaciones de información establecidas para el sistema propuesto, nuevo o modificado.

1. **Cerciorarse**, para proyectos seleccionados de desarrollo o modificación de sistemas de información, de que el equipo de proyecto ha analizado cursos de acción alternativos, y que el informe

del equipo identifica, para la alternativa seleccionada como más viable, las:

- razones para seleccionar o rechazar cada una de las alternativas consideradas
- ventajas y desventajas de la alternativa seleccionada

2.3.2 Estudio de viabilidad tecnológica

- **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debería determinar que se efectúe un examen de la viabilidad tecnológica de cada alternativa que satisfaga las especificaciones de información establecidas para el sistema propuesto, nuevo o modificado.

- **Directiva de Auditoría.**

Deben revisarse las disposiciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización para que se efectúe un examen de la viabilidad tecnológica de cada alternativa que satisfaga las especificaciones de información establecidas para el sistema propuesto, nuevo o modificado. (El Auditor Informático debería reconocer que, en algunos casos, la viabilidad operativa de la alternativa propuesta para un proyecto concreto puede llegar a ser un gran problema. Esto puede ser especialmente cierto cuando vayan a producirse cambios en los cometidos o dependencia del personal. Cuando tiene lugar una situación así, la metodología de ciclo de vida del desarrollo de sistemas de la organización debería disponer un examen por separado de la viabilidad operativa de tal alternativa).

1. **Revisar**, para proyectos seleccionados de desarrollo de sistemas de información, el informe preparado por el equipo de proyecto sobre la viabilidad tecnológica de cada una de las alternativas para satisfacer las especificaciones de información establecidas. **Evaluar** la forma en que dicho informe ha tratado temas tales como:

- a. las necesidades y disponibilidad de equipos
- b. las necesidades y disponibilidad de logical
- c. las necesidades y disponibilidad de material y logical de comunicaciones
- d. restricciones espaciales y temporales válidas implícitas en las solicitudes de información de los departamentos usuarios, y la forma de satisfacerlas
- e. la viabilidad operativa, por ejemplo, si el nuevo proyecto encaja en el entorno actual de material, logical y comunicaciones de la organización
- f. consideraciones legales relativas a la transferencia de tecnología o datos, de ámbito nacional o internacional
- g. restricciones reglamentarias relativas a la utilización de tecnología y a la forma de conseguir la conformidad o aprobación de las autoridades reguladoras pertinentes.

2. Verificar, para proyectos nuevos o de modificación de sistemas informáticos, seleccionados, que la dirección de los departamentos usuarios afectados y la del Departamento de Informática se han puesto de acuerdo sobre la viabilidad tecnológica del método seleccionado para satisfacer las necesidades de información establecidas para el proyecto, en el marco de la metodología de ciclo de vida del desarrollo de sistemas de la organización.

2.3.3 Estudio de viabilidad económica

* **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera requerir, para cada proyecto nuevo o de modificación de sistemas informáticos, que se efectúe un análisis

coste-beneficio, que contemple los costes y beneficios asociados a cada alternativa considerada para satisfacer las necesidades de información establecidas para el proyecto

* **Directiva de Auditoría.**

Deben revisarse las determinaciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización que disponen que se analicen los costes y beneficios de cada alternativa considerada para el proyecto.

1. **Revisar** para proyectos de desarrollo y/o modificación de sistemas de información seleccionados, el resumen de costes del sistema actual, al igual que los costes estimados para cada una de las alternativas consideradas para satisfacer las especificaciones de información establecidas para el proyecto, a fin de cerciorarse de que todos los costes significativos se han incluido en el sumario. En concreto determinar si:

a. los costes presentados cubren todas las fases del ciclo de vida de desarrollo de sistemas para dicho sistema

b. si los costes estimados para cada alternativa considerada incluyen todas las mejoras necesarias en material y logical para apoyar esa alternativa concreta, al igual que los costes en que pueda ser necesario incurrir para formación, preparación y entrada de datos, conversión, y aceptación del sistema, y costes asociados cuando proceda.

2. **Revisar** para proyectos de desarrollo o modificación de sistemas seleccionados, el resumen de los beneficios estimados para cada alternativa considerada para satisfacer las especificaciones de información que han sido establecidas para el proyecto.

3. **Verificar** que los beneficios han sido cuantificados siempre que era posible y que no se ha incluido ningún beneficio no cuantificable en el resumen.

PARTE I - 2. CONTROLES DE DESARROLLO, ADQUISICION Y MANTENIMIENTO

4. **Verificar** para proyectos de desarrollo o modificación de sistemas de información seleccionadas que el análisis de coste y beneficios asociados con cada alternativa considerada para satisfacer las especificaciones de información contempla su impacto sobre los requisitos de seguridad, intimidad y control interno que han sido establecidos para el proyecto de forma general.

5. **Verificar** para proyectos de desarrollo o modificación de sistemas seleccionados, que las direcciones de los departamentos usuarios afectados y la del Departamento de Informática se ha puesto de acuerdo sobre los costes y beneficios asociados a la alternativa seleccionada para satisfacer las especificaciones de información.

2.3.4 Informe del análisis de riesgo.

• **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debería establecer en cada proyecto propuesto de desarrollo o modificación de sistema de información, la confección de un análisis de los riesgos de seguridad, de los controles internos necesarios y de las salvaguardias viables para reducir o eliminar dichas vulnerabilidades.

• **Directiva de Auditoría.**

Deben revisarse las disposiciones del ciclo de vida del desarrollo de sistemas de la organización que exigen que, para cada proyecto propuesto, se analicen los riesgos de seguridad, los controles internos necesarios y las salvaguardias viables para reducir o eliminar tales vulnerabilidades.

1. **Revisar**, para proyectos de desarrollo o modificación de sistemas de información seleccionados, la lista de necesidades de control interno y de vulnerabilidades de seguridad que se ha identifi-

cado para dichos sistemas. Incluir cualquier riesgo conocido en otros sistemas y apreciar si el proceso de determinar tales vulnerabilidades restó atención a:

a. todos los aspectos de la aplicación incluyendo cosas tales como el empleo de enlaces de telecomunicaciones y las disposiciones pertinentes de plan de contingencia

b. la naturaleza y magnitud de cada una de las vulnerabilidades

c. el valor y sensibilidad de todos los ficheros de datos y otros activos de información a incluir en el sistema.

2. **Verificar**, para proyectos de desarrollo o modificación de sistemas de información seleccionados, que en el diseño empleado en el proyecto se incluyeron salvaguardias para reducir los riesgos identificados en dichas sistemas.

3. **Determinar**, mediante entrevistas, que la dirección de los departamentos usuarios, el individuo responsable de la seguridad de la información, los auditores informáticos, y otras personas adecuadas participarán en los análisis de riesgo relacionados con estos proyectos. Cerciorarse de que quedaron satisfechos con cual completos y razonable era el análisis, sus hallazgos y recomendaciones.

2.3.5 Aprobación del proyecto.

• **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debería establecer, que en cada proyecto propuesto, la alta dirección revise los informes de los estudios de viabilidad pertinentes, decida si seguir adelante o no con el proyecto, e identifique una de las alternativas examinadas en tales estudios como base para el trabajo del equipo del proyecto.

• **Directiva de Auditoría.**

Deben revisarse las disposiciones de metodología de ciclo de vida del desa-

rollo de sistemas de la organización que exigen, para cada proyecto propuesto que la alta dirección de la organización revise los estudios de viabilidad pertinentes, determina si se debe seguir adelante con el proyecto e identifique una de las alternativas examinadas en tales estudios.

1. **Determinar** para proyectos de desarrollo o modificación de sistemas de información seleccionadas que los informes del estudio de viabilidad exigidos por la metodología de ciclo de vida del desarrollo de sistemas de la organización, se prepararon y presentaron para revisión por la alta dirección.

2. **Determinar** que dichos informes fueron revisados por la alta dirección y empleados como base para una decisión escrita acerca de si seguir adelante o no con el proyecto.

2.3.6 Plan director del proyecto.

• **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debería establecer para cada proyecto aprobado, que se elabore un plan director del proyecto, adecuado para mantener control sobre el proyecto a lo largo de toda su vida.

• **Directiva de Auditoría.**

Deben revisarse las disposiciones de la metodología de ciclos de vida de desarrollo del sistema de la organización que exigen para cada proyecto aprobado que establezca un plan director del proyecto.

1. **Determinar**, mediante revisión de los registros de proyectos de desarrollo o modificación de sistemas de información relacionados que se estableció un plan director del proyecto.

2. **Determinar** que el nuevo plan director incluía un calendario completo de descomposición del trabajo en activida-

des de proyecto, identificaba los puntos pertinentes de pruebas de aceptación a lo largo de la vida del proyecto, y definía los procedimientos de evaluación y aprobación requeridas en cada uno de dichos puntos.

3. **Determinar** que el plan director se uso para efectuar el requerimiento del progreso del proyecto y que el plan director satisfacía lo dispuesto por la metodología de ciclo de vida del desarrollo de sistemas de la organización.

2.3.7 Control de costes.

• **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debería establecer, para cada proyecto de desarrollo o modificación de sistemas de información aprobado, que se establezca un plan director del proyecto que incluya un método para efectuar el control de los costes en que incurra a lo largo de la vida del proyecto.

• **Directiva de Auditoría.**

Deben revisarse las disposiciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización que exigen que el plan director del proyecto creado para cada proyecto de desarrollo o modificación de sistemas de información aprobado, incluya un método para efectuar el control de los gastos en que se incurra a lo largo de la vida del proyecto.

1. **Revisar** para proyectos de desarrollo o modificación de sistemas de información aprobados, los informes sobre los costes en que se ha incurrido en relación con el trabajo realizado en el proyecto.

2. **Identificar** los componentes de tales costes como tiempo de máquina, horas de empleados y suministros y examinar los justificantes de dichos componentes de costes tales como resúmenes de tiempo de máquina usadas por el equipo del proyecto o informes de tiempo de empleados individuales.

3. **Determinar** si esta información de costes es completa y correcta.

4. **Determinar** para proyectos de desarrollo o modificación de sistemas de información seleccionados, si los informes de costes del proyecto exigidos por la metodología de ciclo de vida del desarrollo de sistema de la organización se prepararon, distribuyeron, revisaron, y aprobaron oportunamente.

2.4 FASE DE DISEÑO.

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera establecer para cada proyecto de desarrollo o modificación de sistemas de información, que las especificaciones del sistema se incorporen adecuadamente a las especificaciones de diseño o del sistema. Debiera usarse una metodología de diseño para estructurar el desarrollo de las especificaciones de entradas, salidas, ficheros, y tratamientos, que describen la solución física a las especificaciones del sistema. Esta metodología de diseño debiera también emplearse para especificar los documentos fuente, los mecanismos de control, las características de seguridad y las pistas de auditoría a incluir en el sistema.

2.4.1 Metodología de diseño

• **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera establecer que se seleccione un procedimiento adecuado para la creación de las especificaciones de diseño de cada proyecto de desarrollo o modificación de sistemas de información.

• **Directiva de Auditoría.**

Deben revisarse las provisiones de la metodología de ciclo de vida del desarrollo de sistema de la organización que exige que se selecciones un procedimiento adecuado para la creación de las especificaciones de diseño en un proyecto de desarrollo o modificación de sistemas de información.

1. **Determinar**, para proyectos de desarrollo o modificación de sistemas de información representativos, el procedimiento de diseño escogido para el sistema (normalmente éste será uno de los siguientes: ciclo de vida, estructurado, base de datos, esqueleto, o prototipo). **Apreciar** si los miembros del equipo de proyecto están familiarizados con - o entrenados en - el empleo de este procedimiento y si el mismo está siendo eficazmente usado en el desarrollo de las especificaciones de diseño del sistema.

2. **Determinar**, para proyectos de desarrollo o modificación de sistemas de información representativos, si los productos finales creados mediante el empleo del procedimiento de diseño seleccionado para el sistema satisfacen las especificaciones del sistema pertinentes.

2.4.2 Definición y documentación de las especificaciones de salida.

• **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera establecer que se seleccione un procedimiento adecuado para crear las especificaciones de salida de cada proyecto de desarrollo o modificación de sistemas de información.

• **Directiva de Auditoría.**

Deben revisarse las provisiones de la metodología de ciclo de vida del desarrollo de sistemas de la organización que exigen que se seleccione un procedimiento adecuado para crear las especificaciones de salida de un proyecto de desarrollo o modificación de sistemas de información.

1. **Revisar**, para proyectos de desarrollo o modificación de sistemas de información seleccionados, si las especificaciones de salida que se han establecido son adecuadas, y determinar si son conformes con la metodología de ciclo de vida del desarrollo de sistemas de la organización.

2. **Revisar** las especificaciones de salida para proyectos de desarrollo o modificación de sistemas de información seleccionados, y **determinar** lo adecuado de las provisiones en cuanto a:

- a. contenido y formato de los informes preparados
- b. autorización de los usuarios que han de recibir los informes
- c. período de retención de los informes
- d. provisiones de pistas de auditoría o gestión
- e. período de retención de ficheros.

3. **Determinar** que las especificaciones de salida retenidas para proyectos de desarrollo o modificación de sistemas de información seleccionadas, brindan a los usuarios del sistema la capacidad de asegurar o controlar que los datos son completos, exactos y autorizados.

2.4.3 Documentación y definición de especificaciones de entrada.

• **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera establecer que se seleccione un procedimiento adecuados para la creación de las especificaciones de entrada en cada proyecto de desarrollo o modificación de sistemas de información.

• **Directiva de Auditoría.**

Deben revisarse las provisiones de metodología de ciclo de vida del desarrollo de sistemas de la organización que exigen que se seleccione un procedimiento adecuado para crear las especificaciones de entrada en un proyecto de desarrollo o modificación de sistemas de información.

1. **Revisar**, para proyectos seleccionadas de desarrollo o modificación de sistemas de información, la adecuación de

las especificaciones de entrada que se han establecido y **determinar** si son conformes con al metodología de ciclo de vida del desarrollo de sistemas de la organización.

2. **Revisar** las especificaciones de entrada para proyectos seleccionados de desarrollo o modificación de sistemas de información y **determinar** cuan adecuadas y razonables son las disposiciones en cuanto a:

- a. las especificaciones de seguridad y de protección de datos relacionados con la intimidad
- b. las medidas de seguridad y de protección de datos relacionadas con la intimidad
- c. las reglas de definición y autorización de transacciones
- d. los procedimientos para el establecimiento de totales de control.

3. **Determinar**, para proyectos seleccionados de desarrollo o modificación de sistemas de información si las definiciones escritas de entradas han sido revisadas y aprobadas por escrito por la dirección del departamento usuario.

2.4.4 Definición y documentación de especificaciones de ficheros.

• **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera disponer que se seleccione un procedimiento adecuado para la definición de las especificaciones de formato y organización de ficheros para cada proyecto o de desarrollo o modificación de sistemas de información.

• **Directiva de Auditoría.**

Deben revisarse las disposiciones de la metodología de ciclo de vida del desarrollo del sistema de la organización de ficheros para cada proyecto de desarro-

PARTE I - 2. CONTROLES DE DESARROLLO, ADQUISICION Y MANTENIMIENTO

llo o modificación de sistemas de información.

Deben revisarse las disposiciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización que exigen que se seleccione un procedimiento adecuado para la creación de las especificaciones de formato y organización de ficheros para un proyecto de desarrollo o modificación de sistemas de información.

1. **Determinar**, para proyectos seleccionados de desarrollo o modificación de sistemas de información, la adecuación de las definiciones de formato y organización y su conformidad con las disposiciones de la metodología de ciclo de vida del desarrollo de sistemas. Si se necesitan ficheros de base de datos **determinar** si la definición cubre las relaciones lógicas, físicas y otras estructurales de los datos, dependencias de los conjuntos de datos, especificaciones de almacenamiento de datos y cualesquiera especificaciones especiales necesarias para asegurar la protección de la intimidad.
2. **Determinar**, para proyectos seleccionados de desarrollo o modificación de sistemas de información si los administradores de bases de datos de la organización participaron en el establecimiento de las definiciones escritas de formato y organización de ficheros.
3. **Determinar**, para proyectos seleccionados de desarrollo o modificación de sistemas de información la adecuación de las definiciones de formato y organización de ficheros, de sensibilidad de contenido de los datos, y períodos de retención de ficheros.
4. **Determinar**, para proyectos seleccionados de desarrollo o modificación de sistemas de información, si las definiciones escritas de formato y organización de ficheros han sido revisadas y aprobadas por la dirección de los departamentos usuarios afectados.

2.4.5 Documentación y definición de especificaciones de proceso.

• Objetivo de Control.

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera disponer que se seleccionen un procedimiento adecuado para definir las especificaciones de los pasos de proceso de datos para cada proyecto de desarrollo o modificación de sistemas de información.

• Directiva de Auditoría.

Deben revisarse las disposiciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización que exigen que se seleccione un procedimiento adecuado para crear las especificaciones de pasos de proceso de datos para un proyecto de desarrollo o modificación de sistemas de información.

1. **Revisar**, para proyectos seleccionados de desarrollo o modificación de sistemas de información la exactitud, validación, oportunidad en el tiempo y flexibilidad de las especificaciones de pasos de proceso que han sido establecidas y determinar si son conforme con la metodología de ciclo de vida del desarrollo de sistemas de la organización.

2. **Determinar**, para proyectos seleccionados de desarrollo o modificación de sistemas de información si las especificaciones de pasos de proceso de datos escritos han sido revisados y aprobados por la dirección de los departamentos usuarios afectados.

2.4.6 Especificaciones de programas.

• Objetivo de Control.

La metodología de ciclo de vida del desarrollo de sistemas debiera exigir que se preparen especificaciones escritas detalladas de programas de desarrollo o modificación de sistemas de información.

• **Directiva de Auditoría.**

Deben revisarse las disposiciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización que exigen que se preparen especificaciones de programas detalladas escritas para cada proyecto de desarrollo o modificaciones de sistemas de información.

1. **Revisar**, para proyectos seleccionados de desarrollo o modificación de sistemas de información la adecuación de las especificaciones de programas que han sido establecidas y determinar si son claras, congruentes y completas y de conformidad con la metodología de ciclo de vida del desarrollo de sistemas de la organización.

2. **Revisar**, para proyectos seleccionados de desarrollo o modificación de sistemas de información, cuan razonable es la lógica del programa que se ha definido mediante un examen de los flujogramas, tablas de decisión, o narrativas pertinentes.

2.4.7 Diseño de la recogida de datos fuente.

• **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera exigir que se especifiquen mecanismos adecuadas para la entrada de información para cada proyecto de desarrollo o modificación de sistemas de información.

• **Directiva de Auditoría.**

Deben revisarse las disposiciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización que exigen que se especifiquen mecanismos adecuados para la entrada de información para cada proyecto de desarrollo o modificación de sistemas de información.

1. **Revisar**, para proyectos seleccionados de desarrollo o modificación de sistemas de información, los mecanismos especificados de recogida de datos fuente para determinar si su diseño facilita una entrada de información exacta y

si dichos diseños han sido aprobadas por la dirección de los departamentos usuarios afectados.

2. **Determinar**, para proyectos seleccionados de desarrollo o modificación de sistemas de información, si los diseños de cualesquiera formularios que hayan sido especificados para la recogida de información, establecen controles tales como un encasillado exacto para las anotaciones, numeración previa de los documentos, y autorización independiente de las transacciones.

3. **Determinar**, para proyectos seleccionados de desarrollo o modificación de sistemas de información si los diseños de cualesquiera procedimientos de entrada en línea de la información establecen formatos de pantalla que emplean mensajes y procedimientos de entrada que facilitan la exactitud y si brindan rutinas de corrección para corregir los errores.

2.4.8 Diseño de controles y seguridad.

• **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera exigir se especifiquen mecanismos adecuadas para asegurar la integridad de los datos almacenados y tratados por un sistema de información y para salvaguardar los recursos del sistema, en cada proyecto de desarrollo o modificación de sistemas de información.

• **Directiva de Auditoría.**

Deben revisarse las disposiciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización que exigen mecanismos adecuados para asegurar la integridad de los datos almacenados y procesados por un sistema de información para salvaguardar los recursos del sistema para cada proyecto de desarrollo o modificación de sistemas de información.

1. **Revisar**, para proyectos seleccionados de desarrollo o modificación de sis-

PARTE I - 2. CONTROLES DE DESARROLLO, ADQUISICION Y MANTENIMIENTO

temas de información, las medidas de control de integridad y mediación de accesos en sus especificaciones y **evaluarlas** respecto de una metodología adecuada de diseño de controles o evaluación de seguridad.

2. **Determinar**, para proyectos seleccionados de desarrollo o modificación de sistemas de información:

- a. Si en las especificaciones de diseño se han incluido, en cada punto crítico del sistema, controles adecuados
- b. que se ha efectuado el análisis coste-beneficio para dichos controles
- c. que se ha establecido una distinción adecuada entre el uso de controles preventivos y controles detectores
- d. si se han establecido controles correctores donde y cuando era adecuado.

3. **Determinar**, para proyectos seleccionados de desarrollo o modificación, si la función de auditoría interna ha evaluado la adecuación de los controles incluidos en las especificaciones de diseño del sistema.

4. **Determinar**, para proyectos seleccionados de desarrollos o modificación de sistemas de información que afectan a transacciones o datos sensibles, si el oficial de seguridad de la información de la organización ha revisado y aprobado. Los controles de integridad y las medidas de mediación de accesos incluidas en sus especificaciones, especialmente en términos de su efecto en la reducción o eliminación de los riesgos asociados con la operación del sistema.

5. **Determinar**, para proyectos seleccionados de desarrollo o modificación de sistemas de información, si los controles de integridad, si los controles de integridad y las medidas de mediación de accesos incluidas en sus especificacio-

nes han sido definidas con detalle suficiente para facilitar que puedan ser probadas adecuadamente.

2.4.9 Diseño de pistas de auditoría.

• Objetivo de Control.

La metodología de ciclo de vida del desarrollo del sistema de la organización debiera exigir que se especifiquen mecanismos adecuados de pistas de auditoría en cada proyecto de desarrollo o modificación de sistemas de información.

• Directiva de Auditoría.

Deben revisarse las disposiciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización que exigen que se especifiquen pistas de auditoría adecuadas para cada proyecto de desarrollo o modificación de sistemas de información.

1. **Revisar**, para proyectos seleccionados de desarrollos o modificación de sistemas de información, las pistas de auditoría especificadas para **determinar** si su diseño es adecuado, especialmente en términos de la inclusión de mecanismos tanto automáticos cuanto normales y de su efectividad para seguir la pista a las transacciones desde el punto de origen hasta los totales de control pertinentes y desde éstos hacia atrás hasta el punto de origen.

2. **Revisar**, para proyectos seleccionados de desarrollo o modificación de sistemas de información, la adecuación de las medidas establecidas para la integridad y seguridad de las pistas de auditoría en las especificaciones de diseño.

3. **Determinar**, para proyectos seleccionados de desarrollo o modificación de sistemas de información, si la función de auditoría interna ha evaluado la adecuación de las pistas de auditoría incluidas en las especificaciones de diseño del sistema.

2.4.10 Aprobación del diseño.

- **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera exigir que las especificaciones de diseño de todos los proyectos de desarrollo o modificación de sistemas de información sean revisados y aprobadas por la dirección del departamento de informática, por la de los departamentos usuarios afectados y, cuando proceda por la alta dirección de la organización.

- **Directiva de Auditoría.**

Deben revisarse las disposiciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización que exigen que las especificaciones de diseño de todos los proyectos de desarrollo o modificación de sistemas de información sean revisados y aprobadas por la dirección del departamento de informática, la de los departamentos usuarios afectados, y cuando proceda por la alta dirección de la organización.

1. **Determinar**, para proyectos seleccionados desarrollo o modificación de sistemas de información, si las especificaciones de diseño han sido revisadas y aprobadas por la dirección del departamento de informática, la de los departamentos usuarios afectados, y cuando proceda por la alta dirección de la organización.

2. **Determinar** que todas las cuestiones que surgieron durante esta revisión y aprobación han sido resueltas antes del comienzo del trabajo en la fase siguiente del proyecto (si en los proyectos seleccionados para revisión por el auditor quedaran cuestiones sin resolver, la naturaleza de las mismas y su significado debieran ser objeto de comentario).

2.4.11 Estándares de documentación de programas.

- **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera incluir estándares de documen-

tación de programas aprobados por el comité de planificación o el comité de dirección del departamento de informática, comunicados a la plantilla del departamento y cuya aplicación se vigila para asegurar la documentación creada durante la ejecución de proyectos de desarrollo o mantenimiento de sistemas de información rehace de conformidad con tales estándares.

- **Directiva de Auditoría.**

Deben revisarse los estándares de documentación de programas que formen parte de la metodología de ciclo de vida del desarrollo de sistemas de la organización y los medios que se emplean para asegurar su cumplimiento.

1. **Obtener** una copia de los estándares de documentación de programas de la organización y **determinar** si dichos estándares han sido aprobados por el comité de planificación o el comité de dirección del departamento de informática, si son apropiados en términos del material, sistemas operativos, y lenguajes de programación en uso en la organización y si aprovechan plenamente las ventajas de las buenas prácticas en ingeniería de logical.

2. **Determinar**, mediante entrevistas con los individuos implicados, y mediante una revisión de la documentación de proyectos seleccionados de desarrollo y modificación de sistemas de información, si los estándares de programación incorporados a la metodología de ciclo de vida del desarrollo de sistemas de la organización se han comunicado a la plantilla del departamento de informática y si se cumplen.

3. **Revisar** la documentación relativa a proyectos seleccionados de desarrollo y modificación de sistemas de información y **determinar** si la dirección del departamento de informática ha revisado dicha documentación para confirmar su adecuación y su cumplimiento con los estándares de documentación de programas integrantes de la metodología de ciclo de vida del desarrollo de sistemas de la organización.

2.4.12 Plan de validación, verificación y pruebas.

• **Objetivo de Control.**

La metodología de ciclos de vida del desarrollo de sistemas de la organización debiera exigir que se establezca un plan de validación, verificación y prueba para cualquier proyecto de desarrollo y modificación de sistemas de información.

• **Directiva de Auditoría.**

Deben revisarse las especificaciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización de que debe establecerse un plan de validación, verificación y pruebas para cada proyecto de desarrollo y modificación de sistemas de información.

1. **Determinar**, para proyectos seleccionados de desarrollo y modificación de sistemas, si se ha establecido un plan para probar el sistema y su logical.

2. **Apreciar** si este plan incluye criterios de medidas y restituciones adecuadas, criterios de reducción de datos de prueba y de evaluación tanto para la fase de desarrollo cuanto para la de pruebas del producto final, y que el mero cumplimiento del mismo no dará lugar a pruebas insuficientes o inadecuadas.

3. **Determinar**, mediante entrevistas con las personas implicadas y mediante una revisión de la documentación relativa a proyectos seleccionados de desarrollo y modificación de sistemas de información, si las pruebas exigidas fueron:

- a. llevadas a cabo por un número suficiente de personas cualificadas independientes del equipo de proyecto
- b. efectuadas con participación adecuada de representantes de los departamentos usuarios afectados
- c. efectuadas en el entorno en el que el sistema se usará realmente.

4. **Determinar**, mediante entrevistas con los individuos implicados, y mediante una revisión de la documentación de proyectos seleccionados de desarrollo y modificación de sistemas de información si el plan de pruebas contemplaba:

- a. la disposición necesaria de material y datos
- b. un adecuado entrenamiento de usuarios u operadores
- c. los contratos de programas de pruebas, ficheros y datos adecuados
- d. la recogida y análisis de los datos pertinentes
- e. la escritura de los informes exigidos.

5. **Determinar**, mediante una revisión de la documentación de pruebas de proyectos seleccionados de desarrollo y modificación de sistemas de información.

- a. la fuente, tipo y adecuación del juego o generador de pruebas
- b. los datos de transacciones reales
- c. el análisis de los resultados de la prueba.

2.5 DESARROLLO E IMPLANTACIÓN.

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera establecer, para cada proyecto de desarrollo o modificación de sistemas de información que los objetivos de programación debieran ser establecidos para el proyecto y debieran asignarse responsabilidades para llevar a cabo la programación, que debieran prepararse manuales del sistema, definirse los estándares de pruebas de programas y sistema, establecerse los criterios de validación y aceptación del sistema, y asegurarse la aceptación del sistema por la

dirección del departamento usuario afectado.

2.5.1 Objetivos de programación.

• **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización exigir que se establezca una declaración escrita de los objetivos de programación a llevar a cabo para cada proyecto de desarrollo y modificación de sistemas de información.

• **Directiva de Auditoría.**

Deben revisarse las especificaciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización respecto a la realización de una declaración escrita de los objetivos de programación a ser efectuados para cada proyecto de desarrollo y modificación de sistemas de información.

1. **Revisar** la documentación de proyectos seleccionados de desarrollo y modificación de sistemas de información y **determinar** si incluye declaraciones escritas adecuadas de los objetivos de programación a alcanzar en el proyecto y si tales declaraciones son conformes con las disposiciones pertinentes de la metodología de ciclo de vida del desarrollo de sistemas de la organización.

2.5.2 Descripción de la narrativa del programa.

• **Objetivo de Control.**

La metodología del ciclo de vida del desarrollo de sistemas de la organización debiera exigir que se produjese durante el proyecto una declaración escrita de los objetivos de programación a alcanzar durante el proyecto para cada proyecto de desarrollo y modificación del ciclo de vida del desarrollo de sistemas.

• **Directiva de Auditoría.**

Deben revisarse las especificaciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización

de que se establezca una declaración escrita de los objetivos de programación a alcanzar para cada proyecto de desarrollo y modificación de sistemas de información.

1. **Revisar** la narrativa detallada preparada como parte de la documentación de los programas y **determinar** la extensión en que es conforme con la narrativa original de definición del sistema (en ocasiones puede usarse como parte de la documentación final de programas pero normalmente habrá de ser escrita de conformidad con el programa tal y como está realmente escrito, y para reflejar la lógica desarrollada por el programador).

2. **Revisar** la documentación de proyectos seleccionados de desarrollo y modificación de sistemas de información y **determinar** si la narrativa lógica detallada ha sido escrita de forma clara y concisa de forma que personas que no estén familiarizadas con el programa fueran capaces de entender su función.

3. **Determinar**, mediante una revisión de la documentación de proyectos seleccionados de desarrollo y modificación de sistemas de información. Si la metodología de ciclo de vida del desarrollo de sistemas de la organización exige que se prepare un flujograma a nivel de programa para cada proyecto y si la documentación existente es conforme con dicha especificación.

4. **Determinar**, a partir de una revisión de la documentación de proyectos seleccionados de desarrollo y modificación de sistemas de información, si las descripciones de ficheros y las maquetas de los informes son conformes con las determinaciones con la metodología de ciclo de vida del desarrollo de sistemas de la organización.

5. **Determinar**, mediante una entrevista con el administrador de bases de datos de la organización y mediante una revisión de la documentación de proyectos seleccionados de desarrollo y modificación de sistemas de informa-

PARTE I - 2. CONTROLES DE DESARROLLO, ADQUISICION Y MANTENIMIENTO

ción, si los elementos de datos empleados en los proyectos seleccionados.

- a. tienen designaciones descritas
- b. están adecuadamente descritas
- c. no están en conflicto con otras definiciones en el sistema de base de datos.

2.5.3 Paquetes de logical de aplicación.

• Objetivo de Control.

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera exigir que se determine la disponibilidad de paquetes de logical comercial que pudieran satisfacer las necesidades de un determinado proyecto de desarrollo o modificación de sistemas de información. Los paquetes de logical comercial debieran ser compatibles con las operaciones de proceso actuales del departamento de informática antes de asignar a miembros de la plantilla del departamento para efectuar cualquiera programación relativa a estos proyectos. Los procedimientos de adquisición de productos logical debieran seguir las políticas de adquisición de la organización y dichos productos debieran ser probados y revisados antes de pagar por ellos y ponerlos en uso.

• Directiva de Auditoría.

Deben revisarse las determinaciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización referentes a la selección y adquisición de paquetes de logical de aplicación.

1. **Revisar** los informes de los estudios de viabilidad económica de proyectos seleccionados de desarrollo o modificación de sistemas de información y **determinar** si se contempló adecuadamente la adquisición de paquetes de logical.

2. **Revisar**, para proyectos seleccionados de desarrollo modificación de sistemas de información, los acuerdos selec-

cionados con la adquisición de paquetes de logical para **determinar** si:

a. sus disposiciones son conformes con las políticas de adquisición pertinentes en la organización y si fueron aprobadas por escrito por la dirección de los departamentos usuarios afectados y del departamento de informática

b. la documentación suministrada con estos paquetes y los controles incorporados en los propios programas eran adecuados

c. los propios paquetes fueron probados y revisados antes de ser utilizados y pagados.

2.5.4 Contratación de programas de aplicación a medida.

• Objetivo de Control.

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera establecer que la contratación de programas de servicios de programación a medida ha de estar justificada mediante una petición escrita de un director de proyecto (los productos finales de los servicios completos de programas a medida debieran ser probados y revisados por el grupo de garantía de calidad del departamento de informática, antes de que se apruebe el pago del trabajo y el producto final).

• Directiva de Auditoría.

Deben revisarse las determinaciones de la metodología del ciclo de vida del desarrollo de sistemas de la organización que tratan con la solicitud y adquisición de servicios de programación a medida y con las pruebas del producto final de tales servicios.

1. **Revisar**, para proyectos seleccionados de desarrollo o modificación de sistemas de información, las solicitudes para contratación de programación a medida para **determinar**:

- a. la razonabilidad de las peticiones
- b. la aprobación de dichas peticiones previa a la gestión de adquisición de los servicios
- c. que el enunciado de los servicios a ser prestados, las estipulaciones para asegurar que se alcanzan los rendimientos deseados, las determinaciones en cuanto a contingencia para el caso de que el contratista falle en ejecutar o prestar el servicio y otras prácticas relativas a la adquisición que se hallan seguidos son conformes con las determinaciones pertinentes de la política de adquisición de la organización.

2. Determinar, mediante entrevistas y una revisión de la documentación relativa a proyectos selección de desarrollo o modificación de sistemas de información si el prestador de los servicios de programación a medida recibió unas directrices adecuadas respecto a los estándares de documentación de programas de la organización y las disposiciones de declaración de objetivos de programación del proyecto y las narrativas de programas asociados.

3. Revisar la documentación de servicios de programación a medida contratados para proyectos selección de desarrollo o modificación de sistemas de información y determinar si la codificación, documentación y controles de los programas desarrollos pro contratos fueron probados por el grupo de garantía de calidad del departamento de informática y que fueron aprobados de conformidad con las determinaciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización y del contratista.

4. Revisar la documentación para servicios de programación a medida contratados para proyectos seleccionados de desarrollo o modificación de sistemas de información y determinar si los pagos efectuados en el marco del contrato estuvieron soportados por pruebas y aportaciones pertinentes.

2.5.5 Manual de operaciones y mantenimiento.

- **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera determinar que se preparen manuales de operación y mantenimiento adecuados como parte de todo proyecto de desarrollo o modificación de sistemas de información.

- **Directiva de Auditoría.**

Deben revisarse las disposiciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización que exigen que se preparen manuales de operaciones y mantenimiento adecuados como parte de todo proyecto de desarrollo o modificación de sistemas de información.

1. **Verificar** que la metodología de ciclo de vida del desarrollo de sistemas de la organización define la documentación de operaciones o manual de explotación que hay que crear para cada proyecto de desarrollo o modificación de sistemas de información.

2. **Verificar**, mediante entrevistas y revisión de la documentación relativa a proyectos seleccionados de desarrollo o modificación de sistemas informáticos, que el manual de explotación correspondiente.

- a. es conforme con la metodología de ciclo de vida del desarrollo de sistemas de la organización

- b. es accesible a y comprensible por los operadores

- c. es usado en las pruebas de lógico.

3. **Verificar**, para proyectos seleccionados el desarrollo o modificación de sistemas de información que el correspondiente manual de explotación específica, para cada paso del trabajo.

- a. la función del programa

PARTE I - 2. CONTROLES DE DESARROLLO, ADQUISICION Y MANTENIMIENTO

- b. las necesidades de equipo
- c. la explicación de todos los mensajes de consola, con la respuesta pertinente del operador
- d. la creación y formación de disponer de las salidas
- e. la adecuada identificación de las etiquetas de los ficheros de salida
- f. los procedimientos adecuados de re arranque o notificación en caso de condiciones de error o fallo
- g. los puntos de control para una adecuada operación del programa entre pasadas del mismo.

2.5.6 Manual de usuario.

* Objetivo de Control.

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera determinar que se preparen manuales de usuarios adecuados como parte de todo proyecto de desarrollo o modificación de sistemas de información.

* Directiva de Auditoría.

Deben revisarse las determinaciones de metodología de ciclo de vida del desarrollo de sistemas de la organización que exigen que se preparen manuales de usuarios adecuados como parte de cada proyecto de desarrollo o modificación de sistemas de información.

1. **Verificar** que la metodología de ciclo de vida del desarrollo de sistemas de la organización define la documentación o manual de usuario a crear para cada proyecto de desarrollo o modificación de sistemas de información.

2. **Verificar**, para proyectos seleccionados de desarrollo o modificación de sistemas de información, que el manual de usuario incluye información adecuada acerca de:

- a. la especificación y formato de los datos de entrada.
 - b. la necesidad de totales de control.
 - c. la formación de presentar los datos al departamento de informática.
 - d. la responsabilidad para convertir los datos a forma legible por el ordenador.
 - e. la responsabilidad para resolver los errores u otras inexactitudes.
 - f. la asignación de prioridades de tratamiento.
 - g. el horario y frecuencia de la distribución de salidas.
 - h. la seguridad, la retención y la disposición de las salidas.
 - i. la lógica de programación.
 - j. el desarrollo de las fórmulas críticas.
 - k. el registro de la aprobación por el usuario.
 - l. el registro de solicitudes y aprobación de cambio a los programas.
 - m. los procedimientos de encendido de terminales, apertura de terminales, cierre de terminales y apagado de terminales.
 - n. la descripción de los mapas de pantalla de los terminales y de los comandos disponibles.
3. **Verificar**, mediante entrevistas y revisión de proyectos seleccionados de desarrollo o modificación de sistemas de información, que los manuales de usuarios se han distribuido de conformidad con las determinaciones pertinentes de la metodología de ciclo de vida del desarrollo de sistemas de la organización y que dichos manuales se han usado para las pruebas de logical.

2.5.7 Plan de Formación.

• **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera determinar que se prepare un plan adecuado para la formación del personal de los departamentos usuarios afectados y de los grupos de operación y mantenimiento del departamento de informática, como parte de todo proyecto de desarrollo o modificación del sistema de información.

• **Directiva de Auditoría.**

Deber revisarse las determinaciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización que exigen la elaboración de los departamentos usuarios y de los grupos de operaciones y mantenimiento del departamento informático.

1. **Determinar**, mediante una revisión de proyectos seleccionados de desarrollo o modificación de sistemas de información si para cada uno de tales proyectos se ha preparado un plan escrito de formación de la plantilla de los departamentos usuarios y de los grupos de operación y mantenimiento del departamento de informática, que verificar que el plan establece un plazo suficiente para completar las actividades de formación necesarias.

2.5.8 Estándares de prueba de programas.

• **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera determinar estándares para la prueba e implantación del logical desarrollado como parte de cada proyecto de desarrollo o modificación de sistemas de información.

• **Directiva de Auditoría.**

Deben revisarse las determinaciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización que establecen estándares para la prueba

ba e implantación del logical desarrollado como parte de todo proyecto de desarrollo o modificación de sistemas de información.

1. **Verificar** que la metodología de ciclo de vida del desarrollo de sistemas de información de la organización define estándares adecuados para la prueba de implantación del logical desarrollado como parte de todo proyecto de desarrollo o modificación de sistemas de información.

2. **Determinar**, mediante una revisión de la documentación referente a proyectos seleccionados de desarrollo o modificación de sistemas de información si los directivos y mandos del departamento de informática, el grupo de garantía de calidad y la dirección de los departamentos usuarios afectados establecieron revisiones escritas de sus pruebas y aprobaciones del trabajo de programación llevado a cabo en tales proyectos.

3. **Verificar** que se programaron todas las funciones, se probó todo el código ejecutable y que dichos resultados eran conformes con las especificaciones originales de programación del proyecto.

2.5.9 Estándares de prueba de sistemas.

• **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera establecer estándares para la prueba del sistema como tal, como parte de todo el proyecto de desarrollo o modificación de sistemas de información.

• **Directiva de Auditoría.**

Deben revisarse la determinación de la metodología de ciclo de vida del desarrollo de sistemas de la organización que establecen estándares para la prueba del sistema como tal, como parte de todo proyecto de desarrollo o modificación de sistemas de información.

PARTE I - 2. CONTROLES DE DESARROLLO, ADQUISICION Y MANTENIMIENTO

1. **Verificar** que la metodología de ciclo de vida del desarrollo de sistemas de la organización define estándares adecuados para la prueba de sistemas de información específicos y que dichos estándares son adecuados al tamaño y complejidad del tratamiento de datos que se lleva a cabo por el departamento de informática.

2. **Revisar** los estándares para la prueba de los sistemas de información específicos contenidos en la metodología de ciclo de vida del desarrollo de sistemas de la organización.

3. **Determinar** si los estándares determinan de forma adecuada la participación de representantes de los departamentos usuarios afectados y la de los miembros de la plantilla de programación y garantía de calidad del departamento informático, en la preparación de datos de prueba para la revisión y aprobación de los resultados de las pruebas.

2.5.10 Documentación de las pruebas de sistema.

* Objetivo de Control.

La metodología de ciclo de vida del desarrollo de sistema de la organización debe establecer, como parte de todo proyecto de desarrollo o modificación de sistemas de información, que los resultados de las pruebas de sistemas se incluyan en forma de registro escrito entre las actividades del equipo el proyecto.

* Directiva de Auditoría.

Deben revisarse las determinaciones de la metodología de ciclo de vida del desarrollo de sistema de la organización que establecen, como parte de todo proyecto de desarrollo o modificación de sistemas de información, que los resultados de las pruebas de sistemas deben incluirse, como un registro escrito, entre las actividades del equipo de proyecto.

1. **Determinar**, mediante una revisión de la documentación referente a proyectos seleccionados de desarrollo o

modificación de sistemas de información si:

a. el sistema fue probado de conformidad con el plan de verificación, validación y prueba

b. si todos los elementos principales del sistema fueron incluidos en el proceso de prueba.

c. si el material de las pruebas se controló adecuadamente durante el proceso de prueba

d. los resultados del proceso fueron aprobados por las direcciones de los departamentos usuarios afectados, la del departamento de informática, y el grupo de garantía de calidad de este departamento.

e. el registro de este proceso de pruebas y aprobación fue el adecuado

f. en los registros de actividades del equipo de proyecto se incluyó un informe escrito sobre los resultados de las pruebas.

2. Determinar, mediante entrevistas con la dirección de los departamentos usuarios afectados y mediante revisión de la documentación de proyectos seleccionados de desarrollo o modificación de sistemas de información, si los representantes de los departamentos usuarios eran conscientes de la importancia del proceso de prueba, si participaron en el mismo adecuadamente, y si se consideraron a sí mismos responsables de la aprobación de los resultados del proceso.

3. Determinar, mediante la revisión de las documentación de pruebas de sistema para proyectos seleccionados de desarrollo o modificación de sistemas de información, si los controles de acceso y autorización y las pistas de auditoría incluidas en el sistema eran adecuados.

4. Determinar si se han desarrollado procedimientos escritos adecuados por la dirección bien de los departamentos escritos adecuados por la dirección bien de los departamentos usuarios afectados, bien del departamento de informática, para mantener la adecuación de tales controles y pistas de auditoría durante la explotación del sistema.

2.5.11 Evaluación de los resultados de las pruebas.

* **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera establecer, como parte de todo proyecto de desarrollo o modificación de sistemas de información, que los resultados de las pruebas de sistemas se evalúen y aprueben por la dirección de los departamentos usuarios afectados y del Departamento de Informática.

* **Directiva de Auditoría.**

Deben revisarse las determinaciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización que establecen, como parte de todo proyecto de desarrollo o modificación de sistemas de información, que los resultados de las pruebas de sistemas han de ser evaluadas y aprobadas por la dirección de los departamentos usuarios afectados y la del departamento de informática.

1. **Determinar**, mediante una revisión de la documentación de pruebas relativa a proyectos seleccionados de desarrollo o modificación de sistemas de información, si antes de realizar las pruebas de sistemas se desarrollaron sistemas previos determinados que se compararon con los resultados de las pruebas y que ambos coincidían. (En los casos en que no hubiera coincidencia entre unos y otros, el auditor debiera examinar tales diferencias y obtener una información de dos individuos que participaron en el proceso de revisión y aprobación de las pruebas).

2. **Determinar**, mediante una revisión de la documentación de pruebas correspondientes a proyectos seleccionados de desarrollo o modificación de sistemas de información, si dicha comunicación contiene información como;

- a. listado de datos de prueba
- b. informes de las salidas del sistema
- c. apuntes pertinentes procedentes del diario del sistema operativo.

3. **Determinar**, mediante una revisión de la documentación de pruebas correspondiente a proyectos seleccionados de desarrollo o modificación de sistemas de información, se efectuaron pruebas de respaldo y recuperación, de carga punta y de capacidad, de fallo planificado, y del plan de contingencia, y de los resultados de tales pruebas fueron evaluados y aprobados por la dirección de los departamentos usuarios afectados y del departamento de informática.

2.5.12 Plan de Conversión.

* **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera establecer, como parte de todo proyecto de desarrollo o modificación de sistemas de información, que se desarrolle un plan de conversión del sistema para pasarlo de desarrollo a explotación.

* **Directiva de Auditoría.**

Deben revisarse las determinación de la metodología de ciclo de vida del desarrollo de sistemas de la organización que exigen, con parte de todo proyecto de desarrollo o modificación de sistemas de información que establezca un plan de conversión del sistema para pasarlo de desarrollo a explotación.

1. **Determinar** mediante una revisión de la documentación de proyectos seleccionados de desarrollo o modificación de sistemas de información si la dirección de los departamentos usuarios

PARTE I - 2. CONTROLES DE DESARROLLO, ADQUISICION Y MANTENIMIENTO

afectados y del departamento de informática desarrollaron un plan escrito completo para la conversión del sistema de desarrollo a explotación, que dicho plan era conforme con las determinaciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización, y que el plan contemplaba:

- a. una revisión conjunta por la organización previa a la iniciación del proceso de conversión, de la adecuación de la documentación de programas, de los manuales de explotación y usuarios y de otros registros creados por el equipo de proyectos
- b. la asignación de suficientes miembros de la plantilla al proceso de conversión
- c. la impartición a dichos individuos de la formación adecuada en el uso de las determinaciones de ese proceso de prueba.

2.5.13 Pruebas en Paralelo

• **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debería definir las circunstancias bajo las cuales se llevará a cabo una prueba en paralelo del sistema actual y el nuevo y debería especificar los criterios para terminar este proceso de prueba.

• **Directiva de Auditoría.**

Deben revisarse las determinaciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización que definen las circunstancias bajo las cuales se llevará a cabo una prueba en paralelo del sistema actual y el nuevo y que especifican los criterios para terminar este proceso de prueba.

1. **Determinar**, mediante una revisión de la documentación correspondiente a proyectos seleccionados de desarrollo o modificación de sistemas de información, si la decisión por la dirección de los departamentos usuarios afectados y del

departamento de informática de exigir que el sistema se sometiese a una prueba en paralelo durante el proceso de conversión.

- a. estaba soportada por un análisis coste-beneficio adecuado
- b. brindaba una base para resolver cualesquiera problemas de tratamiento encontrados durante la prueba
- c. establecía criterios adecuados para terminar el proceso de prueba (el auditor debiera verificar que la decisión real de terminar la prueba en paralelo en el caso de cada uno de los proyectos seleccionados era conforme con los criterios establecidos por la dirección).

2.5.14 Prueba de aceptación final.

• **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas debiera establecer, como parte de las pruebas de aceptación final o de garantía de calidad de un sistema de información nuevo o modificarlo, que se evalúen los resultados de las pruebas por dirección de los departamentos usuarios afectados y del departamento de informática.

• **Directiva de Auditoría.**

Deben revisarse las determinaciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización que exigen, como parte de las pruebas de aceptación final o de garantía de calidad de un sistema de información nuevo o modificado, que la dirección de los departamentos usuarios afectados y la del departamento informática efectúen una evaluación de los resultados de las pruebas.

1. **Verificar** que la metodología de ciclo de vida del desarrollo de sistemas de la organización define estándares adecuados para las pruebas de acepta-

ción final de sistemas de información nuevo o modificados.

2. **Determinar**, mediante una revisión de la documentación de proyectos seleccionados de desarrollo o modificación de sistemas de información, si la dirección de los departamentos usuarios afectados, la del departamento de informática, y los miembros del grupo de garantía de calidad del departamento, participaron en una evaluación del funcionamiento del nuevo sistema.

3. **Determinar** si las posibles ineficiencias en dicho funcionamiento s remediaron antes de declarar operativo al sistema.

2.6 EXPLOTACIÓN Y MANTENIMIENTO.

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera establecer, para cada proyecto de desarrollo o modificación de sistemas de información, que se establezcan los procedimientos de explotación y mantenimiento que aseguren que los datos se tratan de forma congruente y exacta y que el contenido de sistemas sólo será modificado mediante autorización adecuada.

2.6.1 Procedimientos de control de explotación.

* Objetivo de Control.

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera asegurar que se han instalado procedimientos adecuados para controlar las actividades de tratamientos de datos de un sistema de información nuevo o modificado.

* Directiva de Auditoría.

Deben revisarse las determinaciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización que exigen la instalación de procedimientos adecuados para el control de las actividades de tratamientos de datos

de un sistema de información nuevo o modificado.

1. **Determinar**, mediante una revisión de la documentación de proyectos seleccionados de desarrollo o modificación de sistemas de información, si los procedimientos de control establecidos por la organización de los departamentos usuarios afectados y del departamento de informática son adecuados para el tipo de ficheros que se mantiene y para las transacciones que se procesan por el nuevo sistema.

2. **Determinar** que los procedimientos incluyen controles de la distribución de las salidas del sistema de forma que sólo representantes autorizados de los departamentos usuarios afectados reciben dichas salidas.

3. **Determinar** que los procedimientos aseguran que los errores detectados durante la explotación del sistema se identifican, controlan, corrigen y vuelven a tratar se adecuadamente.

4. **Determinar** que los procedimientos aseguran que las funciones clave de explotación, incluidas la explotación de programas de aplicación, la seguridad de datos, la creación y entrada de datos, y la gestión de bases de datos relacionados con el sistema se efectúan por individuos distintos y que la dirección impone esa separación de funciones.

2.6.2 Control de costes.

* Objetivo de Control.

El sistema de contabilidad de la organización debiera, de forma rutinaria, registrar, analizar e informar sobre los costes asociados con la explotación de un nuevo sistema de información.

* Directiva de Auditoría.

Deben revisarse los procedimientos empleados por el sistema de contabilidad de la organización para registrar, analizar e informar, de forma rutinaria, sobre

PARTE I - 2. CONTROLES DE DESARROLLO, ADQUISICION Y MANTENIMIENTO

los costes asociados con la explotación de un nuevo sistema de información.

1. **Revisar** los procedimientos empleados por el sistema de contabilidad de la organización para registrar, analizar, e informar, de forma rutinaria, sobre los costes asociados con la explotación de un nuevo sistema de información.

2. **Verificar** que los procedimientos son adecuados y que han sido revisados y aprobados por la dirección de los departamentos usuarios afectados y del departamento de informática.

2.6.3 Modificaciones al sistema.

• Objetivo de Control.

La metodología de ciclo de vida de desarrollo del sistema de la organización debiera establecer procedimientos para hacer un seguimiento y control de los cambios de todos los sistemas de información en explotación.

• Directiva de Auditoría.

Deben revisarse las determinaciones de la metodología de ciclo de vida desarrollo de sistemas de la organización que establecen las bases para el seguimiento y control de cambios de todos los sistemas de información en explotación.

1. **Determinar**, mediante una revisión de la documentación de sistemas de información en explotación seleccionados si las propuestas de cambios o las modificaciones a tales sistemas se registran y procesan de modo oportuno.

2. **Determinar** si los cambios o modificaciones propuestos para tales sistemas son aprobados por la dirección del departamento usuarios antes de que comience a trabajarse en ellos.

3. **Determinar** que los registros de los cambios introducidos, incluso las revisiones de flujogramas o tablas de decisión y la evaluación y aprobación de los resultados de las pruebas se incorporan a la documentación acumulada para

este sistema por el departamento de informática.

2.6.4 Re-evaluación de las especificaciones de usuario.

• Objetivo de Control.

La metodología de ciclo de vida de desarrollo del sistema de la organización debiera establecer la revisión periódica de las especificaciones de usuario para sistemas de información específicos a fin de determinar si y cómo han cambiado dichas especificaciones.

• Directiva de Auditoría.

Deben examinarse las determinaciones de la metodología de ciclo de vida de desarrollo del sistema de la organización que exigen la revisión periódica de las especificaciones de usuario para sistemas de información específicos a fin de determinar si y como pueden haber cambiado tales especificaciones.

1. **Determinar**, mediante una revisión de las peticiones pendientes de modificaciones a sistemas de información en el departamento de informática, la extensión de las necesidades de los usuarios no satisfechas.

2. **Determinar**, mediante entrevistas o distribución de un cuestionario, la naturaleza de los cambios buscados en tales sistemas, por la dirección de los departamentos usuarios.

3. **Verificar** que los sistemas en cuestión brindan a los usuarios información en formato adecuado y de forma precisa, oportuna, completa y fiable.

2.7 REVISIÓN POST-IMPLANTACIÓN.

La metodología de ciclo de vida de desarrollo del sistema de la organización debiera establecer una revisión completa una vez implantado el sistema de información, de cada proyecto de desarrollo o modificación, para asegurar que el esfuerzo tuvo como resultado un siste-

ma que satisface las necesidades de los usuarios y los objetivos declarados, que está produciendo los beneficios que se esperaba, y que satisface las especificaciones de la metodología.

2.7.1 Plan de revisión post-implantación.

*** Objetivo de Control.**

La metodología de ciclo de vida de desarrollo del sistema de la organización debiera establecer como parte integral de las actividades del equipo de proyecto, el desarrollo de un plan para efectuar una revisión post-implantación de todo sistema de información nueva o modificada.

*** Directiva de Auditoría.**

Deben examinarse las determinaciones de la metodología de ciclo de vida de desarrollo del sistema de la organización para el desarrollo, como parte integral de las actividades del equipo de proyecto, de un plan para ejecutar una revisión post-implantación de todo sistema de información nuevo o modificado.

Determinar, mediante un examen de la documentación de sistema de información en explotación seleccionados, si el equipo de proyecto de desarrollo o modificación estableció un plan de revisión post-implantación, que incluya :

- a. una fecha prevista para la revisión que prevea un tiempo suficiente como para que el sistema esté plenamente operativo
- b. la acumulación de datos para efectuar la revisión
- c. quién ha de efectuar la revisión
- d. objetivos bien definidos de la revisión
- e. el ámbito y naturaleza de la revisión y los recursos necesarios para ella

f. la preparación y publicación de un informe con los resultados de la revisión.

2.7.2 Evaluación de resultados.

*** Objetivo de Control.**

La metodología de ciclo de vida de desarrollo del sistema de la organización debiera exigir que una revisión post-implantación de un sistema de información operativo evalúe si se han alcanzado los objetivos del sistema.

*** Directiva de Auditoría.**

Deben examinarse las especificaciones de la metodología de ciclo de vida de desarrollo del sistema de la organización que establecen que debe efectuarse una revisión post-implantación de los sistemas de información operativos para evaluar si se han alcanzado los objetivos de dicho sistema.

1. **Determinar**, mediante examen de la documentación de sistemas de información en explotación, si la revisión post-implantación comparó el sistema actual con las especificaciones pertinentes, especialmente en términos de :

- a. procedimientos de respaldo y recuperación
- b. mantenimiento y segregación de funciones
- c. pistas de Auditoría
- d. controles sobre las interfaces con otras aplicaciones y sistemas
- e. medidas de seguridad
- f. documentación distribuida a los usuarios.

2.7.3 Evaluación del cumplimiento de las especificaciones de usuario.

• **Objetivo de Control.**

La metodología de ciclo de vida de desarrollo del sistema de la organización debiera exigir que una revisión post-implantación de un sistema de información en explotación evalúe si las necesidades de los usuarios están siendo satisfechas por el sistema.

• **Directiva de Auditoría.**

Deben examinarse las exigencias de la metodología de ciclo de vida de desarrollo del sistema de la organización de que mediante una revisión post-implantación de los sistemas de información en explotación se evalúe si las necesidades de los usuarios están siendo satisfechas.

1. **Determinar**, mediante entrevistas o cuestionarios, si las revisiones post-implantación llevadas a cabo para sistemas de información en explotación seleccionadas evaluaron adecuadamente si las necesidades de los usuarios estaban siendo satisfechas con tales sistemas.

2. **Verificar** esas revisiones mediante un análisis del uso actual que se efectúa del sistema y las propuestas de modificación al sistema que se hicieron desde que el sistema se implantó.

2.7.4 Análisis de evaluación coste-beneficio.

• **Objetivo de Control.**

La metodología de ciclo de vida de desarrollo del sistema de la organización debiera exigir que una revisión post-implantación de los sistemas de información en explotación evalúe si el coste eficacia del sistema coincide con los costes y beneficios originalmente previstos para el sistema.

• **Directiva de Auditoría.**

Deben examinarse las especificaciones de la metodología de ciclo de vida de

desarrollo del sistema de la organización que disponen que, mediante una revisión post-implantación de los sistemas de información en explotación, se evalúe si el coste eficacia del sistema coincide con los costes y beneficios originalmente previstos para el mismo.

1. **Verificar**, mediante examen de la documentación de proyectos seleccionados de desarrollo o modificación de sistemas de información, la precisión del proceso de estimación de costes empleados, comparando los costes totales del proyecto con las proyecciones iniciales de las mismas.

2. **Determinar**, mediante examen de la documentación referente a proyectos de sistemas de información, el grado en que se han alcanzado los beneficios cuantificables y no cuantificables asociados con el sistema y compararlos con las estimaciones originales de proyecto con las estimaciones originales de proyecto de tales beneficios.

3. **Evaluar** la plausibilidad de las razones citadas para explicar las diferencias entre los costes y beneficios reales y estimados de proyectos seleccionados de desarrollo o modificación de sistemas de información y determinan si el comité de planificación o el comité de dirección del departamento de informática ha recibido copias de los análisis que identificaban tales diferencias.

2.7.5 Evaluación del cumplimiento de los estándares de desarrollo.

• **Objetivo de Control.**

La metodología de ciclo de vida de desarrollo de sistemas de la organización debiera exigir que una revisión post-implantación evalúen si el equipo de proyecto se mantuvo a las determinaciones de la metodología.

• **Directiva de Auditoría.**

Deben examinarse las especificaciones de la metodología de ciclo de vida del desarrollo de sistemas de la organización para que mediante una revisión post-

implantación de los sistemas de información en explotación se evalúe si el equipo de proyecto se atuvo a las determinaciones de la metodología.

1. **Verificar**, mediante examen de la documentación referente a proyectos seleccionados de desarrollo o modificación de sistemas de Información que:

a. la documentación era completa

b. se cumplieran las disposiciones de la metodología de ciclo de vida de desarrollo de sistemas de la organización

c. la participación en el proyecto de representantes de departamentos usuarios fue adecuada.

2. **Verificar** mediante entrevistas con participantes en los equipos de proyecto que los recursos de personal, la organización del equipo y las comunicaciones fueron adecuadas para proyectos seleccionados de desarrollo o modificación de sistemas de información.

2.7.6 Informe sobre los hallazgos de la revisión post-implantación.

• **Objetivo de Control.**

La metodología de ciclo de vida del desarrollo de sistemas de la organización debiera exigir que los resultados de una revisión post-implantación de un sistema de información en explotación se presentasen ante la dirección de los departamentos usuarios afectados por el sistema y a la dirección del departamento de informática.

• **Directiva de Auditoría.**

Deben examinarse las disposiciones de la metodología de ciclo de vida del desarrollo de sistema de la organización sobre que la evaluación de los resultados de una revisión post-implantación de un sistema de información en explota-

ción se presente a la dirección de los departamentos usuarios afectados por el sistema y la dirección del departamento de informática.

1. **Determinar**, mediante examen de la documentación de sistemas de información en explotación seleccionadas, si se preparó y aprobó el informe de los resultados de la revisión post-implantación.

2. **Determinar** que dichos informes se presentaron a la dirección de los departamentos usuarios afectados por el sistema y a la del departamento de informática.

3. **Verificar** la naturaleza de las acciones adoptadas en base a las recomendaciones del informe.

PARTE I - 1. CONTROLES DE GESTION.

1.5.3 Formación continuada del personal de auditoría interna.

- **Objetivo de Control.**

Aquellos miembros de la plantilla de la función de auditoría interna de la organización asignados a tareas de auditoría de sistemas de información, deberían recibir ayuda para mantener su competencia técnica mediante una formación continuada relacionada con su profesión.

- **Directiva de Auditoría.**

Deben revisarse las actividades de gestión de la función de auditoría interna de la organización para asegurar que cada auditor de sistemas de información es consciente de la responsabilidad de proseguir en su formación continuada en su profesión. Además, la dirección de ésta función debe revisarse respecto a su estímulo para que los auditores de sistemas de información participen en organizaciones profesionales, asistan a conferencias adecuadas y seminarios.

1. **Asegurar** que la Dirección de auditoría interna respalda un programa para promover la toma de conciencia por el auditor de las necesidades de formación continuada.

2. **Determinar** que la Dirección de auditoría interna promueve la participación de los auditores de sistemas de información en organizaciones profesionales, conferencias y seminarios aplicables, y otros programas de formación adecuados.

1.5.4 Rendimiento del trabajo de auditoría interna.

- **Objetivo de Control.**

Debería ejercerse un cuidado profesional adecuado en todos los aspectos del trabajo de la función de auditoría interna de la organización, incluyendo la observancia de estándares de auditoría aplicables.

- **Directiva de Auditoría.**

Deben revisarse los actos de dirección de la función de auditoría interna de la organización, para confirmar que todas las revisiones de las actividades del Departamento de Informática y de aplicaciones informatizadas se llevan a cabo con el debido celo profesional.

1. **Asegurar** que la Dirección de auditoría interna requiere que todas las auditorías sean planificadas y supervisadas de modo tal que puedan alcanzarse los objetivos de auditoría y puedan satisfacerse los estándares de auditoría pertinentes.

2. **Asegurar** que la Dirección de auditoría interna exige que, en el curso de una auditoría, se obtenga suficiente evidencia como para respaldar los hallazgos y conclusiones de que se informa.

3. **Asegurar** que la Dirección de auditoría interna exige la adhesión, durante todas las revisiones, a estándares de auditoría generalmente aceptados.

1.5.5 Informes de la función de auditoría interna.

- **Objetivo de Control.**

La función de auditoría interna de la organización debería emitir informes escritos a todos los directivos afectados, una vez terminadas sus revisiones.

- **Directiva de Auditoría.**

Deben revisarse las actividades de gestión de la función de auditoría interna de la organización para asegurar que se preparan y distribuyen informes escritos de los hallazgos, conclusiones, y recomendaciones de auditoría a todos los miembros adecuados de la dirección una vez terminada cada auditoría.

1. **Asegurar** que la dirección de auditoría interna exige que todos los informes de auditoría reflejen el propósito, ámbito y resultados de la auditoría.

2. **Asegurar** que la dirección de auditoría interna revisa cada informe de audi-

toría y lo distribuye al personal directivo apropiado.

1.6 ESPECIFICACIONES DE ORIGEN EXTERNO.

Deben considerarse las especificaciones de origen externo pertinentes a los objetivos y planes de la organización y a las responsabilidades y las actividades de la función del Departamento de Informática.

- **Objetivo de Control.**

Al planificar el trabajo de la organización y del Departamento de Informática deberían considerarse las especificaciones gubernamentales u otras externas relativas a prácticas y controles de sistemas informáticos (por ejemplo en las áreas de mantenimiento, operaciones, contabilidad y protección de la intimidad) así como la forma en que se usan los ordenadores, los programas y los datos. Debería prestarse especial atención a estos aspectos en los sectores de la economía que históricamente han sido regulados de forma rigurosa.

- **Directiva de Auditoría.**

Deben revisarse las especificaciones gubernamentales u otras externas relativas a las prácticas informáticas y a los controles y a la forma en que los ordenadores, programas y datos se utilizan y afectan a la organización, para apreciar si la dirección las ha considerado al desarrollar planes y establecer políticas, estándares y procedimientos.

1. **Identificar** aquellas especificaciones gubernamentales u otras externas relativas a las prácticas informáticas y los controles y a la forma en que ordenadores, programas y datos se usan y que son pertinentes a la organización o a las actividades del Departamento de Informática.

2. **Apreciar** si la dirección de la organización y el Departamento de Informática han considerado las especificaciones externas pertinentes al establecer planes y políticas, estándares y procedimientos.

PARTE I - 2. CONTROLES DE DESARROLLO, ADQUISICION Y MANTENIMIENTO

PARTE I: CONTROLES GENERALES Y DE APLICACIONES
CONTROLES DE EXPLOTACIÓN DE SISTEMAS DE INFORMACIÓN

CONTENIDO

3	CONTROLES DE EXPLOTACIÓN DE SISTEMAS DE INFORMACIÓN.	I-3-1
3.1	PLANIFICACIÓN Y GESTIÓN DE RECURSOS DEL DEPARTAMENTO DE INFORMÁTICA.	I-3-1
3.1.1	Presupuesto operativo anual del Departamento de Informática.	I-3-1
3.1.2	Plan de Adquisición de Equipos.	I-3-1
3.1.3	Gestión de capacidad de los equipos.	I-3-2
3.2	EXPLOTACIÓN.	I-3-2
3.2.1	Calendario de carga de trabajo.	I-3-2
3.2.2	Programación del personal.	I-3-3
3.2.3	Mantenimiento Preventivo del Material.	I-3-4
3.2.4	Gestión de Problemas.	I-3-5
3.2.5	Gestión de Cambios.	I-3-6
3.2.6	Contabilidad de Costes de Trabajos.	I-3-7
3.2.7	Procedimiento de Facturación a Usuarios.	I-3-8
3.2.8	Responsabilidades de Gestión de la Biblioteca de Soportes Magnéticos.	I-3-8
3.2.9	Sistema de Gestión de la Biblioteca de Soportes.	I-3-9
3.2.10	Identificación Externa y Control de Soportes Magnéticos.	I-3-10
3.2.11	Procedimientos de Explotación.	I-3-10
3.3	LOGICAL DE SISTEMA OPERATIVO.	I-3-10
3.3.1	Selección de Logical de Sistema.	I-3-11
3.3.2	Análisis Coste-Beneficio del Logical de Sistema.	I-3-11
3.3.3	Instalación de Cambios en el Logical de Sistema.	I-3-11
3.3.4	Mantenimiento del Logical de Sistema.	I-3-12
3.3.5	Control de Cambios en el Logical de Sistema.	I-3-12
3.3.6	Gestión de Problemas con el Logical de Sistema.	I-3-13
3.3.7	Seguridad del Logical de Sistema.	I-3-13
3.4	SEGURIDAD LÓGICA Y FÍSICA.	I-3-14
3.4.1	Responsabilidad de la Seguridad Lógica y Física.	I-3-14
3.4.2	Acceso a las Instalaciones de Ordenadores.	I-3-14
3.4.3	Acompañamiento de Visitas.	I-3-15
3.4.4	Administración de Palabras de Paso.	I-3-15
3.4.5	Informes de Violaciones y Actividad de Seguridad.	I-3-16
3.4.6	Restricciones de Acceso Lógico.	I-3-16
3.4.7	Seguridad del Acceso a Datos En Línea.	I-3-17
3.4.8	Identificación Limitada del Centro de Cálculo.	I-3-17
3.4.10	Formación y Concienciación en Procedimientos de Seguridad.	I-3-18

PARTE I - 3. CONTROLES DE EXPLOTACION.

3.5	PLANIFICACIÓN ANTE CONTINGENCIAS	I-3-18
3.5.1	Plan de Recuperación de Desastres	I-3-19
3.5.2	Seguridad del Personal y Formación en Procedimientos de Emergencia	I-3-19
3.5.3	Aplicaciones críticas de tratamiento de datos	I-3-19
3.5.4	Recursos de Ordenador Críticos	I-3-20
3.5.5	Restauración de Servicios de Telecomunicación	I-3-21
3.5.6	Respaldo: Del Centro de Cálculo y de los Equipos	I-3-21
3.5.7	Plantilla de Programación para Operaciones de Respaldo	I-3-22
3.5.8	Procedimientos de Recuperación de Ficheros	I-3-22
3.5.9	Consumibles para Recuperación de Desastres	I-3-23
3.5.10	Pruebas del Plan de Recuperación de Desastres	I-3-23
3.5.11	Reconstrucción del Centro de Cálculo del Departamento de Informática	I-3-23
3.5.12	Procedimientos de Respaldo Manual de los Departamentos Usuarios	I-3-24

* * *

3 CONTROLES DE EXPLOTACIÓN DE SISTEMAS DE INFORMACIÓN.

3.1 PLANIFICACIÓN Y GESTIÓN DE RECURSOS DEL DEPARTAMENTO DE INFORMÁTICA.

Deben planificarse, aportarse y gestionarse los recursos organizativos adecuados para apoyar el logro de los objetivos aprobados para el Departamento de Informática.

3.1.1 Presupuesto operativo anual del Departamento de Informática.

* **Objetivo de Control.**

La alta dirección de la organización debe establecer un presupuesto operativo anual del departamento de informática.

* **Directiva de Auditoría.**

Debe revisarse, en cuanto a si es completo y adecuado, el presupuesto operativo anual establecido por la alta dirección de la organización para el departamento de informática.

1. **Determinar** si el proceso seguido en la preparación del presupuesto operativo del departamento de informática es participativo, contribuyendo a su preparación la dirección de las principales unidades del departamento, tales como desarrollo de sistemas, preparación, explotación, transmisión de datos y apoyo técnico.

2. **Determinar** que el presupuesto operativo del departamento de informática ha sido adecuadamente revisado por la dirección general del departamento y aprobado por su comité de planificación o por su comité de dirección o por aquellos miembros de la alta dirección de la

organización responsables de supervisar esta función.

3. **Determinar** si las diversas categorías de gasto del departamento de informática -- tales como ordenadores, mantenimiento de ordenadores, adquisición de logical, mantenimiento de logical, sueldos y salarios, equipo de oficina y mantenimiento de oficina -- han sido adecuadamente establecidos y clasificados.

4. **Apreciar** si el nivel de apoyo proporcionado por el presupuesto operativo anual aprobado para el departamento de Informática es suficiente para dar apoyo a los objetivos establecidos para el departamento.

3.1.2 Plan de Adquisición de Equipos.

* **Objetivo de Control.**

Debe establecerse un plan de adquisición de equipos para el departamento de Informática que refleje las especificaciones para satisfacer las necesidades tanto a corto como a largo plazo.

* **Directiva de Auditoría.** Debe revisarse el plan de adquisición de equipos del departamento de informática.

1. **Obtener** una copia del plan de adquisición de equipos del departamento de Informática, y determinar su situación.

2. **Discutir** con la dirección del departamento los elementos del plan de adquisición de equipos del departamento de informática, para **determinar** si se compara regularmente dicho plan con el plan de negocio del departamento, y para determinar su comprensión y uso del plan coordinado.

3. **Revisar** el actual entorno físico del Departamento de Informática para **determinar** en adecuación para acomodar los equipos actualmente instalados y los nuevos a ser añadidos bajo el plan de adquisición de equipos aprobados.

4. **Comparar** el plan de adquisición de equipos del departamento de Informática

PARTE I - 3. CONTROLES DE EXPLOTACION.

ca con sus planes de tratamiento de datos e **identificar** cualesquiera deficiencias del primero.

5. **Determinar** si el plan de adquisición de equipos del departamento de informática ha tomado en consideración la probable obsolescencia tecnológica tanto del equipo actualmente instalado cuanto del nuevo equipo incluido en el plan de adquisición.

6. **Verificar** la adecuación de la documentación de la especificación de equipos de logical, de especificaciones de instalación, y probables plazos de entrega asociados con la adquisición planificada, cuando los planes del departamento de informática necesitan para implementar un nuevo sistema la adición de equipos complementarios o sustitutivos.

3.1.3 Gestión de capacidad de los equipos.

• Objetivo de Control.

El departamento de Informática debiera establecer un plan para la revisión continua del rendimiento y capacidad de los equipos.

• Directiva de Auditoría.

Debe evaluarse el proceso que el departamento de Informática tiene establecido para el seguimiento del rendimiento y capacidad de los equipos.

1. **Obtener** una copia del plan de seguimiento del rendimiento de los equipos del departamento de informática, y **entrevistar** a las personas clave designadas en el plan a fin de **determinar** su situación y funcionamiento con éxito.

2. **Comparar** los criterios de decisión especificados en el plan de seguimiento de rendimiento de los equipos del departamento de informática con los resultados históricos obtenidos de las diarias incidencias, sistema de contabilidad de trabajos, calendarios e informes de mantenimiento preventivos y diarios de distribución de informes a efectos de **deter-**

minar la validez del proceso de seguimiento.

3.2 EXPLOTACIÓN.

Los recursos en ordenadores del departamento de informática debieran ser usados efectivamente, mediante el mantenimiento de un calendario establecido de explotación, permitiendo costes de facturación razonables y protegiendo los ficheros de datos de pérdida.

3.2.1 Calendario de carga de trabajo.

• Objetivo de Control.

Debiera haber un calendario de todas las tareas de tratamiento de datos por el departamento de informática, para asegurar el uso eficiente de sus instalaciones y satisfacer las especificaciones de sus usuarios.

• Directiva de Auditoría.

Debe revisarse el procedimiento de confección de calendarios de carga de trabajo seguido por el departamento de informática, a fin de determinar si todas las tareas de tratamiento de datos están siendo completados de forma oportuna y eficiente.

1. **Obtener** una lista de todas las aplicaciones de tratamiento de datos cuya explotación está programada regularmente dentro del departamento de informática junto con sus fechas de vencimiento de entrada, tiempos de preparación de datos, tiempo estimado de tratamiento, y fechas de las mismas (utilícense, si están disponibles, los informes generados por un sistema automático de gestión del calendario).

2. **Obtener** una lista de todas las aplicaciones procesadas por el departamento de informática de forma irregular o con baja prioridad, junto con los datos pertinentes de calendario y horario.

3. **Determinar** si los usuarios de aplicaciones seleccionadas de tratamiento

de datos participan en la preparación del calendario del departamento de informática, en los que respecta a la entrada de documentos fuente y la salida de informes. Cerciorarse de que los resultados de esta participación se reflejan en un acuerdo escrito sobre nivel de servicio.

4. **Examinar** el calendario de explotación llevado por el departamento de informática para familiarizarse con como se logra la distribución de la carga de trabajo. **Determinar** cuando tienen lugar las puntas de proceso -- por ejemplo a final de mes, final de trimestre o final de año --.

5. **Determinar** si la capacidad de equipos disponibles en el departamento de informática es suficiente para satisfacer las demandas punta de tratamiento y para seguir brindando un nivel adecuado de servicio a los usuarios durante ciclos temporales del equipo.

6. **Cerciorarse** de si el departamento de informática querrá informes de rutina de identificación genera informes de rutina de identificar el trabajo que fue procesado después de cuando estaba programada hacerse. Analizarlas razones por las cuales dicho trabajo no está siendo acabado en plazo.

7. **Determinar** si el departamento de informática ha establecido prioridades de tratamiento para cada aplicación informática.

8. **Determinar** si se han asignado suficientes recursos de equipo al departamento de informática para su actividad de pruebas de aceptación, para asegurar que actividades de prueba pertinentes se completan oportunamente en tiempo.

9. **Cerciorarse** de que el material y logical empleado por la actividad de pruebas del departamento de informática son suficientemente similares a los empleados en el entorno rutinario de explotación para permitir identificar los problemas potenciales de tratamiento

de una manera oportuna a tiempo durante las pruebas de aceptación.

10. **Determinar** si los trabajos urgentes o peticiones de tratamientos son programados para su explotación por el departamento de Informática de forma congruente con sus niveles de prioridad asignados.

11. **Verificar** que las aplicaciones de tratamiento de datos del departamento de informática están identificadas por su prioridad en la hipótesis de un deslizamiento en el calendario de explotación.

12. **Evaluar** si el procedimiento de programación de explotación utilizado por el departamento de Informática logra un óptimo uso de los recursos de ordenador, al tiempo que satisface las especificaciones de servicio.

3.2.2 Programación del personal.

* Objetivo de Control.

Debieran asignarse a explotación del departamento de informática suficientes recursos humanos adecuadamente cualificados y supervisados. Para asegurar que todas sus actividades se llevan a cabo eficazmente.

* Directiva de Auditoría.

Debe revisarse la adecuación de los recursos humanos suministrados a explotación del departamento de informática.

1. **Examinar** el organigrama actual de explotación del departamento de informática e identificar las diversas actividades en el mismo (estas pueden incluir, pero no limitarse al control de entrada de datos, biblioteca de cintas, programación de la explotación, operaciones de tratamiento de datos y distribución de salidas).

3. **Determinar** si al personal de cada turno se le ha asignado la responsabilidad de cada actividad de tratamiento

PARTE I - 3. CONTROLES DE EXPLOTACION.

de datos del departamento de informática. Determinar si en cada turno trabaja más de una persona, para asegurar que todas esas actividades están adecuadamente dotados de recursos humanos.

4. **Obtener** copias de las descripciones de puesto de trabajo de aquellos miembros de la plantilla del departamento de informática asignadas a explotación y **determinar** que sus responsabilidades han sido adecuadamente documentadas y se le han comunicado adecuadamente.

5. **Obtener** el plan de turnos de la plantilla de explotación del departamento de informática para una semana o más, y determinar si todas las áreas funcionales están adecuadamente dotadas de plantilla a la luz del volumen de trabajo a realizar y del entorno en que tiene lugar.

6. **Observar** el trabajo realizado por todas las actividades de explotación del Departamento de Informática y **determinar** si coincide con las actividades definidas en el organigrama del Departamento.

7. **Determinar** si para cada turno y actividad de explotación del Departamento de Informática se lleva un diario de problemas surgidos o se pasan notas entre turnos. **Revisar** dichos registros para determinar el efecto de problemas seleccionados sobre la gestión práctica de calendario del personal.

8. **Determinar**, mediante observación, si todas las actividades de explotación del Departamento de Informática cuenta con la plantilla adecuada en períodos tales como pausas para el desayuno, comida, etc.

9. **Determinar**, mediante observación, si hay adecuada supervisión en todas las operaciones de tratamiento de datos del Departamento de Informática.

10. **Determinar** si los calendarios de asignación de personal de explotación del Departamento de Informática coinciden con las fluctuaciones previstas de carga de trabajo y si dichos calendarios se utilizan realmente.

11. **Determinar** si los calendarios de asignación de personal de explotación del Departamento de Informática incluye tiempo adecuado para formación individual y reuniones de plantilla.

12. **Determinar**, mediante entrevistas a la dirección de explotación del Departamento de Informática, cuán a menudo se revisan los calendarios de asignación de personal para reflejar cosas tales como cambios en la carga de trabajo y vacaciones.

13. **Considerar**, como una evaluación global de la utilización de la plantilla asignada a explotación en el Departamento de Informática, el impacto de cosas tales como la introducción de nuevos equipos o logical, reducciones en el presupuesto operativo del Departamento, y rotación de la propia plantilla.

3.2.3 Mantenimiento Preventivo del Material

• **Objetivo de Control.**

El Departamento de Informática debe programar el mantenimiento periódico rutinario del material para reducir la posibilidad e impacto de fallos de funcionamiento.

• **Directiva de Auditoría.**

Debe revisarse el calendario del Departamento de Informática para mantenimiento periódico y su cumplimiento de la política de la alta dirección de la organización aplicable, al igual que deben determinarse los calendarios de mantenimiento pertinentes del vendedor o los establecidos en los términos contractuales.

1. **Revisar** la documentación suministrada por el vendedor al igual que los

contratos de alquiler o leasing de material pertinentes para **determinar** la frecuencia de mantenimiento preventivo prescrita para cada dispositivo utilizado por el Departamento de Informática.

2. **Verificar** que no se está llevando de cabo durante períodos de carga punta.

3. **Comparar** el calendario de mantenimiento preventivo del material operado por el Departamento de Informática con su planificación de carga de trabajo de explotación, y **determinar** si el tratamiento de aplicaciones críticas o sensibles está siendo afectado negativamente por las actividades de mantenimiento planificado.

4. **Verificar** que el calendario de explotación del Departamento de Informática es lo bastante flexible como para acomodar el mantenimiento preventivo del material requerido.

5. **Revisar** los registros de mantenimiento de cada dispositivo utilizado en el proceso de explotación del Departamento de Informática para **determinar** tanto la necesidad de mantenimiento preventivo adicional cuanto la frecuencia aproximada del mantenimiento no planificado necesario.

6. **Verificar** que el calendario de explotación del Departamento de Informática es lo bastante flexible como para acomodar tiempos de no funcionamiento del sistema razonablemente previstos para mantenimiento no programado.

7. **Determinar** si hay material de recambio o material tolerante a fallos disponible para el tratamiento de aquellos programas de aplicación del Departamento de Informática que exigen un alto nivel de disponibilidad del sistema.

3.2.4 Gestión de Problemas

* **Objetivo de Control.** Debería revisarse periódicamente por la alta

dirección de la organización el funcionamiento del Departamento de Informática en el logro de sus compromisos de suministrar un nivel programado de servicio de tratamiento de datos, para asegurar que todos los problemas surgidos durante la explotación se registran, analizan y resuelven de manera oportuna en el tiempo.

* Directiva de Auditoría.

Deben reunirse y evaluarse pruebas de las revisiones periódicas por la alta división de la organización del funcionamiento del servicio programado del tratamiento de datos por el Departamento de Informática. Debe evaluarse lo adecuado de la elaboración y seguimiento de los calendarios de los recursos de ordenador empleados por el Departamento para tratamiento en línea. Y debe evaluarse la adecuación y eficacia del procedimiento empleado por el Departamento para registrar, evaluar, y resolver cualesquiera problemas operativos o de tratamiento que hayan surgido.

1. **Entrevistar** a la dirección de explotación del Departamento de Informática para **cerciorarse** de que se mantienen registros para evaluar el funcionamiento real del Departamento en el logro de los calendarios de servicio de tratamiento de la información.

2. **Determinar** si la dirección de explotación del Departamento Informática utiliza tales registros para gestionar la programación de sus actividades de servicio.

3. **Revisar** los registros de funcionamiento de explotación del Departamento de Informática para **determinar** dónde hay puntos débiles, y **determinar** para programas de aplicación seleccionados si los momentos en que el trabajo terminado estaba listo para ser distribuido cumplían los calendarios pertinentes.

4. **Determinar**, a partir de un análisis funcional de los registros de explotación del Departamento de Informática aquellos programas de aplicación que están

PARTE I - 3. CONTROLES DE EXPLOTACION.

sufriendo erosión en su funcionamiento y **analizar e informar** sobre cualesquiera ritmos o tendencias recurrentes puestos de manifiesto.

5. **Verificar** que la dirección de explotación del Departamento de Informática hace un control y seguimiento del flujo del trabajo de los tratamientos y de todas las variaciones del calendario de explotación y determinar que el tiempo de retraso transcurrido se registra para todas esas variaciones.

6. **Verificar** que las razones de demoras en el tratamiento programado de programas de aplicación se identifican por la dirección de explotación del Departamento de Informática en base a la causa responsable del retraso.

7. **Determinar** si la alta dirección de la organización ha determinado, mediante una encuesta a la dirección de los departamentos usuarios si los calendarios de explotación llevados por el Departamento de Informática satisfacen sus necesidades de servicio. **Entrevistar** a directivos seleccionados de departamentos de usuarios y validar los resultados de la encuesta.

8. **Determinar** si la alta dirección de la organización ha establecido objetivos de funcionamiento para el tratamiento en línea del Departamento de Informática.

9. **Revisar** el procedimiento seguido por el Departamento de Informática para recoger estadísticas del funcionamiento de su tratamiento en línea para **determinar** si se está informando sobre resultados exactos y completos y si las percepciones por los departamentos usuarios del procedimiento del Departamento están de acuerdo con los datos recogidos por este procedimiento.

10. **Determinar** si el Departamento de Informática para la gestión de problemas de tratamiento de datos.

11. **Determinar** si todos los problemas surgidos en explotación del Departamento de Informática se están registrando y se emplean diarios y ficheros generados por el sistema para verificar esto.

12. **Evaluar** la adecuación del procedimiento del Departamento de Informática para evaluar las causas de los problemas de tratamiento de datos y **determinar** si se están identificando problemas significativos y recurrentes y se están tomando acciones para prevenir su recurrencia.

13. **Determinar** si las solución de problemas específicos de tratamiento de datos se ha asignado a miembros específicos de la plantilla del Departamento de Informática y **cerciorarse** de si se han establecido prioridades sobre cuán rápidamente deben resolverse problemas específicos.

14. **Determinar** si los miembros designados del Departamento de Informática resolvieron oportunamente en el tiempo problemas de tratamiento seleccionados y si el registro de la resolución del problema era completo y razonable.

3.2.5 Gestión de Cambios

• Objetivo de Control.

El impacto de cambios en material y logical debería reflejarse en el calendario de explotación llevado por el Departamento de Informática y todos esos cambios deberían ser probados, puestos en calendario y aprobados antes de ser implantados por el Departamento.

• Directiva de Auditoría.

Debe apreciarse el impacto de los cambios en material y logical sobre la programación de explotación del Departamento de Informática.

1. **Entrevistar** al individuo realmente responsable de la coordinación del calendario de explotación del Departamento de Informática para **determinar** si a esa persona se le advierte con tiempo de los cambios en el logical del sistema o de aplicación y en la configuración del material.

2. **Verificar** que la dirección del Departamento de Informática ha desarrollado y puesto en vigor calendarios de cambios que permiten tiempo para la adecuada instalación y prueba de material y logical.
3. **Verificar** que la dirección de explotación del Departamento de Informática es informada, antes de su implantación, de los nuevos sistemas, calendarios de instalación y necesidades de tiempo de prueba.
4. **Verificar** que, antes de la implantación de cambios de material y logical, la documentación de operación empleada en explotación del Departamento de Informática es adecuadamente revisada.
5. **Seleccionar** una muestra de cambios de material y logical que han afectado al calendario de explotación del Departamento de Informática y **comparar** el calendario anterior al cambio con el actual para **determinar** si los planes de cambio se han cumplido a tiempo.
6. **Cerciorarse** de que las prácticas de comunicación, dentro del Departamento de Informática entre programadores de sistemas, programadores de aplicaciones y personal de explotación aseguran que los cambios y pruebas de material y logical son coordinados adecuadamente.
7. **Evaluar** la eficacia con que la plantilla de explotación del Departamento de Informática establece los calendarios para pruebas de programas y **asegurar** que éstos no interfieren a los compromisos normales de tratamiento de programas de aplicación.

3.2.6 Contabilidad de Costes de Trabajos

• **Objetivo de Control.**

La alta dirección debería evaluar periódicamente los resultados de los procedimientos de contabilidad de costes de trabajos del Departamento de Informática, a la luz de los otros sistemas de me-

dición económica-financiera de la organización, para determinar que los beneficios derivados del tratamiento de datos son mayores que los costes incurridos por el tratamiento.

• **Directiva de Auditoría.** Deben revisarse los procedimientos de contabilidad de costes de trabajo del Departamento de Informática y determinarse si son apropiados.

1. **Revisar** el potencial de información de los procedimientos de contabilidad de costes de trabajos del Departamento de Informática y **determinar** que los informes están siendo usados por la dirección del Departamento para **comparar** el funcionamiento de la explotación con estándares u objetivos establecidos.
2. **Revisar** las convenciones del Departamento de Informática para dar nombres y números a los trabajos de tratamiento de datos, en cuanto a su claridad y conformidad con los estándares del Departamento.
3. **Comparar** los registros generados por el proceso de contabilidad de costes de trabajos del Departamento de Informática con el registro de consola de explotación o con otros sistemas de medida de los recursos de ordenador para **asegurar** que se está registrando todo el tiempo en que el equipo está en operación.
4. **Cerciorarse** de si el procedimiento de contabilidad de costes de trabajo del Departamento de Informática se usa para facturar a los departamentos usuarios los costes incurridos y **entrevistar** a usuarios seleccionados para determinar si consideran justo y comprensible dicho procedimiento.

PARTE I - 3. CONTROLES DE EXPLOTACION.

3.2.7 Procedimiento de Facturación a Usuarios

- **Objetivo de Control.**

El Departamento de Informática debería mantener procedimientos de facturación a usuarios que estimulen el uso adecuado de los recursos de ordenador y aseguren un trato justo a los departamentos usuarios y sus necesidades.

- **Directiva de Auditoría.**

Deben revisarse los procedimientos de facturación a usuarios del Departamento de Informática.

1. **Establecer** si el Departamento de Informática mantiene un procedimiento de facturación a usuarios por el empleo de sus recursos de ordenador.
2. **Entrevistar** a directivos seleccionados de departamentos usuarios para **determinar** si están informados de los procedimientos de facturación de las operaciones de tratamiento de datos del Departamento de Informática, y determinar si están satisfechos con la forma en que tales procedimientos se vienen aplicando.
3. **Determinar**, en los casos en que explotación del Departamento de Informática es tratada como un centro de costes, si la alta dirección de la organización ha establecido que los costes asignados a los departamentos usuarios son inferiores que los que oficinas de servicio independientes facturarían.
4. **Determinar**, en los casos en que explotación del Departamento de Informática es tratada como un centro de beneficios, si la alta dirección de la organización ha comparado las tarifas cargadas a los departamentos usuarios con los que facturarían oficinas de servicio independientes, y que el margen de beneficio del Departamento parece congruente con las directivas de la organización sobre la materia.
5. **Evaluar** si las tarifas cargadas a los departamentos usuarios estimulan su uso más eficaz de los recursos de ordenador del Departamento de Informática y

determinar si el empleo de tarifas diferenciales para utilización fuera de puntas o la asignación de prioridades variables para necesidades de tratamiento variables han sido consideradas por todos los interesados.

3.2.8 Responsabilidades de Gestión de la Biblioteca de Soportes Magnéticos

- **Objetivo de Control.**

Las responsabilidades de gestión de la biblioteca de soportes magnéticos (cintas, cartuchos, discos y diskettes) debería ser asignada a miembros específicos de la plantilla del Departamento de Informática y el Departamento debería establecer procedimientos de gestión interna para proteger los contenidos de la biblioteca de soportes.

- **Directiva de Auditoría.**

Debe revisarse la adecuación de la asignación de responsabilidades de gestión de la biblioteca de soportes dentro del Departamento de Informática y debe apreciarse la adecuación de los procedimientos de gestión interna establecidos por el Departamento para proteger los recursos que son los datos.

1. **Asegurar** que las responsabilidades de bibliotecario de soportes se han asignado a individuos específicos de explotación del Departamento de Informática.
2. **Asegurar** que la biblioteca de soportes está emplazada en un área, dentro del Departamento de Informática, que está a seguro de daños de fuego, agua y sabotaje y que es operada por individuos que funcionan independientemente de los operadores y programadores del Departamento.
3. **Determinar** mediante observación que los procedimientos de control de soportes magnéticos del Departamento de Informática se cumplen cuando el

bibliotecario de soportes no está presente.

4. **Determinar** si hay procedimientos para controlar el acceso a y el uso de todos los ficheros de explotación de programas de aplicación del Departamento de Informática.

5. **Verificar** la existencia de cualquier instalación remota que pueda ser utilizada por el Departamento de Informática para almacenar copias de ficheros de datos críticos mantenidos en la biblioteca de soportes del Departamento y determinar, mediante visita a las mismas que en ellas se están conservando realmente copias de ficheros seleccionados.

6. **Examinar** los procedimientos del Departamento de Informática para la creación de copias de ficheros a ser almacenados en las instalaciones remotas y **determinar** si el período de tiempo transcurrido entre copia y copia es razonable.

3.2.9 Sistema de Gestión de la Biblioteca de Soportes

* **Objetivo de Control.**

El Departamento de Informática debería establecer procedimientos para asegurar que los contenidos de su biblioteca de soportes se inventarían periódicamente, que todas las discrepancias puestas de manifiesto por dicho inventario se corrigen en tiempo oportuno y que se adoptan medidas para conservar la integridad de los soportes magnéticos.

* **Directiva de Auditoría.**

Deben examinarse los procedimientos del Departamento de Informática para inventariar los contenidos de su biblioteca de soportes y para limpiar y conservar los soportes magnéticos que la integran.

1. **Revisar** las posibles funciones de cualquier logical de Sistema de Gestión de Bibliotecas de Soportes que pueda

venir utilizándose por el Departamento de Informática.

2. **Determinar** si los bibliotecarios de soportes del Departamento de Informática verifican periódicamente la exactitud de la información creada y mantenida por un Sistema de Gestión de Bibliotecas de Soportes. Hacer muestreos selectivos de registros del Sistema de Gestión de Bibliotecas de Soportes, para cerciorarse de que son exactos y completos.

3. **Verificar** que los registros de los inventarios de contenido de la biblioteca de soportes del Departamento de Informática especifican el número del soporte, el período de retención, quién lo custodia actualmente y su localización física.

4. **Seleccionar** una muestra aleatoria de los contenidos inventariados de la biblioteca de soportes del Departamento de Informática y asegurar de que tienen identificación adecuada mediante etiquetas internas.

5. **Verificar** que las etiquetas internas empleadas con los soportes de la biblioteca de soportes de la biblioteca de informática identifican, al menos:

- a. nombre del fichero
- b. fecha de creación
- c. número del programa que lo creó
- d. período de retención del soporte
- e. número de registros o bloques contenidos en el soporte.

6. **Revisar** los procedimientos del Departamento de Informática para restringir la utilización del logical que puentee la comprobación de etiquetas internas y **determinar** que dichos procedimientos son razonables y eficaces.

7. **Determinar** si los procedimientos de conservación de los soportes magnéticos

PARTE I - 3. CONTROLES DE EXPLOTACION.

del Departamento de Informática especifican un ciclo periódico de limpieza de los soportes de la biblioteca y **revisar** los registros pertinentes para asegurar que eso se está haciendo.

8. **Verificar** que el Departamento de Informática ha establecido estándares de funcionamiento y puesta fuera de servicio de soportes individuales y que el bibliotecario pone fuera servicio soportes o borra datos de ficheros de conformidad con dichos estándares.

3.2.10 Identificación Externa y Control de Soportes Magnéticos

* **Objetivo de Control.**

El Departamento de Informática debería establecer estándares para la identificación externa de los soportes magnéticos y para el control de su movimiento físico.

* **Directiva de Auditoría.**

Deben revisarse los procedimientos del Departamento de Informática para la identificación externa de los soportes magnéticos y para el control de su movimiento físico.

1. **Asegurar** que el Departamento de Informática tiene procedimientos y estándares adecuados para identificar externamente, conservar, controlar el movimiento y proteger sus soportes magnéticos.

2. **Observar** los procedimientos del Departamento de Informática para trasladar soportes magnéticos para ser procesados y devueltos a la biblioteca y **verificar** que los estándares y procedimientos del Departamento se están cumpliendo.

3. **Asegurar** que se llevan a cabo revisiones periódicas de las etiquetas externas de los soportes magnéticos del Departamento de Informática, para **verificar** la exactitud de las prácticas de identificación de ficheros.

4. **Determinar** que el Departamento de Informática conserva registros adecua-

dos de todos los soportes magnéticos recibidos de o enviados a terceros.

3.2.11 Procedimientos de Explotación

* **Objetivo de Control.**

El Departamento de Informática debería establecer procedimientos estándar de explotación, y éstos deberían ser revisados periódicamente, para determinar que son efectivos y que se cumplen.

* **Directiva de Auditoría.**

Deben revisarse los procedimientos estándar de explotación del Departamento de Informática.

1. **Determinar** que los procedimientos estándar de explotación del Departamento de Informática cubren todos los procesos significativos de los equipos, incluyendo arranques en frío y rutinas de re arranque y recuperación.

2. **Entrevistar** a la dirección del Departamento de Informática para **determinar** la extensión con que los procedimientos estándar de explotación se revisan periódicamente para asegurar que son eficaces y que se cumplen.

3. **Determinar** si para todos los programas de aplicación de que dispone explotación del Departamento de Informática y para todos los equipos que requieren intervención de operadores y para todas las aplicaciones de logical de sistemas existen manuales de operación.

3.3 LOGICAL DE SISTEMA OPERATIVO

El Departamento de Informática debería usar procedimientos estándar para identificar, seleccionar, programar, probar, implementar y controlar el logical de sistema operativo.

3.3.1 Selección de Logical de Sistema

• **Objetivo de Control.**

El Departamento de Informática debería seguir un procedimiento estándar para identificar todos los programas de logical de sistema potenciales que satisfarán sus especificaciones operativas.

• **Directiva de Auditoría.**

Debe revisarse el procedimiento seguido por el Departamento de Informática para identificar y seleccionar todos los programas de logical de sistema potenciales que satisfarán sus especificaciones operativas.

1. **Determinar** si el Departamento de Informática ha formulado una arquitectura técnica global y **cerciorarse** de que ésta contempla tanto los planes de negocio a largo plazo de la organización cuanto las innovaciones probables en las técnicas informáticas.

2. **Obtener** un inventario de todo el logical de sistema del Departamento de Informática y la documentación del vendedor que cubre las capacidades de tales productos, identifica las posibles debilidades de control asociadas con su uso y describe las opciones de control ofrecidas por tales productos.

3. **Revisar** el procedimiento del Departamento de Informática para seleccionar logical de sistema. **Determinar**, mediante la evaluación de una muestra de logical de sistema recientemente instalado si se están satisfaciendo los requisitos de la organización.

3.3.2 Análisis Coste-Beneficio del Logical de Sistema

• **Objetivo de Control.**

El procedimiento utilizado por el Departamento de Informática para seleccionar logical de sistema debería incluir una comparación entre costes y beneficios de varias alternativas distintas.

• **Directiva de Auditoría.**

Debe revisarse el procedimiento de análisis de coste-beneficio utilizado por el Departamento de Informática para seleccionar logical de sistema.

1. **Seleccionar** una muestra de adquisiciones de logical de sistema por el Departamento de Informática, para **determinar** si, durante la evaluación de tales productos, se han considerado los siguientes aspectos:

- a. Los costes financieros directos asociados con la utilización del producto.
- b. El coste de las modificaciones al producto y del mantenimiento por el proveedor.
- c. Los requisitos de equipos y la capacidad del producto.
- d. Las necesidades de formación y apoyo técnico asociadas con la utilización del producto.
- e. El impacto del producto en la fiabilidad del proceso.
- f. El aumento o disminución en la seguridad de los datos asociado con la utilización del producto.
- g. La dirección a largo plazo y la estabilidad financiera de las operaciones del proveedor.

3.3.3 Instalación de Cambios en el Logical de Sistema

• **Objetivo de Control.**

Los cambios al logical del sistema empleados por el Departamento de Informática deberían ser probados detalladamente antes de comenzar su utilización en operaciones regulares de tratamiento de datos.

• **Directiva de Auditoría.**

Debe revisarse el procedimiento empleado por el Departamento de Informática

PARTE I - 3. CONTROLES DE EXPLOTACION.

para probar los cambios a logical de sistema ya instalado, antes de comenzar su utilización en operaciones regulares de tratamiento de datos.

1. Obtener una lista de los últimos cambios introducidos en el logical de sistema empleado por el Departamento de Informática.
2. Determinar si el Departamento de Informática ha establecido un plan escrito para la prueba de cambios en el logical de sistema. Determinar si las pruebas se han completado como se había planificado, si los problemas puestos de manifiesto durante las pruebas fueron identificados y resueltos adecuadamente, y si se volvieron a ejecutar pruebas tras los cambios.
3. Determinar si en el Departamento de Informática existen instalaciones de prueba adecuadas para brindar una seguridad razonable de que cualesquiera problemas con los cambios en el logical de sistema se identificarán antes de ponerlos en el entorno de explotación.
4. Determinar si el Departamento de Informática programa la instalación de los cambios en el logical de sistema cuando se puede esperar razonablemente que tenga lugar un impacto mínimo sobre la explotación.
5. Determinar si a los programadores del Departamento de Informática y a los usuarios del logical de sistema se les notifican adecuadamente los cambios en el producto.

3.3.4 Mantenimiento del Logical de Sistema

• Objetivo de Control.

Todas las actividades de mantenimiento de logical de sistema debieran documentarse de modo que satisfagan los estándares del Departamento de Informática.

• Directiva de Auditoría.

Deben revisarse los procedimientos del Departamento de Informática para documento el mantenimiento de logical de sistema.

1. Revisar los procedimientos del Departamento de Informática para mantenimiento de logical de sistema y determinar si todos los cambios introducidos en estos productos están documentados. Verificar que la documentación contiene una historia de quién hizo el cambio, cuándo se hizo el cambio, y una descripción del mismo.
2. Determinar la extensión con la que la versión de logical de sistema empleado por el Departamento de Informática es soportada por el proveedor.

3.3.5 Control de Cambios en el Logical de Sistema

• Objetivo de Control.

Todo el logical de sistema debiera tenerse en bibliotecas de programas separadas y protegidas, en el Departamento de Informática.

• Directiva de Auditoría.

Deben revisarse las bibliotecas usadas por el Departamento de Informática para tener el logical de sistema.

1. Obtener una lista de las bibliotecas de prueba y explotación utilizadas por el Departamento de Informática para tener el logical de sistema.
2. Determinar si el acceso de las bibliotecas que tienen el logical de sistema del Departamento de Informática está limitada por la necesidad del individuo, relacionada con su trabajo, de tener dicho acceso.
3. Revisar los controles establecidos por el Departamento de Informática para asegurar que los programadores de sistemas no introducen cambios en dichos productos sin probarlos y documentarlos adecuadamente.

4. Determinar el nivel de autorización que se exige a los programadores de sistemas del Departamento de Informática para traspasar los cambios en estos productos al entorno de explotación. Seleccionar una muestra de cambios recientes en el logical de sistema para verificar que se obtuvo la autorización necesaria para implantarlos.

3.3.6 Gestión de Problemas con el Logical de Sistema

* Objetivo de Control.

Todos los problemas de explotación experimentados por el Departamento de Informática que puedan ser atribuidos al logical de sistema deben registrarse, analizarse y resolverse.

* Directiva de Auditoría.

Debe revisarse el procedimiento de gestión de problemas con el logical de sistema del Departamento de Informática.

1. Revisar los procedimientos del Departamento de Informática para identificar y documentar problemas con el logical de sistema y verificar que se están registrando todos los problemas mediante una comprobación de los registros de los problemas pertinentes con los diarios y ficheros del sistema pertinentes.

2. Determinar si los registros de problemas con el logical de sistema del Departamento de Informática identifican la gravedad del problema, registran la asignación de su análisis y solución a individuos concretos y especifican la puntual resolución del problema.

3. Revisar las causas y frecuencia de los problemas recurrentes con el logical de sistema, en el Departamento de Informática, y cerciorarse de si el proceso de control de cambios debiera haber prevenido tales problemas.

3.3.7 Seguridad del Logical de Sistema

* Objetivo de Control.

El logical de sistema instalado por el Departamento de Informática no debiera poner en peligro la integridad de los datos y programas almacenados en el ordenador.

* Directiva de Auditoría.

Debe revisarse el impacto del logical de sistemas del Departamento de Informática sobre la seguridad de los datos que se procesan.

1. Revisar las posibilidades de puentear las restricciones de acceso de seguridad lógica ya existentes de las brindadas por el logical de sistema utilizado por el Departamento de Informática, y determinar si el Departamento ha establecido procedimientos para restringir tales posibilidades.

2. Revisar las capacidades que el logical de sistema utilizado por el Departamento de Informática tienen para interrumpir el entorno de explotación y determinar si existe en el Departamento un procedimiento para limitar el acceso a esas capacidades.

3. Determinar qué terminales han sido habilitados con consolas de sistema, bajo el logical de sistema actualmente usado por el Departamento de Informática y verificar que las medidas de seguridad física y lógica existentes restringen adecuadamente el acceso a dichas consolas de sistema.

4. Determinar si las palabras de paso suministradas por el proveedor de logical de sistema se cambiaron por el Departamento de Informática en el momento de la instalación como un procedimiento de rutina.

PARTE I - 3. CONTROLES DE EXPLOTACION.

3.4 SEGURIDAD LÓGICA Y FÍSICA

El acceso a los recursos de ordenador del Departamento de Informática debiera estar limitado a aquellos individuos que tengan necesidad documentada y autorizada de efectuar dicho acceso. Para proteger los recursos de ordenador del Departamento contra utilización o modificación no autorizadas, daño o pérdida, debieran establecerse estratos de controles de acceso lógicos y físicos.

3.4.1 Responsabilidad de la Seguridad Lógica y Física

• Objetivo de Control.

La responsabilidad de asegurar la seguridad, tanto lógica como física, de los activos de información de la organización debiera estar asignada a un director de seguridad de la información, dependiente de la alta dirección de la organización. Dicha persona no debiera tener responsabilidad alguna de programación, operación de equipos, o entrada de datos a ser procesados por el Departamento de Informática.

• Directiva de Auditoría.

Deben revisarse los procedimientos de la organización para asegurar la seguridad, tanto lógica como física, de sus activos de información.

1. Revisar el organigrama de la organización para determinar si se ha nombrado un director de seguridad de la información y si dicha persona depende de algún miembro de la alta dirección de la organización.
2. Revisar la declaración de política de seguridad de la información de la organización para determinar si define claramente las responsabilidades, en esos temas, de usuarios, dirección y administradores de la seguridad.
3. Entrevistar al director de seguridad de la información de la organización, si es que esa posición está cubierta, o a otros empleados a quienes se hayan

asignado responsabilidades de la seguridad de la información, para determinar si su comprensión de las tareas que tienen asignadas es congruente con la declaración de política de seguridad de la información de la organización.

4. Entrevistar a personal seleccionado del Departamento de Informática para determinar el grado de su concienciación general sobre la importancia de la seguridad lógica y física de la información y del cumplimiento de las determinaciones específicas de la declaración de política de seguridad de la información de la organización.

5. Revisar los procedimientos que la organización pueda tener para identificar riesgos potenciales para la seguridad de la información planteados por los miembros de la plantilla del Departamento de Informática y determinar si tales procedimientos cumplen los estatutos o regulaciones pertinentes sobre la protección de la intimidad.

3.4.2 Acceso a las Instalaciones de Ordenadores

• Objetivo de Control.

Debieran adoptarse medidas para asegurar que el acceso a las instalaciones (o salas) de ordenadores del Departamento de Informática queda restringido a los individuos que han sido autorizados a tener dicho acceso.

• Directiva de Auditoría.

Deben revisarse los procedimientos establecidos por el Departamento de Informática para restringir el acceso a sus instalaciones de ordenadores.

1. Asegurar que se ha publicado una declaración escrita que define las restricciones de acceso a las instalaciones de ordenadores del Departamento de Informática.
2. Determinar si hay en vigor procedimientos adecuados para evitar que personas no autorizadas logren acceder

a las instalaciones de ordenadores del Departamento de Informática.

3. Obtener un plano de la distribución física de las instalaciones de ordenadores del Departamento de Informática. Identificar todas las posibles entradas a las instalaciones y determinar si en cada una de ellas se han instalado restricciones adecuadas al acceso físico. Determinar si tales entradas están restringidas por el uso de llaves, tarjetas u otros dispositivos automáticos de seguridad. Si se usa una llave, código de entrada u otro dispositivo para activar el mecanismo de cierre, verificar que los medios de entrada se cambian periódicamente.

4. Obtener una lista de todos los individuos autorizados a tener acceso a las instalaciones de ordenadores del Departamento de Informática y determinar que dicho acceso es necesario. Verificar que la dirección del Departamento de Informática revisa periódicamente dicha lista para decidir si las autorizaciones de acceso siguen siendo válidas.

5. Observar las actividades desarrolladas en las instalaciones de ordenadores del Departamento de Informática, a distintas horas, para verificar que sólo se permite entrar en ellas a personal autorizada.

6. Asegurar que cuando las instalaciones de ordenadores del Departamento de Informática están desocupadas, hay una vigilancia periódica del área o que se transmiten señales de alarma de entrada no autorizada a una entidad externa responsable de supervisar la seguridad de las instalaciones.

3.4.3 Acompañamiento de Visitas

* Objetivo de Control.

Las personas que no son miembros de la plantilla de explotación del Departamento de Informática debieran ser acompañadas por un miembro de dicha plantilla cuandoquiera que tengan que

entrar en las instalaciones de ordenadores del Departamento.

* Directiva de Auditoría.

Deben revisarse los procedimientos del Departamento de Informática para asegurar que cualquier persona que no sea de la plantilla de explotación es acompañada por un miembro de la plantilla de explotación cuandoquiera que tengan que entrar en las instalaciones de ordenadores del Departamento.

1. Revisar los procedimientos establecidos por el Departamento de Informática para identificar a las visitas a las instalaciones de ordenadores y para acompañarles mientras estén presentes en esas áreas.

3.4.4 Administración de Palabras de Paso

* Objetivo de Control.

El acceso lógico a los ordenadores del Departamento de Informática debiera estar restringido mediante el uso de palabras de paso asociadas a reglas de acceso.

* Directiva de Auditoría.

Debe revisarse el Departamento de Informática para empleo de palabras de paso y otras restricciones lógicas de acceso a los recursos de ordenador.

1. Revisar el procedimiento del Departamento de Informática para añadir personas a la lista de las autorizadas a tener acceso a los recursos de ordenador, para cambiar sus autorizaciones de acceso y para borrarles de la lista.

2. Revisar el procedimiento del Departamento de Informática para suministrar palabras de paso, para asegurar que las palabras de paso individuales no se revelan de forma inadvertida y determinar si --y cuándo-- se exige que individuos cambien sus palabras de paso recientemente asignadas.

PARTE I - 3. CONTROLES DE EXPLOTACION.

3. Determinar si las palabras de paso suministradas por el Departamento de Informática tienen una longitud adecuada, no pueden ser eliminadas fácilmente, y no contienen caracteres repetidos.

4. Cerciorarse de si el procedimiento del Departamento de Informática exige que las palabras de paso se cambian periódicamente y que el mismo individuo no puede reutilizar la misma palabra de paso.

5. Verificar que los procedimientos del Departamento de Informática aseguran que las palabras de paso no aparecen en pantalla durante el proceso de identificación del usuario, no aparecen impresas y se almacenan por explotación de proceso de datos en un fichero cifrado.

6. Determinar si los procedimientos del Departamento de Informática restringen a los usuarios a terminales, horarios, y días de la semana específicos, cuando el riesgo justifica controles adicionales de acceso.

7. Determinar si los usuarios quedan despedidos y desconectados automáticamente, bajo los procedimientos del Departamento de Informática si no han estado activos durante un período específico, expresado normalmente en minutos de inactividad.

8. Determinar si la dirección de los departamentos usuarios de la organización valida periódicamente las libertades de acceso actualmente concedidas a personas de su departamento.

9. Determinar si los procedimientos del Departamento de Informática establecen la rápida cancelación de códigos de identificación y palabras de paso cuando ha terminado el empleo de la persona a quien se haya asignado.

10. Determinar si los procedimientos del Departamento de Informática establecen la suspensión de códigos de identificación de usuario o la desactivación del terminal, microordenador o dispositivo de entrada de datos después de un

cierto número de violaciones del procedimiento de seguridad.

3.4.5 Informes de Violaciones y Actividad de Seguridad

* Objetivo de Control.

Los procedimientos de seguridad de la información del Departamento de Informática debieran asegurar que se revisan periódicamente los informes de violaciones y actividad de seguridad para identificar y resolver incidentes relativos a actividad no autorizada.

* Directiva de Auditoría.

Deben revisarse la adecuación e eficacia de los procedimientos del Departamento de Informática para revisar y resolver los informes sobre violaciones de seguridad y actividades asociadas.

1. Revisar los procedimientos del Departamento de Informática para revisar y resolver los informes sobre violaciones de seguridad y verificar que están cumpliendo.

2. Determinar si se vienen registrando cambios en los registros de violaciones de seguridad del Departamento de Informática y si dichos cambios son revisados por un individuo independiente y verificar que existen los documentos autorizando tales cambios de ficheros.

3. Determinar si los registros de violaciones de seguridad del Departamento de Informática están protegidos contra destrucción accidental o intencional.

3.4.6 Restricciones de Acceso Lógico

* Objetivo de Control.

El Departamento de Informática debiera establecer reglas automáticas que regularan el acceso a sus recursos de ordenador.

• **Directiva de Auditoría.**

Deben examinarse los procedimientos del Departamento de Informática para conceder acceso autorizado a sus recursos de ordenador.

1. Determinar si los procedimientos del Departamento de Informática que los usuarios autorizados de sus recursos de ordenador han de recibir permiso específico para acceder a recursos particulares incluyendo ficheros de datos, programas de aplicación, el sistema operativo, y ciertos comandos.

2. Determinar si existe documentación que justifique la necesidad de y autorización para acceder el usuario a recursos del sistema de información.

3. Revisar los procedimientos para acceso de emergencia o temporal a los recursos del sistema de información. Determinar si se debe obtener autorización especial, si sólo se concede acceso temporal, y si se notifica a la dirección el acceso. Verificar que el acceso temporal sólo se concede con poca frecuencia.

4. Verificar que la separación de funciones dentro del sistema de información se mantiene mediante el sistema de control de accesos y determinar que los programadores de sistemas y los de aplicación no tienen acceso a programas y datos de explotación.

3.4.7 Seguridad del Acceso a Datos En Línea

• **Objetivo de Control.**

En un entorno en línea de tratamiento de datos, los procedimientos del Departamento de Informática debieran brindar controles de seguridad de los accesos basados en la necesidad probada del individuo de ver, añadir, cambiar o borrar datos.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos del Departamento de Informática para

autorizar acceso a un entorno de tratamiento en línea.

1. Determinar si los procedimientos del Departamento de Informática para autorizar acceso a un entorno de tratamiento en línea permiten limitar las funciones de ver, añadir, cambiar o borrar datos y restringir el acceso individual tan sólo a datos o transacciones para las cuales esté demostrada la necesidad de dicho acceso.

2. Determinar si la dirección de los departamentos usuarios valida periódicamente las libertades de acceso al entorno de tratamiento en línea actualmente concedidas a individuos de su departamento.

3.4.8 Identificación Limitada del Centro de Cálculo

• **Objetivo de Control.**

El Departamento de Informática debiera identificar la identidad física de su centro de cálculo.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos empleados por el Departamento de Informática para la identificación de su centro de cálculo.

1. Visitar el centro de cálculo del Departamento de Informática y verificar que la naturaleza de ese local no es fácilmente identificable mediante carteles y otros signos.

2. Revisar las guías y listines telefónicos y otra documentación producida por la organización para asegurar que en ellos no se identifica el local en que se lleva a cabo la explotación del Departamento de Informática.

PARTE I - 3. CONTROLES DE EXPLOTACION.

3.4.9 Protección Contra el Fuego

- **Objetivo de Control.**

Las medidas de protección contra el fuego de explotación del Departamento de Informática debieran ser conformes con los estándares generalmente aceptados para dichas medidas protectoras.

- **Directiva de Auditoría.**

Debe evaluarse la adecuación de las medidas de protección contra el fuego adoptadas por explotación del Departamento de Informática.

1. Revisar los estándares generalmente aceptados publicados por organizaciones nacionales de protección contra el fuego y apreciar si las medidas de protección contra el fuego seguidas en los centros de cálculo del Departamento de Informática son conformes con dichos estándares.
2. Determinar mediante entrevistas con la alta dirección de la organización y con la dirección del Departamento de Informática su comprensión de la adecuación del cumplimiento del Departamento con estándares de protección contra el fuego generalmente aceptados en centros de cálculo.
3. Revisar las evaluaciones realizadas por la agencia de seguros o por el jefe de bomberos o autoridad con jurisdicción sobre el tema de la adecuación de las medidas, o cambios previstos en ellas, de protección contra el fuego en los centros de cálculo del Departamento de Informática.
4. Inspeccionar los centros de cálculo del Departamento de Informática para determinar la adecuación de las medidas de protección contra el fuego existentes y el grado en que cumplen con los estándares generalmente aplicados relativos a dichas medidas.

3.4.10 Formación y Concienciación en Procedimientos de Seguridad

- **Objetivo de Control.**

El personal de explotación del Departamento de Informática debiera recibir información periódica sobre los controles y procedimientos de seguridad que se espera que cumplan.

- **Directiva de Auditoría.**

Debe verificarse la formación sobre medidas y procedimiento de seguridad recibida por el personal de explotación del Departamento de Informática.

1. Verificar que los miembros de la plantilla de explotación del Departamento de Informática han recibido periódicamente formación adecuada sobre los procedimientos que deben seguir en casos de emergencias de fuego, agua y alarma.
2. Determinar mediante observación que los miembros de la plantilla de explotación del Departamento de Informática conocen la localización de los alarmas de fuego, de los extintores, de los interruptores de energía normales y auxiliares, de los de suministro de agua y aire acondicionado, de los aparatos respiradores y de cualesquiera otros dispositivos de emergencia que se espera utilicen en caso de emergencia.
3. Determinar si el personal de explotación del Departamento de Informática efectúa simulacros de incendio periódicos.

3.5 PLANIFICACIÓN ANTE CONTINGENCIAS

Debieran existir planes adecuados para el respaldo de recursos de ordenador críticos y para la recuperación de los servicios del Departamento de Informática después de una interrupción imprevista de los mismos.

3.5.1 Plan de Recuperación de Desastres

• **Objetivo de Control.**

El Departamento de Informática debiera mantener un plan escrito para el tratamiento para programad de aplicación críticos, en caso de un fallo serio del material o lógico o de una destrucción temporal o permanente de las instalaciones.

• **Directiva de Auditoría.**

Debe evaluarse la adecuación del plan de recuperación de desastres del Departamento de Informática

2. Entrevistar a la dirección del Departamento de Informática para determinar su participación en el procedimiento de planificación del plan de recuperación de desastres del Departamento.

3. Determinar el tiempo que transcurriría tras la interrupción de la explotación del Departamento de Informática hasta que las funciones críticas de la organización quedaran interrumpidas y evaluar si el plan de recuperación de desastres del departamento permitiría la restauración de dichas funciones críticas d la organización en un período razonable de tiempo.

4. Evaluar lo completo y actualizado del plan de recuperación de desastres del Departamento de Informática y determinar si se han colocado copias del mismo en emplazamientos remotos.

5. Entrevistar a miembros seleccionados de la plantilla de explotación del Departamento de Informática para determinar su conocimiento y comprensión del plan de recuperación de desastres del departamento.

3.5.2 Seguridad del Personal y Formación en Procedimientos de Emergencia

• **Objetivo de Control.**

El plan de recuperación de desastres del Departamento de Informática debiera

incluir procedimientos de emergencia para asegurar la seguridad de los miembros de su plantilla y éstos deberian recibir formación periódica en el uso de dichos procedimientos.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos incluidos en el plan de recuperación de desastres del Departamento de Informática para asegurar la seguridad de todos los miembros de su plantilla y la formación que reciben en el uso de dichos procedimientos.

1. Revisar los procedimientos de emergencia incluidos en el plan de recuperación de desastres del Departamento de Informática en cuanto a si suponen una cobertura completa y exhaustiva de todas las emergencias que pueden tener lugar en un centro de cálculo.

2. **Cerciorarse** de si los miembros de la plantilla de explotación del Departamento de Informática reciben formación periódica sobre el uso de los procedimientos de emergencia apropiados y de si se han realizado pruebas periódicas de tales procedimientos.

3.5.3 Aplicaciones críticas de tratamiento de datos

• **Objetivo de Control.**

El plan de recuperación de desastres del Departamento de Informática debería establecer prioridades para la restauración del tratamiento de programas de aplicación críticos o sensitivos.

PARTE I - 3. CONTROLES DE EXPLOTACION.

• Directiva de Auditoría.

Debe evaluarse la lista de prioridades a seguir en la restauración de tratamiento de los programas de aplicación críticos o sensitivos del Departamento de Informática, para establecer que se contemplaron todos los programas de aplicación del Departamento, en relación con la naturaleza y extensión de un posible desastre así como el tiempo razonable esperado hasta la restauración de la explotación normal, las pérdidas potenciales para la organización si el tratamiento de los programas de aplicación no se restaura puntualmente, y el punto en que operaciones de tratamiento normalmente cíclico podrían ser interrumpidas.

1. **Determinar** si la dirección de los departamentos usuarios fue consultada por el Departamento de Informática cuando estaba estableciendo un factor de riesgo de pérdidas para secuenciar la restauración de cada aplicación de tratamiento de datos una vez acaecido un desastre.
2. **Apreciar** lo razonable de las prioridades asignadas por el Departamento de Informática a sus programas de aplicación críticos o sensitivos.
3. **Discutir** con la dirección de los departamentos usuarios y del Departamento de Informática si las prioridades asignadas a los programas de asignación críticos pueden cumplirse razonablemente una vez acaecido un desastre.

3.5.4 Recursos de Ordenador Críticos

• Objetivo de Control.

El plan de recuperación de desastres del Departamento de Informática debería identificar programas de aplicación, sistemas operativos y ficheros de datos críticos necesarios para la recuperación una vez acaecido un desastre.

• Directiva de Auditoría.

Debe revisarse la lista de recursos de ordenador críticos identificados en el plan de recuperación de desastres del Departamento de Informática.

1. **Revisar** la lista de recursos de ordenador críticos del Departamento de Informática y determinar si es razonable.
2. **Determinar** si en el plan de recuperación de desastres del Departamento de Informática están adecuadamente identificados los ficheros de datos críticos.
3. **Examinar** el emplazamiento remoto usado como almacén de ficheros por el Departamento de Informática y determinar si los ficheros de datos pertinentes del Departamento—incluyendo, cuando proceda, tanto ficheros de transacciones como sumarios— se vienen guardando en ese emplazamiento.
4. **Determinar** si se vienen enviando las nuevas versiones de ficheros de datos al emplazamiento remoto usado como almacén de ficheros por el Departamento de Informática, antes de que versiones anteriores de tales ficheros sean devueltas al local de explotación del departamento.
5. **Determinar** si, tras un desastre, se genera un fichero de respaldo del fichero del emplazamiento remoto a efectos de respaldar el fichero remoto antes de que sea usado.
6. **Examinar** el inventario de la biblioteca de soportes del Departamento de Informática y compararlo con los ficheros de datos actualmente retenidos en la biblioteca y con aquéllos mantenidos en el emplazamiento remoto usado como almacén de ficheros por el Departamento.

3.5.5 Restauración de Servicios de Telecomunicación

• **Objetivo de Control.**

El plan de recuperación de desastres del Departamento de Informática debería incluir procedimientos para restablecer los servicios de telecomunicación usados por la organización.

• **Directiva de Auditoría.**

El plan de recuperación de desastres del Departamento de Informática debería incluir procedimientos para restablecer los servicios de telecomunicación usados por la organización.

Deben revisarse los procedimientos del Departamento de Informática para restablecer, tras una interrupción, los servicios de telecomunicaciones usados por la organización.

1. **Revisar** el plan de recuperación de desastres del y **determinar** sus disposiciones para el uso en caso de emergencia de servicios alternativos de telecomunicación.
2. **Determinar** si se han preparado pedidos de servicios de telecomunicación por adelantado para ser usados por el Departamento de Informática para restaurar los servicios empleados por la organización tras su interrupción.
3. **Determinar** si hay disponibles para el Departamento de Informática líneas de telecomunicación por red conmutada adecuadas, para su utilización durante la recuperación de desastres, como alternativa a cualesquiera líneas alquiladas en las que haya interrumpido el servicio.
4. **Determinar** si en el emplazamiento elegido para recuperación de desastres de explotación del Departamento de Informática se han establecido enlaces para servicios alternativos de telecomunicación.

3.5.6 Respaldo: Del Centro de Cálculo y de los Equipos

• **Objetivo de Control.**

El plan de recuperación de desastres del Departamento de Informática debería establecer disposiciones para el centro de cálculo de respaldo y los equipos de respaldo necesarios para restaurar la explotación del Departamento una vez acaecido un desastre.

• **Directiva de Auditoría.**

Deben revisarse las disposiciones del Departamento de Informática en cuanto a centro de cálculo de respaldo y a ordenadores de respaldo a ser utilizados para restaurar su explotación una vez acaecido un desastre.

1. **Revisar** el plan de recuperación de desastres del Departamento de Informática para **determinar** las disposiciones en cuanto al centro de cálculo de respaldo y ordenadores de respaldo para restaurar la explotación una vez acaecido un desastre.
2. **Determinar** si existe un acuerdo escrito o contrato para el uso por el Departamento de Informática de un centro de cálculo específico para restaurar la explotación una vez acaecido un desastre, y **cerciorarse** de si las disposiciones adoptadas son razonables.
3. **Determinar** si el equipo de respaldo a emplearse para restaurar la explotación una vez acaecido un desastre es compatible con el equipo primario utilizado en la explotación regular del Departamento.
4. **Determinar** si en el centro de cálculo de respaldo y en el equipo de respaldo habrá suficientes tiempo y capacidad de proceso disponibles para restaurar la explotación una vez acaecido un desastre.
5. **Determinar** si se efectúan pruebas periódicas del equipo de respaldo planificado para ser usado por el Departamento para restaurar la explotación una vez acaecido un desastre.

PARTE I - 3. CONTROLES DE EXPLOTACION.

6. **Entrevistar** a miembros de la plantilla de explotación del Departamento de Informática para **determinar** su familiaridad con la operación del equipo de respaldo y con los procedimientos para conmutar al centro de cálculo de respaldo y equipo de respaldo cuando acaece un desastre.

3.5.7 Plantilla de Programación para Operaciones de Respaldo

* Objetivo de Control.

El plan de recuperación de desastres del Departamento de Informática debería disponer, cuando sea apropiado, que una plantilla de programación adecuada lleve la explotación de respaldo del Departamento.

* Directiva de Auditoría.

Deben revisarse las políticas y procedimientos del plan de recuperación de desastres del Departamento de Informática que se refieren a la aportación de una plantilla de programación adecuada lleve la explotación de respaldo del Departamento.

1. **Determinar** la extensión con que se ha solicitado a la plantilla de programadores de aplicaciones que aporten capacidades especiales o versiones de programas para explotación de respaldo.
2. **Revisar** las disposiciones del plan de recuperación de desastres del Departamento de Informática que traten con los pasos a seguir por la plantilla y programadores de aplicaciones y de sistemas para satisfacer las necesidades de personal de explotación para operar el equipo de respaldo, y **determinar** las acciones que han de adoptarse por la plantilla de programadores de aplicaciones y de sistemas para alcanzar familiaridad con dichas disposiciones.
3. **Seleccionar** programas de aplicación representativos que han sido identificados como necesitados de modificación antes de poder ser usados en explotación de respaldo y probarlos para

determinar si las modificaciones se han llevado a cabo correctamente. **Revisar** la documentación de apoyo de tales modificaciones para **asegurar** que dichos programas de respaldo son adecuados.

4. **Revisar** los procedimientos del Departamento de Informática para asegurar que los programas de respaldo a ser usados para restaurar la explotación una vez acaecido un desastre, son adecuadamente modificados cuando se cambian los programas usados en explotación normal.

3.5.8 Procedimientos de Recuperación de Ficheros

* Objetivo de Control.

El Departamento de Informática debería establecer procedimientos para minimizar las necesidades de recuperación de ficheros de respaldo una vez acaecido un desastre.

* Directiva de Auditoría.

Deben revisarse los procedimientos del Departamento de Informática para minimizar las necesidades de recuperación de ficheros de respaldo una vez acaecido un desastre.

1. **Determinar** mediante observación que el bibliotecario de soportes del Departamento de Informática ejecuta rutinariamente procedimientos de respaldo de ficheros —incluyendo la copia periódica del contenido de ficheros en disco a cinta u otro soporte magnético.
2. **Verificar** que los ficheros de respaldo se trasladan regularmente al almacenamiento remoto.
3. **Verificar** que la documentación de programas de aplicación críticos del Departamento de Informática especifica el uso de procedimientos específicos de reconstrucción de ficheros en puntos significativos del tratamiento de la aplicación.

4. **Determinar** que existen procedimientos escritos de regeneración de ficheros del sistema.

5. **Verificar**, mediante observación, que el área remota de almacenamiento tiene medidas de seguridad adecuadas para proteger a los ficheros y reglas de retención de ficheros adecuadas que aporten datos suficientemente recientes a las operaciones de recuperación.

3.5.9 Consumibles para Recuperación de Desastres

• **Objetivo de Control.**

El plan de recuperación de desastres del Departamento de Informática debería establecer más de una fuente de consumibles --incluyendo existencias de cualquier formulario especial necesario-- para ser usados en la restauración de la explotación del Departamento una vez acaecido un desastre.

• **Directiva de Auditoría.**

Deben revisarse las disposiciones del plan de recuperación de desastres del Departamento de Informática en cuanto a existencias de consumibles --incluyendo existencias de cualquier formulario especial necesario-- para ser usados en la restauración de la explotación del Departamento una vez acaecido un desastre.

1. **Revisar** los procedimientos de adquisición de suministros de proceso de datos de la organización y **determinar** si se emplean proveedores múltiples para cualquiera de los consumibles que serán necesarios para llevar a cabo el plan de recuperación de desastres del Departamento de Informática.

2. **Determinar** si las existencias de consumibles --incluyendo existencias de cualquier formulario especial necesario-- necesarias para llevar a cabo el plan de recuperación de desastres del Departamento de Informática están almacenadas en más de una localización, además del almacén de los vendedores en cuestión (consumibles fraccionados).

3.5.10 Pruebas del Plan de Recuperación de Desastres

• **Objetivo de Control.**

La adecuación y eficacia del plan de recuperación de desastres del Departamento de Informática debería probarse periódicamente.

• **Directiva de Auditoría.**

Debe verificarse la prueba periódica de la adecuación y eficacia del plan de recuperación de desastres del Departamento de Informática.

1. **Revisar** la documentación de pruebas anteriores del plan de recuperación de desastres del Departamento de Informática para **verificar** cuán adecuadas y frecuentes son las pruebas.

2. **Revisar** el proceso de aprobación de las pruebas del plan de recuperación de desastres para **determinar** la adecuación de los niveles de autoridad y responsabilidad para conceder dicha aprobación.

3. **Participar en y observar los resultados de** una prueba del plan de recuperación de desastres del Departamento de Informática para **determinar** la adecuación de los procedimientos de prueba.

3.5.11 Reconstrucción del Centro de Cálculo del Departamento de Informática

• **Objetivo de Control.**

El plan de recuperación de desastres del Departamento de Informática debería contener procedimientos, cuando sea necesario, para la reconstrucción del centro de cálculo del Departamento, una vez acaecido un desastre.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos del plan de recuperación de desastres del Departamento de Informática para cualquier reconstrucción necesaria del cen-

PARTE I - 3. CONTROLES DE EXPLOTACION.

tro de cálculo del Departamento, una vez acaecido un desastre.

1. **Revisar** los procedimientos del plan de recuperación de desastres del Departamento de Informática para cualquier reconstrucción necesaria del centro de cálculo del Departamento, una vez acaecido un desastre.

2. **Verificar** si dichos procedimientos son adecuados y están actualizados mediante la determinación de si se llevan a cabo revisiones y pruebas regulares de los mismos.

3.5.12 Procedimientos de Respaldo Manual de los Departamentos Usuarios

• **Objetivo de Control.**

Los departamentos usuarios deberían establecer procedimientos alternativos manuales de tratamiento de los datos que puedan ser empleados hasta que el Departamento de Informática sea capaz de restaurar su explotación tras el acaecimiento de un desastre.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos manuales de tratamientos de datos desarrollados por departamentos usuarios seleccionados para ser empleados hasta que el Departamento de Informática sea capaz de restaurar su explotación tras el acaecimiento de un desastre.

1. **Determinar** que departamentos usuarios seleccionados han desarrollado procedimientos manuales adecuados de tratamiento de datos para ser empleados hasta que el Departamento de Informática sea capaz de restaurar su explotación tras el acaecimiento de un desastre.

2. **Verificar** que el personal asignado a funciones de respaldo manuales está informado de sus misiones y las comprende.

PARTE I: CONTROLES GENERALES Y DE APLICACIONES

CONTROLES DE APLICACIONES

CONTENIDO

4. CONTROLES DE APLICACIONES

4.1	CONTROL DE CREACIÓN DE DATOS.	I-4-1
4.1.1	Procedimientos de preparación de datos.	I-4-1
4.1.2	Diseño de documentos fuente.	I-4-1
4.1.3	Control de documentos fuente.	I-4-2
4.1.4	Procedimiento de autorización de entrada de datos.	I-4-2
4.1.5	Retención de documentos fuente.	I-4-3
4.2	CONTROL DE ENTRADA DE DATOS.	I-4-4
4.2.1	Procedimientos de conversión y entrada de datos.	I-4-4
4.2.2	Procedimientos de conversión y entrada de datos en línea. ...	I-4-5
4.2.3	Validación y corrección de datos.	I-4-6
4.3	CONTROLES DE TRATAMIENTOS DE DATOS	I-4-8
4.3.1	Integridad del Tratamiento de Datos	I-4-8
4.3.2	Disposiciones acerca de la integridad del tratamiento de los datos en el logical de aplicación.	I-4-9
4.3.3	Validación y Corrección del Tratamiento de Datos.	I-4-10
4.3.4	Manejo de Errores de Proceso de Datos.	I-4-11
4.4	CONTROL DE SALIDAS DE DATOS	I-4-11
4.4.1	Revisión de salidas	I-4-12
4.4.2	Cuadre y Reconciliación de Salidas	I-4-12
4.4.3	Distribución de salidas.	I-4-13
4.4.4	Gestión de errores en las salidas.	I-4-14
4.4.5	Manejo y retención de las salidas	I-4-15
4.4.6	Disposiciones de seguridad sobre los informes de salida	I-4-16

* * *

PARTE I - 4. CONTROLES DE APLICACIONES.

1
2
3

4 CONTROLES DE APLICACIONES

4.1 CONTROL DE CREACIÓN DE DATOS.

Las declaraciones de procedimientos escritas de la organización que tratan sobre la entrega de datos a ser procesados deberían asegurar que los datos se autorizan, recopilan, preparan, transmiten y se comprueba su integridad de forma apropiada.

4.1.1 Procedimientos de preparación de datos.

* **Objetivo de Control.**

La alta dirección de la organización debería establecer procedimientos de preparación de datos a ser seguidos por las departamentos usuarios.

* **Directiva de Auditoría.**

Debe evaluarse la adecuación de los procedimientos de la organización para preparación de datos por la departamentos usuarios.

1. **Identificar** los documentos utilizados para cada tipo de entrada. **Cerciorarse** de si se establecieron procedimientos para la preparación de los datos a introducir en cada documento.
2. **Identificar** los datos específicos que pueden ser introducidos en cada documento fuente.
3. **Identificar** a aquellos individuos responsables de la preparación de entradas, de la revisión de los documentos fuente, y de la autorización de las entradas.
4. **Determinar** que existen procedimientos escritos para cada actividad del proceso de datos. **Verificar** que dichos procedimientos establecen instrucciones

significativas para el personal de preparación de datos.

5. **Apreciar** la adecuación de las funciones de control de preparación de datos efectuadas antes de la transmisión de los datos para ser procesados.

4.1.2 Diseño de documentos fuente.

* **Objetivo de Control.**

Los procedimientos para diseño de documentos fuente de la organización deberían asegurar que se minimizan los errores y omisiones.

* **Directiva de Auditoría.**

Debe evaluarse la adecuación de los procedimientos de la organización para el diseño de documentos fuente.

1. **Determinar** si documentos fuente representativos se ha diseñado específicamente para la recogida de datos de forma exacta y congruente.
2. **Determinar** si documentos fuente representativos están prenumerados, sino identificar cualesquiera procedimientos que hayan sido establecidos para asegurar que todos los documentos fuente han sido introducidos y pueden ser objeto de seguimiento o contabilización.
3. **Determinar** si, para cada tipo de transacción, el documento fuente empleado dispone de una código o identificación único.
4. **Determinar** si en documentos fuente representativos y en transacciones se ha incluido un número para referencia cruzada o un identificador comparable para facilitar su seguimiento.
5. **Determinar** si documentos fuente representativos han sido diseñados para destacar claramente los campos de datos específicos que hay que incluir en ellos.

PARTE I - 4. CONTROLES DE APLICACIONES.

6. **Determinar**, cuando sea aplicable, si documentos fuente representativos identifican los códigos de entrada que son válidos.

4.1.3 Control de documentos fuente.

* Objetivo de Control.

La organización debería establecer procedimientos para asegurar que las personas que participan en la generación de las transacciones no tienen en su custodia documentos fuente en blanco relativos a tales transacciones. (Debería establecerse una separación de funciones para la generación y aprobación de documentos fuente).

* Directiva de Auditoría.

Debe revisarse la forma en que en la organización se almacenan los documentos fuente en blanco.

Deber cerciorarse la garantía de separación de funciones en el manejo de documentos fuente.

1. **Determinar** si los documentos fuente en blanco son custodiados por personas designadas que no juegan papel alguno en la generación de las transacciones con las que dichos documentos están relacionadas.

2. **Apreciar** si los documentos fuente en blanco se almacenan de forma segura.

3. **Determinar** si la salida de almacén de los documentos fuente en blanco exige la autorización de dos o más individuos.

4. **Identificar** a las personas que preparan las transacciones. **Determinar** que un individuo no prepara más que un tipo de transacción (por ejemplo, el establecimiento de nuevos registros maestros y la modificación o actualización de registros maestros deberían ser consideradas como dos tipos de transacciones.)

5. **Identificar** a las personas implicadas en diversas fases de la preparación de datos. **Asegurar** que no hay ningún individuo que lleva a cabo más que uno de los siguientes aspectos del tratamiento de los documentos fuente:

- creación
- autorización
- control.

6. **Verificar** que se efectúan periódicamente inventarios físicos y reconciliaciones de las existencias de documentos fuente en blanco de naturaleza sensitiva, crítica o negociable y que cuando procede se puede efectuar un seguimiento y asignación de responsabilidades de todos esos documentos.

7. **Determinar** si hay en vigor procedimientos documentados para asegurar que toda los documentos fuente se custodian, controlan e imputan adecuadamente.

4.1.4 Procedimiento de autorización de entrada de datos.

* Objetivo de Control.

La organización debería establecer procedimientos adecuados para la autorización de datos de entrada.

* Directiva de Auditoría.

Debe evaluarse la adecuación de los procedimientos de la organización para autorizar datos de entrada.

1. **Observar** el proceso de control de entradas y **verificar** que el proceso de aprobación está limitado a aquellos individuos especificados en las declaraciones de procedimientos pertinentes de la organización como responsables para autorizar entradas.

2. **Verificar** que el personal responsable de la autorización de entrada de datos no efectúa tareas incompatibles.

3. **Verificar** para aplicaciones en que la entrada de datos se produce mediante terminales u ordenadores personales que los procedimientos pertinentes de la organización suponen el uso, mantenimiento y control de códigos de operador de terminal o estación.

4. **Observar** que en el proceso de autorización de entrada de datos se usan códigos de operador y de terminal adecuada y que las mismas se cambian cuando procede de acuerdo con el procedimiento escrito aplicable de la organización.

5. **Asegurar** que la autoridad del operador de terminal u ordenador personal para introducir datos es congruente con las declaraciones de política escritas pertinentes de la organización.

6. **Asegurar** que la autoridad del operador de terminal u ordenador personal para aprobar la entrada de datos es congruente con la declaración de política escrita pertinente de la organización.

7. **Determinar** que los documentos fuente se encaminan al personal adecuados para su aprobación previa a la entrada de datos según determinan las declaraciones de política escritas pertinentes de la organización.

4.1.5 Retención de documentos fuente.

• **Objetivo de Control.**

La organización debería retener los documentos fuente originales durante un período de tiempo adecuado para facilitar la recuperación o reconstrucción de los datos.

• **Directiva de Auditoría.**

Evaluar las prácticas de la organización para retener documentos fuente originales para asegurar que está disponible la información que pueda ser necesario para la reconstrucción o unificación de los datos.

1. **Determinar** que los documentos fuente se retienen durante tiempo suficiente para permitir la reconstrucción de los datos en el supuesto de que los mismos pierdan en el proceso y para satisfacer los requisitos de la Administración en cuanto a retención de documentos fuente según proceda.

2. **Determinar** si el período de retención de cada tipo o parte o copia de documentos fuente en concreto figura impreso en el propio documento en blanco.

3. **Evaluar** la facilidad con que pueden recuperarse documentos fuente archivados.

4. **Determinar** que el departamento que genera los datos conserva archivadas copia de los documentos fuente que generan y transmiten a otros departamentos.

5. **Determinar** que los documentos fuente archivados en los departamentos que generaron los datos son sólo accesibles a personal autorizado.

6. **Determinar** que los documentos fuente cuando ya dejan de estar en vigor se retiran del archivo y se destruyen de conformidad con las clasificaciones de seguridad impuestas por la organización y con sus declaraciones de procedimientos escritas pertinentes.

7. **Determinar**, para el caso de documentos transmitidos electrónicamente, que los datos del documento, los de su encaminamiento y los de su aprobación se conservan de conformidad con las declaraciones de política aplicables de la organización relativos a la retención de registros escritos.

8. **Determinar** que existen declaraciones de procedimientos escritas dentro de la organización para establecer períodos de retención de documentos fuente (dichas declaraciones de procedimientos pueden ser conocidas, en algunos casos, como calendarios de retención de registros.)

PARTE I - 4. CONTROLES DE APLICACIONES.

4.2 CONTROL DE ENTRADA DE DATOS.

Las declaraciones escritas de procedimiento de la organización que versan sobre la entrada de datos a su procesador deberían asegurar que los datos se validan y corrigen tan próximamente al punto de origen como sea posible. Deberían establecerse procedimientos de tratamiento de errores para facilitar que los datos vuelvan a presentarse con puntualidad y corrección.

4.2.1 Procedimientos de conversión y entrada de datos.

• Objetivo de Control.

La organización debería establecer procedimientos para la conversión y entrada de datos que aseguren una separación de funciones entre aquellos que participan en dicha actividad y también una verificación rutinaria del trabajo llevado a cabo en el proceso de entrada de datos.

• Directiva de Auditoría.

Deben revisarse los procedimientos establecidos por la organización para la conversión y entrada de datos.

1. **Determinar** que existen declaraciones de procedimientos escritas en la organización que explican la forma en que deben convertirse e introducirse los datos.

2. **Revisar** los procedimientos de control de datos de la organización y **asegurar** que los mismos especifican:

- a. las autorizaciones pertinentes para cada aplicación
- b. operaciones a efectuar durante la entrada inicial de los datos
- c. mensajes de error para cada aplicación

d. establecimiento de diarios de control que registren errores y excepciones

e. procedimientos para resolver errores y excepciones

f. controles que aseguren que todos los datos de entrada son revisados por la unidad de control de datos de la organización antes del proceso y procedimiento a seguir para la comunicación de la pérdida de datos que se ha echado en falta

h. controles sobre la extensión de la corrección de errores a ser efectuado por la unidad de control de datos de la organización

i. controles sobre los cambios y actualizaciones de los ficheros maestros

j. el encaminamiento adecuado para las aprobaciones y el de devoluciones al originador de los datos para la corrección de documentos electrónicos.

3. **Observar y probar** los procedimientos especificados por la organización para control de datos. **Determinar** el grado de cumplimiento de los procedimientos documentados y la efectividad de los mismos en la práctica real.

4. **Identificar** a las personas que realmente participan en el proceso de entrada de datos en la organización. **Determinar** que ninguna de las mismas lleva a cabo más que una de las siguientes operaciones.

- a. creación de datos
- b. entrada de datos
- c. verificación de datos y totales de control
- d. verificación de datos
- e. distribución de datos.

5. **Determinar** si existe un grupo independiente bien dentro de Departamento de Informática, bien dentro de los departamentos usuarios pertinentes -- responsable de efectuar operaciones de entrada de datos.

6. **Determinar** si hay un grupo de control responsable de efectuar operaciones de entrada de datos que controle independientemente los datos a introducir. **Identificar** los dispositivos de control realmente utilizados. Estos pueden incluir, sin limitarse a ellos, los siguientes:

- a. documento circulante
- b. técnicas de lotes
- c. cuentas de registros
- d. totales de control predeterminados
- e. uso de diarios.

7. **Determinar** -- en el caso de que los grupos de control de los departamentos usuarios de la organización no controlen la entrada de datos-- si en el punto de origen se llevan a cabo una entrada y registro de datos fuente simultáneos.

8. **Determinar** si los documentos fuente utilizados en los procesos de conversión o entrada de datos de la organización están marcados como protección contra la duplicación o nueva entrada de los datos o si las aplicaciones pertinentes se han diseñado para prevenir la duplicación de entradas.

4.2.2 Procedimientos de conversión y entrada de datos en línea.

* **Objetivo de Control.**

La organización debería establecer procedimientos que dificulten el uso no autorizado o el abuso de ordenadores personales o terminales para la conversión o entrada de datos.

* **Directiva de Auditoría.**

Deben revisarse los procedimientos de la organización para la conversión y entrada de datos a través de ordenadores personales y terminales.

1. **Determinar** si los dispositivos, ordenadores personales o terminales usadas por la organización para la conversión y entrada de datos están instalados en salas físicamente seguras.

2. **Determinar** que los procedimientos de entrada de datos de la organización aseguran que esta actividad sólo puede llevarse a cabo por individuos a los que se han asignado ciertos niveles de autoridad.

3. **Determinar** que los procedimientos de entrada de datos de la organización determinan la emisión, gestión y uso de palabras de paso para impedir el uso no autorizado de ordenadores personales y terminales.

4. **Determinar** si se deniega el acceso tras un número predeterminado de intentos fallidos de acceder desde o a través de un terminal.

5. **Cerciorarse** de que los procedimientos de la organización para el uso de palabras de paso y códigos de autorización aseguran que las palabras de paso y los códigos no aparecen impresas ni en pantalla, o que cuando se teclean en la pantalla aparecen caracteres no legibles.

6. **Determinar** que la organización utiliza número de identificación o códigos individuales o únicos para **establecer** la imputabilidad individual respecto al acceso de datos.

7. **Determinar** que la organización ha instalado mecanismos de seguridad para gestionar la autorización de acceso a transacciones en línea y a sus registros asociados.

8. **Determinar** que la organización ha establecido mecanismos de seguridad

PARTE I - 4. CONTROLES DE APLICACIONES.

para gestionar el acceso o lotes a ficheros, en función de su sensibilidad.

9. **Evaluar**, en aquellos casos en que la estructura de la organización o la extensión del tratamiento de transacción sin papeles reduce la separación de funciones tradicional, los controles detectores instalados para compensar cualquier reducción que pueda haber sucedido en los controles preventivos pertinentes.

10. **Determinar** que los mecanismos de seguridad de la organización aseguran que todos los intentos de acceso tanto con éxito cuanto fallidos quedan registrados y que los registros creados en este proceso contienen la fecha y hora del acceso e identifican al individuo que lo efectúa.

4.2.3 Validación y corrección de datos.

* Objetivo de Control.

La organización debiera establecer procedimientos para asegurar que los datos de entrada se validan y corrigen tan próximamente como sea posible al punto de origen.

* Directiva de Auditoría.

Deben evaluarse los procedimientos de validación y corrección de datos de entrada de la organización para asegurar que cada uno de ellos se lleva a cabo de forma adecuada y completa.

1. **Determinar** si la organización emplea formatos pre-programados de grabación de datos para asegurar que los datos se introducen en los campos y con los formatos adecuados.

2. **Determinar** si en las rutinas de captación de datos de la organización hay establecidos mensajes del terminal a fin de facilitar la introducción de datos y ayudar a reducir el número de errores en entrada de datos.

3. **Determinar** si la organización utiliza terminales inteligentes o logical de ordenador personal adecuado para efectuar

la validación, corrección y control del proceso de entrada de datos en el momento de la captación de datos (en el caso de que no se estén usando terminales inteligentes o logical de ordenador personal adecuado para la introducción de datos, determinar, mediante un análisis coste-beneficio, si se debe encomendar la introducción en la organización de esas técnicas)

4. **Determinar** los puntos en la organización en que se validan y corrigen los datos de entrada. **Cerciorarse** de que se han establecido procedimientos para asegurar que los datos incorrectos se identifican, rechazan y no se permite su entrada al sistema o que actualicen el fichero maestro.

5. **Cerciorarse** de que los procedimientos de validación que con corrección de datos de la organización se llevan a cabo sobre todos los campos de un registro de entrada, incluso aunque pudiera haberse registrado un error en alguno de los campos anteriores.

6. **Determinar** si los procedimientos de validación y corrección de datos de la organización incluyen la ejecución de pruebas de la presencia de:

- a. códigos del individuo y de autorización o aprobación por el revisor
- b. dígitos de control en todas las claves de identificación
- c. dígitos de control al final de un literal o de un dato numérico que no es objeto de cuadro
- d. códigos válidos
- e. valores numéricos o alfanuméricos válidos
- f. tamaños de campos válidos
- g. campos combinados
- h. límites válidos o valores razonables o rango razonables de los valores

- l. signos
- j. coincidencias y no coincidencia de registros
- k. secuencias de registros
- l. conservación de totales de campos
- m. registros de entrada completos
- n. campos repetitivos, que evitan la necesidad de introducir repetidamente el mismo valor.

7. **Determinar** que los procedimientos de entrada de datos de la organización no permiten a nadie saltarse o puentear las rutinas de validación y corrección de errores de los datos. Si los supervisores están autorizados para saltarse o puentear dichas actividades, **cerciorarse** de que un mecanismo de diario automático registra dichas actividades y que el correspondiente diario se analiza posteriormente para determinar su corrección.

8. **Determinar** la extensión con que se utilizan en los procesos de entrada de datos de la organización códigos que permitan saltarse o puentear la validación y corrección de errores en los casos de que dicho uso sea frecuente o excesivo, evalúen la extensión en que las rutinas de corrección de datos pudieran ser modificadas para mejorar la eficiencia y validez de la actividad de entrada de datos.

9. **Cerciorarse** de que los grupos de control de los departamentos usuarios de la organización utilizan totales de control de lotes, generados por los terminales de entrada de datos, logical de ordenador personal, o concentradores, para validar que los lotes de datos recibidos como entrada están completos.

10. **Determinar** si el procedimiento de entrada de datos de la organización mantiene un diario de número de documento fuente introducidos para asegurar la imputabilidad de todos esos documentos.

11. **Asegurar** que el procedimiento de entrada de datos de la organización establece que los datos introducidos se incluyan en un registro de pista de auditoría para su posible empleo en la gestión de errores y para recuperación en el caso de un fallo de la aplicación de tratamiento de datos.

4.2.4 Manejo de errores en entrada de datos.

- **Objetivo de Control.**

La organización debería establecer procedimientos para la corrección y nueva presentación de los datos de entrada erróneos

- **Directiva de Auditoría.**

Deben revisarse los procedimientos de la organización para la corrección y nueva presentación de los datos de entrada erróneos.

1. **Determinar** que los procedimientos de la organización para la identificación, corrección y volver a presentar datos que contenían errores han sido establecidos y difundidos en forma escrita.

2. **Determinar** si el procedimiento de entrada de datos de la organización establece la presentación en pantalla o supresión de los datos erróneos inmediatamente una vez detectados a fin de facilitar su ágil corrección y nueva presentación.

3. **Determinar** si los mensajes de error generados por procedimientos de entrada de datos de la organización están claramente establecidos y pueden ser comprendidos fácilmente por el operador del terminal u ordenador personal de forma que la corrección y reintroducción de los datos puedan efectuarse rápidamente.

4. **Cerciorarse** de que todos los datos rechazados por los procedimientos de entrada de datos de la organización se graban automáticamente en ficheros de

PARTE I - 4. CONTROLES DE APLICACIONES.

datos rechazados, clasificados por aplicación.

5. **Revisar** entradas seleccionadas en el fichero de datos rechazados de la organización para establecer se incluyen información como:

a. códigos que identifican los tipos de error

b. fecha y hora en que se grabó un registro en el fichero de datos rechazados

c. Identificación del individuo cuya actividad de entrada de datos originó el registro.

6. **Determinar** si el fichero de datos rechazados de la organización cuenta automáticamente los registros, para controlar el número de los registros de dicho fichero.

7. **Identificar** a los individuos de la organización que han sido autorizados a incluir correcciones a datos que han sido rechazados del proceso de entrada porque contenía errores. **Determinar** si alguno de los grupos de control de los departamentos usuarios establecen un control independiente sobre la ejecución de dichas correcciones.

8. **Determinar** si los ficheros de datos rechazados de la organización producen de forma rutinaria mensajes de seguimiento e informan de modo regular sobre el estado de transacción no corregidas.

9. **Determinar** que el procedimiento de corrección de errores en datos de entrada de la organización establece que antes de que vuelvan a ser introducidos, todas las correcciones deben ser revisadas y aprobadas de forma independiente por supervisores (cuando no se prepara documentos fuente antes de la introducción en línea de los datos, cualesquiera transacciones de corrección de errores en datos debieran ser objeto de revisión por un supervisor antes de que los ficheros de entrada pertinentes vuel-

ven a ser presentados para su tratamiento.

10. **Determinar** si la dirección de los departamentos usuarios revisan los informes de los ficheros de datos rechazados de la organización para analizar la frecuencia de errores en transacciones y el estado de transacciones no escogidas (el procedimiento de rechazo de entrada de datos erróneos debiera facilitar un análisis de la antigüedad de la información para ayudar al control de la realización de errores en tiempo oportuno). **Determinar** si la dirección de los departamentos usuarios es consciente de que la responsabilidad final de que los datos de entrada sean completos o correctos es suya.

11. **Determinar** que del fichero de datos rechazados de la organización sólo pueden borrarse registros por personal autorizado y siguiendo procedimientos estándar que incluyen controles detectores adecuados.

12. **Determinar**, cuando en la organización se usan técnicas de tratamiento de errores en línea, si —y cómo— se comprueban los datos corregidos en cuanto a su validez, exactitud, y que están completos.

4.3 CONTROLES DE TRATAMIENTOS DE DATOS

El tratamiento de los datos por programas de aplicación individuales de 00 debiera ser controlado para asegurar que durante el tratamiento no se añaden, retiran datos.

4.3.1 Integridad del Tratamiento de Datos

• Objetivo de Control.

La organización debiera establecer procedimientos de proceso de datos que aseguren que mantiene la separación de funciones y al mismo tiempo la verificación rutinaria del trabajo realizado.

* **Directiva de Auditoría.**

Deben revisarse los procedimientos de la organización para mantener la integridad de los datos durante su tratamiento.

1. **Determinar** que se han escrito declaración de procedimiento que explican la forma en que los datos son tratados por la organización.

2. **Identificar** a las personas que trabajan en la actividad de proceso de datos de la organización. **Asegurar** que ninguno de esos individuos realiza más de una de las operaciones siguiente:

- a. generación de datos
- b. entrada de datos
- c. tratamiento de datos
- d. verificación de totales de control
- e. distribución de datos.

3. **Determinar** si la organización mantiene un diario de registros, por aplicación para suministrar una pista de auditoría de las transacciones de datos que se procesan (el auditor debiera entender que el mantenimiento de este registro no es un control de proceso o explotación).

4. **Determinar** que en los registro de diarios de tratamientos de datos de la organización además de la hora y fecha de los mismos figuran los códigos de identificación del terminal, ordenador personal y usuario.

5. **Determinar** si el departamento de informática de la organización tiene un grupo de control que desarrolla actividades como:

- a. la investigación y corrección de cualesquiera problemas de terminal, ordenador personal u otro dispositivo de entrada de datos que no puedan ser resueltos en la fuente
- b. investiguen cualesquiera acciones de intervención del operador

c. asegurar que los re-arranques se lleven a cabo adecuadamente.

6. **Determinar** si el departamento de informática de la organización tiene un grupo de administración de seguridad que realiza actividades como:

- a. el control de actividad de terminales ordenadores personales u otros dispositivos de entrada de datos
- b. la investigación de cualquier desviación respecto a los procedimientos establecidos de entrada de datos.

7. **Determinar** si el Departamento de Informática de la organización tiene un grupo de control de entradas y salidas que ejecuta actividades tales como el saldo de las cuentas de registro, cuentas de lotes y totales de control para los datos procesados.

4.3.2 Disposiciones acerca de la integridad del tratamiento de los datos en el logical de aplicación.

* **Objetivo de Control.**

La organización debiera establecer procedimientos para asegurar, cuando proceda, que el logical de aplicación contiene determinación para verificar de forma rutinaria el trabajo realizado por el logical y para ayudar a asegurar la integridad de los datos.

* **Directiva de Auditoría.**

Deben revisarse los procedimientos de la organización para asegurar la integridad del tratamiento de los datos mediante el logical de aplicación.

1. **Determinar**, para logical de aplicación seleccionado, si la organización a tomado medidas positivas para evitar la entrada de datos desde la consola.

2. **Determinar**, para logical de aplicación seleccionado, si la organización identifica positivamente el tipo de datos de entrada a ser procesados.

PARTE I - 4. CONTROLES DE APLICACIONES.

3. **Determinar** si la organización ha incluido opciones estándar, por defecto, razonables, en la lógica de programas de aplicación seleccionados.

4. **Determinar** si el logical de aplicación seleccionado genera totales de control y efectúa reconciliaciones, para comprobar que el tratamiento es completo.

5. **Determinar**, para logical de aplicación seleccionado, que las etiquetas internas en los ficheros de movimientos contienen totales de control para permitir comprobar que todos los registros están en el fichero.

6. **Determinar**, para logical de aplicación seleccionado, que incorpora controles de haber completado el fichero, para asegurar que tanto el fichero maestro cuanto el de transacciones han sido procesados completamente.

7. **Verificar**, para logical de aplicación seleccionado, que las fechas de transacción en las entradas se comparan con fechas de corte de fin de mes controladas por el sistema para asegurar la congruencia.

4.3.3 Validación y Corrección del Tratamiento de Datos.

• Objetivo de Control.

La organización debiera establecer procedimientos para asegurar que la validación y corrección del tratamiento de datos se efectúa lo más próximo posible al punto de origen.

• Directiva de Auditoría.

Deben revisarse los procedimientos de la organización para validar y corregir el tratamiento de datos (cuando las transacciones las genera un programa de aplicación que las pasa a un segundo programa de aplicación), el auditor debiera determinar si los datos de transacción en cuestión son validados y corregidos de manera rutinaria antes de que se acceda a los registros pertinentes del fichero maestro.

1. **Determinar** los puntos de la organización en que tienen lugar validación y corrección de datos. **Cerciorarse** de que los datos incorrectos se reciclarán antes de que se lleve a cabo la actualización de los ficheros maestros.

2. **Cerciorarse** de que los procedimientos de validación y corrección de datos de la organización se llevan a cabo sobre todos los campos del registro incluso aunque pudiera haber sido detectado un error en un campo anterior.

3. **Determinar** que los procedimientos de validación y corrección de datos de la organización disponen la ejecución de correcciones de relación, entre el tratamiento de la transacción de entrada y los registros relacionados de los ficheros maestros. Esta corrección debería comprobar que las transacciones son apropiadas y correctas antes de iniciar el proceso de actualización.

4. **Determinar**, para logical de aplicación seleccionado, que contenga tablas de valores, que los procedimientos de validación y corrección de datos de la organización incluyen un mecanismo para asegurar la exactitud de los valores de la tabla.

5. **Determinar** para logical de aplicación seleccionado, que actualizará ficheros directamente, que los procedimientos de validación y corrección de datos de la organización producen versiones o imágenes anteriores y posteriores del registro que se corrige.

6. **Determinar** para logical de aplicación seleccionado que actualiza ficheros directamente, que de forma rutinaria se producen apuntes en un diario de transacciones el cual muestra la fecha y hora de la transacción así como la identificación de la persona que inicia la transacción.

7. **Revisar y evaluar** para logical de aplicación seleccionado las características que tenga de redondeo en cálculos matemáticos para determinar el impacto de los errores de redondeo.

4.3.4 Manejo de Errores de Proceso de Datos.

• **Objetivo de Control.**

La organización debiera establecer procedimientos de manejo de errores de proceso de datos que permitan identificar transacciones erróneas sin que éstas sean procesadas y sin que se produzca una alteración indebida en el tratamiento de otras transacciones válidas.

• **Directiva de Auditoría.**

Deben verificar los procedimientos de la organización para el manejo de los errores identificados durante el proceso de tratamiento de datos.

1. **Determinar** que la organización ha difundido procedimientos escritos para la identificación, corrección y repetición del tratamiento de datos rechazados previamente durante el proceso de entrada.

2. **Evaluar** si los mensajes generados por los procedimientos de manejo de errores de proceso de datos de la organización son claros y fáciles de entender, de modo que el sistema solicite las acciones correctivas necesarias.

3. **Cerciorarse** de que todos los datos rechazados por los procedimientos de validación y corrección de datos de la organización se graban de forma rutinaria en ficheros de datos rechazados en los cuales los datos erróneos se clasifican por aplicación.

4. **Revisar** los registros de los ficheros de datos rechazados de la organización para establecer que incluyen información como:

a. códigos para indicar los tipos de errores

b. la fecha y hora en que se grabó el registro en el fichero de datos rechazados

c. la identificación del usuario que originó la transacción.

5. **Determinar** si los ficheros de datos rechazados de la organización incluyen cuentas automáticas de registro para controlar el número de registros de los ficheros.

6. **Determinar** si los ficheros de datos rechazados de la organización producen mensajes de seguimiento e informan periódicamente sobre transacciones pendientes de corregir.

7. **Determinar** que los procedimientos de validación y corrección de datos de la organización disponen que todas las correcciones se revisen y aprueben por supervisores antes de volver a introducir los datos.

8. **Determinar** que los procedimientos de la organización para el tratamiento de transacciones corregidas son los mismos procedimientos que los de tratamiento de las transacciones originales seleccionadas, con la excepción de que el tratamiento de transacciones corregidas exige la revisión y aprobación por un supervisor.

9. **Indagar** si la dirección de los departamentos usuarios de la organización es consciente de que ellos son los responsables últimos de que el tratamiento de datos sea completo y exacto.

4.4 CONTROL DE SALIDAS DE DATOS

Los informes de salida del tratamiento de datos debieran revisarse para ver si parecen razonables y debieran revisarse con puntualidad a los individuos autorizados para recibirlos. Los informes de salida debieran también estar protegidos contra acceso en línea no autorizada.

PARTE I - 4. CONTROLES DE APLICACIONES.

4.4.1 Revisión de salidas

• Objetivo de Control.

La alta dirección de la organización debería establecer procedimientos para asegurar que tanto el departamento de informática cuanto los departamentos de usuarios pertinentes revisan los informes de salida de proceso de datos.

• Directiva de Auditoría.

Deben revisarse los procedimientos utilizados en la organización tanto por el departamento de informática cuanto por los departamentos de usuarios, para asegurar que los informes de salida de proceso de datos son completos y exactos.

1. **Determinar** si el departamento de informática de la organización tiene un grupo de control responsable de revisar todos los informes de salida de proceso de datos en cuanto a que son generalmente aceptables y completos.

2. **Determinar** si el grupo de control del departamento de informática de la organización controla el flujo del tratamiento para asegurar que los programas de aplicación se procesen conforme al calendario.

3. **Determinar**, mediante entrevistas con departamentos de usuarios seleccionados dentro de la organización, si:

- a. consideran pertinentes los informes que reciben
- b. encuentran que los datos presentados en dichos informes son exactos, fiables, razonables y útiles
- c. debiera retirárseles de las listas de distribución de alguno de los informes de salida que actualmente reciben
- d. debiera incluirseles en las listas de distribución de informes adicionales que no reciben actualmente

e. tienen sugerencias para mejorar el formato, contenido, frecuencia y puntualidad de los informes que reciben

f. alguno de los informes que reciben --o que creen que deberían recibir-- debiera ofrecerse en línea a fin de reducir el coste de imprimir y almacenar los datos en cuestión y para mejorar la eficiencia administrativa general.

4.4.2 Cuadre y Reconciliación de Salidas

• Objetivo de Control.

La organización debería establecer procedimientos para asegurar que las salidas de los programas de aplicación se cuadran de forma rutinaria con los totales de control pertinentes. Deberían disponerse pistas de auditoría para facilitar el trazado o seguimiento del proceso de las transacciones y la reconciliación de los datos puestos en cuestión.

• Directiva de Auditoría.

Deben revisarse los procedimientos de la organización para cuadrar la salida de los programas de aplicación con totales de control y para reconciliar los datos puestos en cuestión.

1. **Determinar** que la organización ha publicado procedimientos escritos para el cuadre y reconciliación de las salidas producidas por programas de aplicación.

2. **Determinar** si toda la información que necesitan los departamentos de usuarios de la organización está disponible para informes seleccionados.

3. **Determinar** si, según los procedimientos de la organización, se identifican todas las excepciones y se informa sobre ellas.

4. **Determinar** si los totales y otros datos incluidos en los informes son generados bajo los procedimientos de la organiza-

ción y si son completos y exactos. **Verificar** que dichos informes incluyen todas las excepciones posibles.

5. **Determinar** si el grupo de control del departamento de informática de la organización reconcilia cada total del lote de salida con totales del lote de entrada antes de que el informe de salida sea transmitido, para asegurar que durante el tratamiento no se añadió ni perdió dato alguno.

6. **Determinar** si se lleva un registro de los terminales y ordenadores personales de la organización a través de los cuales se transmiten las salidas.

7. **Determinar** si el diario de transmisiones que se lleva en cada uno de los terminales y ordenadores personales de la organización se compara regularmente con el registro de transacciones que se lleva para programas de aplicación seleccionado a fin de asegurar que todas las salidas se han transmitido adecuadamente a sus usuarios.

8. **Determinar** si los procedimientos de preparación de informes de salida de la organización permiten el trazado hacia adelante hasta las salidas finales y trazado hacia atrás hasta las entradas de datos fuente originales.

9. **Determinar** si los grupos de control de los Departamentos usuarios de la organización reconcilian cada total del lote de salida con totales del lote de entrada antes de que tenga lugar la entrega o puesta a disposición de las salidas al propio usuario.

10. **Determinar** que los grupos de control de los Departamentos usuarios de la organización reciben a tiempo listas de todos:

- a. los cambios a los ficheros maestros de los programas de aplicación pertinentes

b. las transacciones generadas internamente por los programas de aplicación pertinentes

c. las transacciones de interfaz procesadas por los programas de aplicación pertinentes.

d. las transacciones introducidas en el sistema.

11. **Determinar** si los grupos de control de los departamentos usuarios de la organización usan las listas del punto 10 anterior para verificar que todas las salidas son exactas y completas.

12. **Determinar** si los procedimientos de información sobre los tratamientos de la organización establecen que los usuarios deben reconciliar los cuadros actuales del sistema con la del día anterior —o tratamiento anterior—.

13. **Determinar** los procedimientos usados por un seleccionado en la organización para asegurar que todas las salidas son exactas y completas y hacer pruebas de cumplimiento o de tales procedimientos.

14. **Apreciar** si la dirección de un seleccionado en la organización es consciente de que son los responsables últimos de la exactitud de todas las salidas de programa de aplicación.

4.4.3 Distribución de salidas.

• **Objetivo de Control.**

La organización debería publicar procedimientos para la distribución de las salidas de proceso de datos.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos escritos de la organización para la distribución de salidas de proceso de datos. Debe revisarse el acceso en línea a informes de salida.

1. **Determinar** si todos los procesos de la organización para distribución de salidas

PARTE I - 4. CONTROLES DE APLICACIONES.

de proceso o de datos -- y cualesquiera cambios a dichos procedimientos -- se han comunicado por escrito.

2. **Revisar** los procedimientos escritos de la organización para distribución de salidas en lo que respecta a que sean exactas y completas.
3. **Determinar** si existe una lista de distribución de todas las aplicaciones de proceso de datos de la organización.
4. **Determinar** si las listas de distribución pertinentes cuando quiera que tenga lugar algún cambio en las necesidades de distribución de salidas de la organización.
5. **Determinar** si las listas de distribución de salidas de proceso de datos de la organización incluyen, para cada informe, además de cualquier instrucción especial:
 - a. la frecuencia de su preparación
 - b. como debe disponerse del original y copias
 - c. calendario y horarios de su distribución.
6. **Observar**, para aplicaciones seleccionadas la distribución actual de las salidas para determinar el flujo de tales documentos en la organización.
7. **Comparar** para aplicaciones seleccionadas, la entrega real en la organización de las salidas con su calendario de distribución, para determinar la puntualidad y exactitud de su calendario.
8. **Determinar** que los controles del logical de control de salidas en línea impiden la lectura, copia, borrado o redireccionado de la salida.
9. **Probar** el método usado por la organización para corregir los errores en la distribución de salidas.
10. **Discutir** con el personal encargado de la distribución su opinión sobre el

sistema actual y sus recomendaciones para mejorar el sistema de distribución de las salidas de proceso de datos de la organización.

11. **Discutir** con usuarios seleccionados dentro de la organización su opinión sobre el sistema de distribución de las salidas y sus recomendaciones para mejorarlo.

12. **Determinar** si los procedimientos de distribución de salidas de proceso de datos de la organización establecen que se lleve un registro de distribución de salidas.

a. **Revisar** el formato de dicho registro, para **determinar** si contiene información suficiente para determinar la distribución real de las salidas de aplicaciones de proceso de datos seleccionadas y quién era responsable de disponer finalmente de dichas salidas

b. **Observar** cómo las personas responsables de distribuir las salidas llevan dicho registro

c. **Comparar** cualesquiera errores de distribución de las salidas previamente puestos de manifiesto con este registro, para **determinar** su exactitud y utilidad.

4.4.4 Gestión de errores en las salidas.

* **Objetivo de Control.**

La organización debiera establecer procedimientos para controlar e informar acerca de los errores contenidos en las salidas de sus aplicaciones de proceso de datos.

* **Directiva de Auditoría.**

Deben revisarse los procedimientos establecidos por la organización para controlar e informar acerca de los errores contenidos en las salidas de sus aplicaciones de proceso de datos.

1. **Determinar** que la organización ha publicado procedimientos escritos para controlar e informar acerca de los erro-

res contenidos en las salidas de sus aplicaciones de proceso de datos.

2. **Determinar** si los grupos de control del Departamento de Informática y de los departamentos usuarios notifican rápidamente a los usuarios los problemas con las salidas.
3. **Determinar** si los grupos de control del Departamento de Informática y de los departamentos usuarios llevan un registro de todas las salidas de programas de aplicación de proceso de datos que contienen errores.
4. **Determinar** si los diversos grupos de control de la organización llevan un registro de errores en las salidas de las aplicaciones para **asegurar** que tales errores se corrijan. Esto supone usar el contenido del registro para:
 - a. identificar problemas con errores de salidas
 - b. identificar las personas del Departamento de Informática con quienes se ha establecido contacto y registrar la fecha y hora de dicho contacto
 - c. registrar la acción correctora adoptada por el Departamento de Informática
 - d. registrar la fecha y hora en que se recibe del Departamento de Informática la salida corregida
 - e. identificar las causas --y cualesquiera posibles tendencias-- de los errores en las salidas.
5. **Establecer** que los procedimientos de la organización establecen que las salidas corregidas sean sometidas a la misma revisión de calidad aplicada a la salida errónea.

4.4.5 Manejo y retención de las salidas

• **Objetivo de Control.**

La organización debiera establecer procedimientos para el manejo y retención de las salidas de sus programas de aplicación de proceso de datos.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos de la organización para el manejo y retención de las salidas de sus programas de aplicación de proceso de datos.

1. **Determinar** que la organización ha publicado procedimientos formales por escrito --que pueden denominarse **calendario de retención de registros**-- relativos a las salidas de sus programas de aplicación de proceso de datos.
2. **Apreciar** si el período de retención establecido por la organización para una muestra seleccionada de salidas de programas de aplicación de proceso de datos es razonable a efectos de respaldo y de auditoría.
3. **Determinar** si la organización emplea métodos adecuados de desmagnetización, picado, u otros, para disponer de las salidas no actualizadas innecesarias de los programas de aplicación de proceso de datos.
4. **Determinar** que los procedimientos pertinentes de la organización aseguran que el acceso a las salidas de los programas de aplicación de proceso de datos está restringido a las personas autorizadas.
5. **Determinar** si se efectúan revisiones periódicas si las salidas de los programas de aplicación de proceso de datos que se transmiten a personas en concreto continúan siendo necesarias para dichas personas.

PARTE I - 4. CONTROLES DE APLICACIONES.

4.4.6 Disposiciones de seguridad sobre los informes de salida

• **Objetivo de Control.**

La organización debiera establecer procedimientos para asegurar que se garantiza la seguridad de los informes de salida de proceso de datos pendientes de distribución a los usuarios.

• **Directiva de Auditoría.**

Deben evaluarse las disposiciones adoptadas por la organización para asegurar que se garantiza la seguridad de los informes de salida de proceso de datos pendientes de distribución o distribuidos a los usuarios.

1. **Determinar** si los procedimientos escritos de la organización incluyen listados de aquellos informes de salida de proceso de datos clasificados como críticos o sensibles.

2. **Evaluar** el riesgo asociado a los informes de salida de proceso de datos de la organización, críticos o sensitivos, y **probar** los procedimientos seguidos para proteger tales informes.

3. **Apreciar** si los procedimientos de la organización para garantizar la seguridad de los informes de salida de proceso de datos (tanto en línea cuanto impresos) pendientes de distribución son adecuados y se siguen.

4. **Apreciar** si departamentos usuarios seleccionados, que reciben informes de salida de proceso de datos críticos o sensibles, (1) son conscientes de la clasificación de dicho material y (2) adoptan las medidas adecuadas para proteger su confidencialidad tanto mientras los tienen en su poder cuanto en el momento de disponer de ellos.

5. **Determinar** si los informes de salida de aplicaciones críticas o sensibles de la organización se marcan claramente como confidenciales para promover una conciencia de seguridad y garantizar que ese material se maneja adecuadamente.

6. **Determinar** si la organización utiliza técnicas de doble custodia para controlar la transmisión, distribución, destrucción o retorno al archivo de las salidas de aplicaciones de proceso de datos críticos o sensibles, y **cerciorarse** de su eficacia.

* * *

PARTE II: CONTROLES ESPECÍFICOS DE CIERTAS TECNOLOGÍAS
CONTROLES EN SISTEMAS INFORMÁTICOS EN ENTORNOS DE BASES DE DATOS

CONTENIDO

1	CONTROLES EN SISTEMAS INFORMÁTICOS EN ENTORNOS DE BASES DE DATOS	II-1-1
1.1	SISTEMAS DE GESTIÓN DE BASES DE DATOS	II-1-1
1.2	ADMINISTRACIÓN DE DATOS	II-1-2
1.3	RESPONSABILIDAD DE LA ADMINISTRACIÓN DE LAS BASES DE DATOS	II-1-2
1.4	DESCRIPCIÓN DE DATOS Y CAMBIOS DE DATOS	II-1-3
1.5	CONTROL DE ACCESO A DATOS Y DE CONCURRENCIA	II-1-3
1.6	RECUPERACIÓN DEL CONTENIDO DE LAS BASES DE DATOS	II-1-4
1.7	INTEGRIDAD DE LAS BASES DE DATOS	II-1-5
1.8	DISPONIBILIDAD DE LAS BASES DE DATOS	II-1-5

* * *

PARTE II - 1. CONTROLES DE BASES DE DATOS

1 **CONTROLES EN SISTEMAS INFORMÁTICOS EN ENTORNOS DE BASES DE DATOS**

En el desarrollo y mantenimiento de sistemas informáticos en entornos de bases de datos debiera considerarse el control, la integridad y la seguridad de los datos compartidos por múltiples usuarios. Esto debe abarcar a todos los componentes del entorno de bases de datos.

1.1 **SISTEMAS DE GESTIÓN DE BASES DE DATOS**

• **Objetivo de Control.**

El logical de gestión de bases de datos usado por la organización para proveer el acceso a, la estructuración de, y el control sobre los datos compartidos, debiera instalarse y mantenerse de modo tal que asegure la integridad del logical, las bases de datos y las instrucciones de control que definen el entorno de las bases de datos.

• **Directiva de Auditoría.**

Debe revisarse la adecuación de los controles de la organización sobre la instalación y mantenimiento del logical de gestión de bases de datos destinado a asegurar la perpetuación de su integridad

- 1 **Identificar** los objetivos y metas del entorno de base de datos de la organización y determinar que se ha establecido un proceso para medir su funcionamiento.
- 2 **Identificar** las características de control incorporados de sistema de gestión de base de datos usado por la organización, y en concreto aquellas características referentes a:
 - a. el acceso a datos compartidos
 - b. la organización de los datos

c. el control de datos compartidos

- 3 **Identificar** los componentes del entorno de base de datos usado por la organización.
- 4 **Revisar** cómo se mantiene la integridad del logical de gestión de base de datos usado por la organización y **determinar** que se usan procedimientos adecuados de control de cambios.
- 5 **Revisar** cómo se mantiene la integridad de las bases de datos particular que se está investigando. **Determinar** si la arquitectura de las bases de datos fija instrucciones sobre si la integridad debe asegurarse mediante procedimientos desarrollados dentro de las bases de datos o mediante rutinas de corrección incluidas en las aplicaciones que llevan a cabo la actualización de sus contenidos. (La responsabilidad del mantenimiento de la integridad de los contenidos de las bases de datos debería estar asignada tanto administrativamente cuanto en la jerarquía técnica de proceso de datos).
- 6 **Determinar** que se mantiene la integridad de las instrucciones de control del sistema de gestión de las bases de datos.
- 7 **Determinar** que se mantiene la integridad del diccionario de datos del sistema de gestión de las bases de datos.
- 8 **Determinar** que el sistema de gestión de las bases de datos minimiza la redundancia de datos. **Cerciorarse**, cuando existan datos redundantes, de que en el diccionario de datos del sistema o en otra documentación se mantienen referencias cruzadas adecuadas.
- 9 **Determinar** cómo y a quien se brinda acceso a datos específicos dentro de esa base de datos concreta.

PARTE II - 1. CONTROLES DE BASES DE DATOS

1.2 ADMINISTRACIÓN DE DATOS

- **Objetivo de Control.**

Deberían asignarse responsabilidades para la planificación, organización, dotación de plantillas y control de los activos de datos de la organización. Cuando proceda, debería establecerse la posición del administrador de datos, en un nivel suficientemente alto dentro de la organización como para asegurar la independencia de juicio y toma de decisiones de quien la ocupe.

- **Directiva de Auditoría.**

Debe revisarse la asignación de la responsabilidad de gestión de los activos de datos de la organización, para evaluar su adecuación.

- 1 **Establecer** si las responsabilidades relacionadas con la administración de los activos de datos de la organización han sido definidas claramente y por escrito, incluyendo, cuando menos, dos puntos.
 - a. Decisiones de política sobre la utilización de activos de datos específicos.
 - b. El establecimiento de políticas de seguridad de los datos, que incluyan la confidencialidad, la integridad y la disponibilidad.
 - c. La coordinación de la creación de datos al ser añadidos a la base de activos de datos.
 - d. La asignación de la responsabilidad del mantenimiento de los elementos de datos, incluyendo, pero sin limitarse a ello, el establecimiento de la propiedad sobre los datos.
- 2 **Identificar** a la persona nombrada para la función de administración de datos para evaluar la competencia administrativa y el nivel en la organización de dicha persona.

1.3 RESPONSABILIDAD DE LA ADMINISTRACIÓN DE LAS BASES DE DATOS

- **Objetivo de Control.**

Debería asignarse la responsabilidad de la administración del entorno de base de datos de la organización. Cuando proceda, debería crearse la función de administrador de las bases de datos, en un nivel suficientemente alto en la estructura de la organización como para asegurar la independencia de la persona que ocupe dicha posición.

- **Directiva de Auditoría.**

Debe revisarse, para evaluar su adecuación, la asignación de la responsabilidad de administración del entorno de gestión de las bases de datos de la organización.

- 1 **Establecer** si las responsabilidades relativas a la administración del entorno de las bases de datos de la organización se han definido claramente y por escrito, incluyendo:
 - a. coordinación
 - b. revisión
 - c. documentación
 - d. formación
 - e. desarrollo y mantenimiento de estándares
 - f. seguridad
- 2 **Identificar** a la persona nombrada para la posición de administración de las bases de datos de la organización, y **evaluar**:
 - a. la competencia técnica y administrativa de dicha persona
 - b. su posición en la organización para asegurar que el interesado tiene independencia y autoridad suficientes para desempeñar las responsabilidades asignadas

3 **Determinar** que el administrador de las bases de datos ha establecido estándares y directivas para ayudar al desarrollo de aplicaciones que utilizan bases de datos. (tales estándares y directivas deberían cubrir aspectos tanto de funcionamiento técnico cuanto de control)

4 **Asegurar** que ninguna otra responsabilidad que pueda haber sido asignada a la persona que ocupa la posición de administrador de las bases de datos, supone la utilización de las bases de datos administradas por dicha persona. (Esta limitación brindará una garantía razonable de segregación de funciones).

1.4 DESCRIPCIÓN DE DATOS Y CAMBIOS DE DATOS

• **Objetivo de Control.**

Deberían establecerse, por escrito, los procedimientos a ser usados en la organización para la descripción de datos, los cambios de datos, y el mantenimiento del diccionario de datos.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos usados en la organización para la descripción de datos, los cambios de datos, y el mantenimiento del diccionario de datos.

1 **Establecer** si el proceso de descripción de datos se lleva a cabo de forma manual o utilizando un logical específico.

2 **Seleccionar** muestras de descripciones de datos y **evaluar**:

a. su adecuación

b. su actualización

c. el grado en que los datos son compartidos en las mismas

3 **Establecer** la forma en que, en el caso de nuevos nombres para datos:

a. se sugiere la adopción de los mismos

b. se aprueban para ser incluidos en la descripción de datos

c. se introducen en la descripción de datos

4 **Asegurar** que los cambios a las descripciones de datos:

a. se solicitan por escrito

b. se acuerden entre los usuarios de descripciones de datos compartidos

c. se aprueban por la dirección

d. se comunican a todos los usuarios de descripciones de datos compartidos

5 **Evaluar** el papel del administrador de las bases de datos en la creación de descripciones de nuevos datos o en el cambio o supresión de descripciones de datos existentes

6 **Determinar** si los estándares y procedimientos de la organización para incorporar nuevos nombres de datos y para cambiar descripciones de datos están puestos por escrito y si se controla su cumplimiento

7 **Determinar** los controles incorporados en cualquier logical usado para crear descripciones de datos y **evaluar** si se controla la adecuación y actualización de dichas descripciones de datos

1.5 CONTROL DE ACCESO A DATOS Y DE CONCURRENCIA

• **Objetivo de Control.**

Los procedimientos usados en la gestión de las bases de datos de la organización deberían contemplar el acceso a los datos en general y el acceso a los datos sensitivos en particular, el control sobre accesos concurrentes a los datos.

PARTE II - 1. CONTROLES DE BASES DE DATOS

• Directiva de Auditoría.

Deben revisarse los procedimientos usados en la gestión de las bases de datos de la organización deberían contemplar el acceso a los datos en general y el acceso a los datos sensitivos en particular, el control sobre accesos concurrentes a los datos.

- 1 **Determinar** que el acceso a datos significativos sólo puede hacerse a través del sistema de gestión de base de datos de la organización.
- 2 **Asegurar** que están identificados los elementos de datos sensitivos contenidos en el sistema de gestión de base de datos y que las autorizaciones para acceder a los mismos son adecuadas y congruentes con la política de la organización.
- 3 **Determinar** cómo el sistema de gestión de las bases de datos y su paquete de logical de seguridad gestionan el acceso a los datos y también las instrucciones y utilidades significativas del sistema de gestión de base de datos.
- 4 **Determinar** que el sistema de gestión de las bases de datos controla a los accesos concurrentes a un mismo elemento de datos y evaluar su adecuación para prevenir un tratamiento erróneo de dichos datos.
- 5 **Determinar** que el sistema de gestión de las bases de datos de la organización ofrece sensibilidad adecuada, a nivel de campo.
- 6 **Asegurar** que las peticiones para autorizar acceso a elementos de datos concretos se hacen por escrito y que se aprueban de acuerdo con los procedimientos escritos significativos de la organización.
- 7 **Comparar** una selección de solicitudes escritas de acceso con las autorizaciones realmente concedidas.
- 8 **Establecer** la existencia de un diario de seguridad en el sistema de gestión

de base de datos de la organización y evaluar su utilidad como pista de auditoría para la revisión del acceso a contenidos específicos de las bases de datos.

- 9 **Determinar** que se han establecido en el sistema de gestión de base de datos de la organización controles que aseguran que las actualizaciones de elementos de datos, sólo pueden hacerse mediante programas de producción autorizados.
- 10 **Determinar** si el concepto de propiedad de los datos si ha establecido en la organización, si se ha identificado al propietario de cada elemento de datos y si éste es consciente de su responsabilidad de garantizar la integridad de tales datos.
- 11 **Asegurar** que el acceso al diccionario de datos está restringido a aquellos de la organización autorizados para efectuar cambios adecuados en su contenido.
- 12 **Determinar** que la organización ha hecho esfuerzos razonables para asegurar que la protección o enclavamiento de registros no crea una condición fatal, y que las aplicaciones no retienen un registro durante más tiempo del necesario.
- 13 **Evaluar** el uso de las características de seguridad del sistema de gestión de base de datos para controlar la autorización de instrucciones de control.

1.6 RECUPERACIÓN DEL CONTENIDO DE LAS BASES DE DATOS

• Objetivo de Control.

La alta dirección de la organización debería establecer procedimientos escritos suficientes para minimizar los fallos, recuperar el entorno de las bases de datos hasta el punto de la caída y mini-

mizar el tiempo necesario para la recuperación.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos de la organización para la recuperación de las bases de datos

- 1 **Evaluar** la adecuación de los procedimientos escritos de la organización para la recuperación tanto física cuanto lógica del entorno de las bases de datos.
- 2 **Indagar** si han sido probados los procedimientos de recuperación de las bases de datos de la organización. Si es así, revisar los resultados de las pruebas para evaluar la adecuación de dichos procedimientos para llevar a cabo la recuperación lógica y física de las bases de datos.
- 3 **Establecer** la forma en que se registran en el sistema de gestión de base de datos de la organización las transacciones —incluyendo registros de la imagen tanto antes cuanto después, evaluar la adecuación de dichas prácticas en la ejecución de una recuperación lógica del contenido de las bases de datos.
- 4 **Determinar** las prácticas de la organización en cuanto a frecuencia de respaldos de las bases de datos y evaluar su adecuación a la luz de la volatilidad de los datos y del tiempo de recuperación de las bases de datos.
- 5 **Cerciorarse** de que los informes de salida de las fases automatizadas de la recuperación se revisan y archivan por el administrador de las bases de datos de la organización.

1.7 INTEGRIDAD DE LAS BASES DE DATOS

• **Objetivo de Control.**

Debieran establecerse procedimientos adecuados para asegurar la integridad de los datos contenidos en las bases de datos de la organización.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos establecidos por la organización para asegurar la integridad de los datos contenidos en sus bases de datos.

- 1 **Evaluar** los procedimientos de control de cambios usados en el lógico del sistema de gestión de bases de datos de la organización.
- 2 **Establecer** si se usan periódicamente programas de utilidad adecuados para comprobar los enlaces físicos — esto es los punteros— asociados con los datos de las bases de datos de la organización.
- 3 **Establecer** si el sistema de gestión de bases de datos de la organización utiliza registros de control para mantener balances transitorios de transacciones para su ulterior cuadro con totales generados por el usuario o por otros sistemas. **Establecer** si los propios elementos de datos son objeto de balance periódico con los registros de control.
- 4 **Establecer** si los estándares de programación de aplicaciones de la organización incluyen:
 - a. la exigencia de que en cada acceso de base de datos se comprueben los códigos de estado.
 - b. medios para manejar los errores
 - c. otras disposiciones para mantener la integridad de las bases de datos

1.8 DISPONIBILIDAD DE LAS BASES DE DATOS

- 1 **Revisar** las disposiciones para el respaldo de equipos y lógico para las bases

PARTE II - 1. CONTROLES DE BASES DE DATOS

de datos, para asegurar la disponibilidad de las bases de datos para aplicaciones críticas en el tiempo.

- 2 **Revisar** la redundancia de la red o las disposiciones que establezcan rutas alternativas para acceder a bases de datos a través de dicha red, para asegurar la disponibilidad de las bases de datos para aplicaciones críticas en el tiempo.

PARTE II: CONTROLES ESPECÍFICOS DE CIERTAS TECNOLOGÍAS

CONTENIDO

2.- CONTROLES DE EXPLOTACIÓN EN INFORMÁTICA DISTRIBUIDA Y REDES	II-2-1
2.1 COMPRENSIÓN DE LOS OBJETIVOS DE LA DIRECCIÓN	II-2-1
2.2 PLAN DE IMPLANTACIÓN	II-2-1
2.3 ESTANDÁRES DE CONTROL PARA LA RED	II-2-2
2.4 OPCIONES DE CONTROL DEL MATERIAL Y LOGICAL	II-2-3
2.5 DISTRIBUCIÓN DE BASES DE DATOS	II-2-3
2.6 ESTÁNDARES DE DATOS PARA LA RED	II-2-4
2.7 ACCESO A DATOS DE LA RED	II-2-5
2.8 MECANISMO DE REVISIÓN DE DATOS DE LA RED	II-2-5
2.9 DISPOSICIONES SOBRE RESPALDO DE MATERIAL Y LOGICAL	II-2-6
2.10 EXPLOTACIÓN DE LA RED	II-2-7
2.11 LOGICAL DE COMUNICACIONES	II-2-8
2.12 ACCESO AL LOGICAL DE SISTEMA OPERATIVO DE LA RED	II-2-8
2.13 ACCESO A LAS INSTALACIONES DE EXPLOTACIÓN DE LA RED	II-2-9
2.14 CIFRA (CRIPTOGRAFÍA) DE DATOS	II-2-10
2.15 SEGURIDAD DE LA RED	II-2-10
2.16 REVISIONES DE SEGURIDAD DE LA RED	II-2-11
2.17 DOCUMENTACIÓN Y FORMACIÓN DEL PERSONAL DE OPERACIÓN DE LA RED	II-2-12
2.18 REVISIÓN POST-IMPLANTACIÓN DE LA RED	II-2-12
2.19 CONTROL DE FUNCIONAMIENTO DE LA RED	II-2-13
2.20 PLANES DE CONTINGENCIA DE EXPLOTACIÓN DE LA RED	II-2-14

* * *

PARTE II - 2. CONTROLES DE EXPLOTACION EN INFORMATICA DITRIBUIDA Y REDES

2.- CONTROLES DE EXPLOTACIÓN EN INFORMÁTICA DISTRIBUIDA Y REDES

Una informática distribuida debiera brindar a los departamentos usuarios de la organización datos de forma descentralizada, basándose en consideraciones de coste-beneficio. Deben contemplarse los procedimientos para explotar la informática distribuida de forma controlada y segura.

2.1 COMPRENSIÓN DE LOS OBJETIVOS DE LA DIRECCIÓN

• Objetivo de Control.

La decisión de adoptar informática distribuida por la alta dirección de la organización debiera estar documentada y basarse en análisis coste-beneficio.

• Directiva de Auditoría.

Debe revisarse la decisión de la alta dirección de la organización de adoptar informática distribuida y deben evaluarse los análisis de coste-beneficio pertinentes.

1. **Revisar** los objetivos a corto y largo plazo establecidos por la alta dirección de la organización para la informática distribuida. Tales objetivos debieran incluir, cuando menos:

- a. situar los recursos informáticos más próximos al usuario descentralizado
- b. situar la información generada por los ordenadores más próxima a la dirección descentralizada de la organización
- c. mejorar el coste-beneficio general del tratamiento de datos
- d. mejorar el tiempo de respuesta de los recursos informáticos tanto a nivel de dirección central cuanto descentralizado
- e. empleo de la red de informática distribuida en lugar de los procedimientos actuales de respaldo de explotación de proceso de datos.

2. **Evaluar** si los requisitos definidos para la informática distribuida responden a los objetivos de la alta dirección de la organización en términos de:

- a. configuración de equipos: esto es, si es centralizada, interconectada o plenamente distribuida
- b. configuración de la base de datos: esto es, si es centralizada, partida o duplicada una o más veces
- c. el interfaz entre los equipos y la red de comunicaciones.

3. **Revisar** las especificaciones definidas por la alta dirección de la organización para la informática distribuida en términos de los análisis de coste-beneficio pertinentes, para determinar si:

- a. la dirección ha recibido datos de coste-beneficio de configuraciones de informática distribuida alternativas y viables
- b. si los objetivos de la dirección han tenido en cuenta los datos de coste-beneficio que se le han suministrado
- c. si los análisis de coste-beneficio han sido preparados adecuadamente.

2.2 PLAN DE IMPLANTACIÓN

• Objetivo de Control.

Debieran desarrollarse planes adecuados de implantación, conversión y pruebas de aceptación para la red de informática distribuida de la organización.

• Directiva de Auditoría.

Deben revisarse los planes de la organización para la implantación, conversión y pruebas de aceptación de su red de informática distribuida.

1. **Revisar** el plan general de la organización para implantar su red de informática distribuida y asegurarse de que el logical a ser usado se desarrollará de

PARTE II - 2. CONTROLES DE EXPLOTACION EN INFORMATICA DITRIBUIDA Y REDES

conformidad con la metodología de ciclo de vida del desarrollo de sistemas de la organización.

2. **Evaluar** el plan de implantación y pruebas de los ordenadores y enlaces de comunicaciones de la red.

3. **Revisar** el plan de conversión general a la red de informática distribuida de la organización y Verificar que:

a. todos los usuarios e interfaces han sido incluidos en el desarrollo del plan

b. que el plan ha contemplado cualquier riesgo especial asociado a la red

c. que el plan ha tenido en cuenta las diversas necesidades de proceso de datos de los usuarios de la red en diferentes localidades.

4. **Revisar** el plan general de la organización para la aceptación de la red de informática distribuida y **verificar** que:

a. el plan fue desarrollado conjuntamente por el Departamento de Informática y la dirección de los departamentos usuarios afectados

b. en el plan de aceptación de la red se han incluido procedimiento de prueba y criterios de aceptación prescritos por los usuarios

c. los departamentos usuarios afectados han participado en las pruebas de aceptación de la red y han revisado y aprobado los resultados de las mismas.

5. **Revisar** las determinaciones de naturaleza operativa del plan de implantación de informática distribuida de la organización para determinar su coherencia con las leyes y regulaciones que rigen la transmisión de datos en el país y con las leyes y regulaciones internacionales que rigen la transmisión de datos transfronteriza.

2.3 ESTANDÁRES DE CONTROL PARA LA RED

• **Objetivo de Control.**

El Departamento de Informática debiera establecer y mantener, de forma actualizada, políticas y estándares para el control general de la red de informática distribuida de la organización.

• **Directiva de Auditoría.**

Debe revisarse el grado de actualización y adecuación de las políticas y estándares establecidos por el Departamento de Informática para el control general de la red para informática distribuida de la organización.

1. **Verificar** que los procedimientos de control generales de la red de informática distribuida establecidos por el Departamento de Informática se prueban y evalúan periódicamente.

2. **Verificar** que existe un grupo de control de la red de informática distribuida, compuesto por representantes de todos los departamentos usuarios afectados y del Departamento de Informática, que revisa periódicamente las políticas y estándares pertinentes de control de la red.

3. **Establecer** que la autoridad y responsabilidad de mantener los controles de la red de informática distribuida de la organización se ha distribuido a los departamentos usuarios afectados de forma paralela a la distribución general de las capacidades de proceso de la red asignadas a tales departamentos.

4. **Revisar** las declaraciones escritas de la organización que tratan de las actividades que pueden procesarse en la red de informática distribuida y anotar cualesquiera excepciones y condiciones calificativas contenidas en dichas declaraciones y si el tratamiento real de tales actividades es conforme a dichas declaraciones.

5. **Verificar** que el Departamento de Informática ha establecido un mecanismo para asegurar la compatibilidad de conjuntos de datos entre aplicaciones

cuando la red de informática distribuida de la organización crece en tamaño y complejidad.

6. **Verificar** que el Departamento de Informática ha distribuido a los lugares en que se encuentran departamentos usuarios afectadas declaraciones escritas de procedimientos operativos relativas a la red de informática distribuida de la organización.

7. **Verificar** que el Departamento de Informática ha emitido una declaración escrita de política que exige crear de forma rutinaria pistas de auditoría y registros de respaldo para todos los mensajes de la red de informática distribuida y los datos relacionados con aplicaciones.

8. **Examinar** una muestra representativa de las declaración escrita de política de la organización acerca de la red de informática distribuida y las operaciones locales. Verificar que dichas declaraciones están actualizadas y que se aplican de forma congruente y determinar si las posibles peticiones de cambio o modificación de las declaraciones se han remitido de forma rutinaria al grupo de revisión del control de la red.

2.4 OPCIONES DE CONTROL DEL MATERIAL Y LOGICAL

- **Objetivo de Control.**

El Departamento de Informática debiera establecer políticas para la selección y adquisición de las opciones de control a utilizar con el material y logical instalado en la red de informática distribuida de la organización.

- **Directiva de Auditoría.**

Deben revisarse las políticas establecidas por el Departamento de Informática para la selección y adquisición de las opciones de control a ser utilizadas por el material y logical utilizado en la red de informática distribuida de la organización.

1. **Revisar** cualquier declaración escrita de política que haya sido emitida por el

Departamento de Informática acerca de las opciones de control del material y logical a ser incluidas en la red de informática distribuida de la organización.

2. **Entrevistar** a aquellos miembros del Departamento de Informática responsable del desarrollo o adquisición de las opciones de control del material y logical a ser incluidas en la red de informática distribuida de la organización y **verificar** que hay un plan para la oportuna adquisición de los controles requeridos.

3. **Apreciar** las opciones de control del material y logical y **determinar** si --cuando se combinan con el control existente o previsto por el usuario-- puede asegurarse un control continuado de la integridad de la red de informática distribuida de la organización.

2.5 DISTRIBUCIÓN DE BASES DE DATOS

- **Objetivo de Control.**

El Departamento de Informática debiera establecer procedimientos que definan los controles y medidas de seguridad a ser usados en la red de informática distribuida de la organización en conexión con la distribución del contenido de bases de datos entre los departamentos que usan la red.

- **Directiva de Auditoría.**

Debe revisarse el impacto de los controles y medidas de seguridad establecidos por el Departamento de Informática sobre la distribución de contenidos de las bases de datos entre los departamentos que utilizan la red de informática distribuida de la organización.

1. **Evaluar** la conformidad con los procedimientos establecidos por el Departamento de Informática de distribución de contenidos de las bases de datos entre los departamentos que utilizan la red de informática distribuida de la organización.

2. **Entrevistar** a representantes de los departamentos usuarios y del Departamento de Informática para **verificar** el grado de actualización de la documentación sobre datos para la red de informática distribuida de la organización y **confirmar** esto seleccionando unos pocos conjuntos de datos existentes y comparándolos con la documentación pertinente sobre los datos.

2.6 ESTÁNDARES DE DATOS PARA LA RED

• Objetivo de Control.

El Departamento de Informática debiera establecer controles de la utilización del contenido de las bases de datos. Dichos controles debieran ser efectivos para asegurar la compatibilidad e integridad de dicho contenido y la eficiencia de su utilización. El Departamento de Informática debiera ofrecer formación adecuada sobre la utilización de dichos controles.

• Directiva de Auditoría.

Deben revisarse los controles establecidos por el Departamento de Informática sobre la utilización del contenido de las bases de datos y la formación impartida a los departamentos usuarios sobre la utilización de dichos controles.

1. **Revisar** los controles establecidos por el Departamento de Informática sobre la utilización de contenidos de las bases de datos en la red de informática distribuida de la organización, con el administrador de bases de datos del Departamento y con representantes seleccionados de los departamentos usuarios. **Determinar** que se han implantado mecanismos adecuados a través de tales controles para estandarizar las definiciones de datos compartidos, para mantener diccionarios de datos comunes y para reconciliar desviaciones respecto de las definiciones de los datos.

2. **Verificar** que los controles establecidos por el Departamento de Informática sobre la utilización de contenidos de las bases de datos en la red de informática

distribuida de la organización prohíben a usuarios de la red el redefinir arbitrariamente las definiciones de datos.

3. **Verificar** que los controles establecidos por el Departamento de Informática sobre la utilización de contenidos de las bases de datos de la red de informática distribuida de la organización exigen que se establezca siempre con claridad la propiedad de los conjuntos de datos. **Asegurarse** de que las responsabilidades de reconciliar y coordinar cualesquiera diferencias entre las bases de datos distribuidas o copiadas antes de comenzar la explotación de la red, están claramente definidas.

4. **Seleccionar** procedimientos representativos de reconciliación de las bases de datos que ya vienen siendo explotadas por la organización y **compararlas** con registros previamente procesados en la red de informática distribuida. **Verificar** que tales reconciliaciones pueden llevarse a cabo satisfactoriamente en condiciones normales de explotación así como el en período subsiguiente a un fallo de la red sin ser perturbadas por cosas tales como cualesquiera cambios en los cierres de fin de mes de los diversos departamentos que usan la red.

5. **Verificar** que los controles establecidos por el Departamento de Informática sobre la utilización de contenidos de las bases de datos explotados en la red de informática distribuida de la organización facilitan su fácil integración y consolidación o resumen al nivel general de la organización.

6. **Determinar** si los controles establecidos por el Departamento de Informática sobre la utilización de contenidos de las bases de datos explotadas en la red de informática distribuida de la organización definen adecuadamente los procedimientos a ser usados para controlar los cambios en los conjuntos de datos. **Verificar** que dichos procedimientos aseguran la compatibilidad de los datos, se aplican a todos los conjuntos de datos de la red y pueden llevarse a cabo con puntualidad.

7. **Verificar** que a los usuarios de la red de informática distribuida de la organización se les viene suministrando documentación y formación adecuada sobre el desarrollo del contenido de los conjuntos de datos y sobre la utilización de los controles establecidos por el Departamento de Informática.

2.7 ACCESO A DATOS DE LA RED

• Objetivo de Control.

El Departamento de Informática debiera establecer y mantener un control adecuado tanto sobre la explotación del Departamento cuanto sobre la de los departamentos usuarios, respecto a la seguridad del contenido de las bases de datos usadas en la red de informática distribuida de la organización.

• Directiva de Auditoría.

Deben revisarse los procedimientos establecidos por el Departamento de Informática para controlar la seguridad de los contenidos de las bases de datos utilizadas en la red de informática distribuida de la organización.

1. **Verificar** la eficacia de los procedimientos de seguridad establecidos por el Departamento de Informática para la red de informática distribuida de la organización respecto de los sistemas de gestión de bases de datos utilizados y para instalaciones seleccionadas de los departamentos usuarios.

2. **Determinar** la eficacia de las políticas establecidas por el Departamento de Informática para la identificación y oportuna retirada de los datos redundantes mantenidos en la red de informática distribuida de la organización.

3. **Determinar** la eficacia de las políticas establecidas por el Departamento de Informática para la identificación y clasificación de datos sensibles mantenidos en la red de informática distribuida de la organización.

a. **verificar** que todos los conjuntos de datos sensibles de la red se han identificado y que se han determina-

do las especificaciones para su seguridad. **Asegurarse** de que todos los conjuntos de datos agrupados o combinados que son accesibles por un usuario único se han incluido en este proceso.

b. **determinar** si un tráfico pesado de datos a través de líneas de comunicación amplias o carentes de monitorización restringe de forma significativa la capacidad del Departamento de Informática para mantener la seguridad de la red de informática distribuida de la organización

c. **verificar** que el Departamento de Informática ha establecido y comunicado a los departamentos usuarios los procedimientos a ser utilizados para disponer de documentos sensibles relacionados con la red de informática distribuida de la organización.

4. **Determinar** si el Departamento de Informática ha establecido procedimientos efectivos para coordinar la operación de los programas de aplicación y el contenido de las diversas bases de datos entre las instalaciones de departamentos usuarios servidas por la red de informática distribuida de la organización.

2.8 MECANISMO DE REVISIÓN DE DATOS DE LA RED

• Objetivo de Control.

El Departamento de Informática debiera establecer procedimientos que aseguren su control efectivo sobre el material y logical utilizado por los departamentos servidos por la red de informática distribuida de la organización.

• Directiva de Auditoría.

Deben revisarse los procedimientos establecidos por el Departamento de Informática para asegurar el control efectivo del material y logical utilizado por los departamentos servidos por la red de informática distribuida de la organización.

PARTE II - 2. CONTROLES DE EXPLOTACION EN INFORMATICA DITRIBUIDA Y REDES

1. **Determinar** mediante entrevistas con miembros del Departamento de Informática responsables de la gestión de la red de informática distribuida de la organización que se ha establecido una función centralizada para controlar la utilización del material y los datos de las diversas instalaciones de departamentos usuarios servidas por la red.

2. **Determinar** que los departamentos usuarios mantienen inventarios de los activos de la red de informática distribuida de la organización que están en sus instalaciones y que se revisa periódicamente la actualización y exactitud de dichos registros de inventario.

3. **Verificar** que el Departamento de Informática ha establecido procedimientos para los departamentos usuarios servidos por la red de informática distribuida de la organización para revisar periódicamente la eficacia de las prácticas operativas y de seguridad de los datos utilizadas en las instalaciones.

4. **Determinar** que se suministran a la función de control central de la red del Departamento de Informática informes de los resultados de dichas revisiones, y que ahí se comparan los contenidos de tales informes con los registros pertinentes de funcionamiento de la red.

5. **Determinar** si dichos informes comparativos se utilizan para verificar:
(1) que el control ejercido por los departamentos usuarios sobre el material, logical y datos utilizados en sus instalaciones y (2) que se distribuyen resúmenes de los informes comparativos a los directivos de los departamentos usuarios.

2.9 DISPOSICIONES SOBRE RESPALDO DE MATERIAL Y LOGICAL

* **Objetivo de Control.**

El Departamento de Informática debiera establecer procedimientos de respaldo del material y logical utilizado en la red de informática distribuida de la organización.

* **Directiva de Auditoría.**

Deben revisarse los procedimientos establecidos por el Departamento de Informática para respaldo del material utilizados en la red de informática distribuida de la organización.

1. **Determinar**, mediante entrevistas con aquellos miembros de la directiva de la plantilla del Departamento de Informática responsables de la gestión de la red de informática distribuida de la organización, que el material, logical y datos almacenados en cada instalación de los departamentos usuarios están respaldados en otra instalación y pueden ser transmitidos cuando y a donde sea necesario de forma puntual si se produce una interrupción en las operaciones de la red.

2. **Verificar** que la red de informática distribuida de la organización ha sido diseñada para asegurar que el fallo de servicio en cualesquiera de las instalaciones de los departamentos usuarios tenga solo un efecto mínimo sobre el servicio continuado a las otras instalaciones servidas por la red. (si ese no es el caso, incluir en el informe de auditoría cualesquiera oportunidades de cambio de configuración de la red que hayan sido identificadas).

3. **Verificar** que en cada instalación de los departamentos usuarios servidos por la red de informática distribuida de la organización se han instalado mecanismos adecuados de re-arranque y recuperación, y que dichos mecanismos minimizan la participación del usuario en el restablecimiento de los ficheros de datos y transacciones hasta el momento de caída de la red.

4. **Determinar** si el Departamento de Informática ha establecido para cada instalación de los departamentos usuarios servidos por la red de informática distribuida de la organización procedimientos adecuados de recuperación de desastres y si tales procedimientos se prueban se prueban periódicamente para comprobar que se son adecuados y están actualizados.

5. **Determinar** los procedimientos operativos establecidos, en los casos en que se haya instalado equipos conmutadores de telecomunicaciones o "patch" para ser utilizados en la red de informática distribuida de la organización, para permitir reasignaciones de terminales, controladores de agrupaciones de equipos u otros dispositivos para el respaldo de otras operaciones de la red. **Asegurarse** de que dicha opción no puede ser utilizada para transferir una sesión en línea de un terminal a otro de modo que no fuera detectable por el logical de comunicaciones de la red.

2.10 EXPLOTACIÓN DE LA RED

• Objetivo de Control.

El Departamento de Informática debiera establecer procedimientos para asegurar que en la explotación de la red de informática distribuida de la organización se coordinan, controlan y gestionan adecuadamente cosas tales como las especificaciones de salida, los calendarios de explotación, los procedimientos de tratamiento y las prácticas de mantenimiento preventivo.

• Directiva de Auditoría.

Deben revisarse los procedimientos establecidos por el Departamento de Informática para la gestión de explotación de la red de informática distribuida de la organización.

1. **Determinar**, mediante entrevistas a los miembros de la plantilla del Departamento de Informática responsables de la gestión de la red de informática distribuida de la organización y a representantes de departamentos usuarios seleccionados servidos por la red, que se han establecido por los departamentos usuarios y comunicado a la función de control de explotación de la red del Departamento de Informática especificaciones para todas las aplicaciones acerca de la disponibilidad de la red, de información, de horario y tiempo de res-

puesta, de almacenamiento, de respaldo y de control operativo.

2. **Verificar** que todos los departamentos usuarios servidos por la red de informática distribuida de la organización se comunican periódicamente para discutir los calendarios de explotación y para coordinar sus especificaciones de tratamiento y procedimientos operativos.

3. **Determinar** si todas las instalaciones de los departamentos usuarios servidos por la red de informática distribuida de la organización establecen previsiones de sus necesidades de suministro de material fungible, registran su utilización y la coordinan con los contratos pertinentes con los suministradores.

4 **Verificar** que en todas las instalaciones de los departamentos usuarios servidos por la red de informática distribuida de la organización se efectúa mantenimiento preventivo del material según un calendario periódicamente. **Determinar** que para todos los equipos de todas las instalaciones se mantienen registros de los problemas de mantenimiento y **verificar** cuán razonables son los calendarios de mantenimiento preventivo, mediante un examen de sus registros periódicos.

5. **Identificar** oportunidades para mejorar la coordinación de la explotación de la red de informática distribuida de la organización.

6. **Identificar** todos los terminales de control remoto y de red local utilizados en la red de informática distribuida de la organización y **determinar** las personas autorizadas para utilizarlos. **Verificar** que el ámbito de los comandos de control de la red en línea —tales como los que activan y desactivan nodos— es apropiado a las responsabilidades y nivel de experiencia de cada una de tales personas.

PARTE II - 2. CONTROLES DE EXPLOTACION EN INFORMATICA DITRIBUIDA Y REDES

2.11 LOGICAL DE COMUNICACIONES

• **Objetivo de Control.**

El Departamento de Informática debiera establecer procedimientos para la gestión y control del uso de logical de comunicaciones en la red de informática distribuida de la organización.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos establecidos por el Departamento de Informática para la gestión y control de logical de comunicaciones en la red de informática distribuida de la organización.

1. **Determinar**, mediante entrevistas a los miembros de la plantilla del Departamento de Informática responsables del diseño y mantenimiento de las comunicaciones en la red de informática distribuida de la organización, que se utilizan procedimientos estándares de transmisión de datos y que se han enviado descripciones escritas de tales procedimientos a cada una de las instalaciones servidas por la red.

2. **Determinar** si cada mensaje de la red o cada unidad de datos transmitida enviada a través de la red de informática distribuida de la organización contiene códigos que identifican al emisor y al destinatario. Verificar que todos los mensajes de salida se validan de forma rutinaria para asegurar que contienen direcciones de destino válidas.

3. **Determinar** si existen procedimientos en la red de informática distribuida de la organización para: (1) almacenar temporalmente mensajes destinados a instalaciones de departamentos usuarios que no están en servicio en el momento de transmisión original del mensaje y (2) retransmitir automáticamente tales mensajes cuando dichas instalaciones vuelven a estar en servicio.

4. **Verificar** que el Departamento de Informática ha emitido declaración escrita relativas al mantenimiento de posibilidades de comunicación normales o alternativas en la red de informática distribuida de la organización, y que en

cada una de las instalaciones de los departamentos usuarios servidas por la red hay copias actualizadas.

5. **Revisar** las prioridades de transmisión asignadas a los mensajes enviados por la red de informática distribuida de la organización. Las definidas por tipo de usuario debieran utilizar tablas de identificación del usuario. Las definidas por líneas debieran utilizar prioridades de interrupción de líneas.

6. **Determinar** que tales asignaciones son congruentes con las políticas pertinentes de la alta dirección de la organización y que son adecuadas para las necesidades de los departamentos usuarios implicados.

7. **Verificar** que todo logical adquirido para ser usado en la red de informática distribuida de la organización contiene rutinas incorporadas de corrección de errores y características de control y análisis del funcionamiento.

8. **Verificar** que el logical utilizado en la red de informática distribuida de la organización es mantenido bien por personal encargado en el Departamento de Informática o por representantes del proveedor adecuado.

2.12 ACCESO AL LOGICAL DE SISTEMA OPERATIVO DE LA RED

• **Objetivo de Control.**

El Departamento de Informática debiera establecer procedimientos para gestionar y controlar el uso seguro de —y cualesquiera cambios a— el logical de sistema operativo utilizado en la red de informática distribuida de la organización.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos establecidos por el Departamento de Informática para gestionar y controlar la utilización de logical de sistema operativo utilizado por la red de informática distribuida de la organización.

1. **Verificar** que todos los cambios al logical de sistema operativo usado por

la red de informática distribuida de la organización introducidos en las instalaciones de los departamentos usuarios y por el Departamento de Informática son controlados por el Departamento de Informática y que los miembros de dicho Departamento de Informática responsables de la gestión de explotación de la red pueden detectar rápidamente cualquier cambio no autorizado.

2.13 ACCESO A LAS INSTALACIONES DE EXPLOTACIÓN DE LA RED

* Objetivo de Control.

El Departamento de Informática debiera establecer procedimientos para restringir el acceso no autorizado a las instalaciones de explotación y tratamiento de la red de informática distribuida de la organización.

* Directiva de Auditoría.

Deben revisarse los procedimientos establecidos por el Departamento de Informática para restringir el acceso no autorizado a las instalaciones de explotación y tratamiento de la red de informática distribuida de la organización.

1. **Revisar** los procedimientos de seguridad establecidos por el Departamento de Informática para las instalaciones centrales o la principal de explotación de la red de informática distribuida de la organización. **Verificar** que el acceso al material de prueba de la red y a las líneas de comunicación locales o privadas que se usen está adecuadamente controlado.

2. **Asegurarse** de que los números de teléfono utilizados para acceder a la red de informática distribuida de la organización se cambian periódicamente y que en ningún caso figuran en los listines. **Determinar** si se han establecido controles adecuados de acceso y uso de dichas líneas.

3. **Determinar** si para identificar la localización de alguien que intenta acceder a la red mediante dispositivos de telecomunicación por red conmutada es

deseable emplear un procedimientos automático o manual de devolución de la llamada.

4 **Determinar** si se usan palabras de paso en línea para identificar a los usuarios de terminales u ordenadores conectados a la red de informática distribuida de la organización y que cuando se introducen las palabras de paso éstas no quedan impresas.

5. **Verificar** que las palabras de paso tienen una longitud suficiente y que no son palabras del diccionario para desanimar a los asediadores "hackers" de intentar adivinarlas.

6. **Determinar** que, siempre que desde un terminal u ordenador personal se intente un número predeterminado de accesos no autorizados a la red de informática distribuida de la organización, éste se desconecta automáticamente y que se requiere un permiso especial para reactivar dicha conexión.

7. **Determinar** si en el sistema operativo de la red de informática distribuida de la organización se han establecido perfiles de usuarios individuales para restringir los recursos de la red a los que tienen acceso. **Verificar** que los procedimientos para establecer tales perfiles disponen que:

a. dichas personas deben tener acceso solamente a aplicaciones, procesadores de transacciones y conjuntos de datos autorizados

b. se prohíbe a todos los usuarios de la red introducir comandos en un sitio para ser ejecutados en otro distinto

c. el uso de los comandos de sistema que afecten a más de una instalación de la red, queda restringido a un terminal y que sólo a una persona autorizada que tiene una responsabilidad general de control de la red y una acreditación de seguridad adecuada puede iniciar esos comandos

d. los perfiles del usuario sólo pueden ser modificados por personal autoriza-

PARTE II - 2. CONTROLES DE EXPLOTACION EN INFORMATICA DITRIBUIDA Y REDES

do que tiene autoridad de control sobre la red.

8. **Verificar** que las instalaciones de los departamentos usuarios se desconectan automáticamente de la red de informática distribuida de la organización siempre que dicha instalación normalmente no está en funcionamiento. **Verificar** también que sólo se producen excepciones cuando el Departamento de Informática ha aprobado una exención especial de este requisito.

9. **Verificar** que se preparan informes regulares que contienen todas las violaciones de acceso por instalación de departamentos usuarios y que dichos informes se revisan de forma oportuna por los miembros del Departamento de Informática responsables de mantener y controlar la seguridad de la red de informática distribuida de la organización.

2.14 CIFRA (CRIPTOGRAFÍA) DE DATOS

* Objetivo de Control.

El Departamento de Informática debiera establecer procedimientos para proteger mediante cifra, siempre que sea apropiado, los datos sensibles en la red de informática distribuida de la organización.

* Directiva de Auditoría.

Deben revisarse los procedimientos establecidos por el Departamento de Informática para proteger mediante cifra, siempre que sea apropiado, los datos sensibles en la red de informática distribuida de la organización.

1. **Revisar** las políticas de la alta dirección relativas a la protección de datos sensibles en la organización. **Determinar** si alguna de la información transmitida o utilizada por la red de informática distribuida de la organización se considera, bajo tales políticas, como información crítica, sensible o personal que debiera ser protegida. (Los datos sensibles están definidos por leyes o regulaciones pertinentes o son aquellos cuya revelación

no autorizada pudiera dañar o molestar a la organización).

2. **Evaluar** la eficacia de los procedimientos usados para proteger datos sensibles en la red de informática distribuida de la organización. **Revisar** cualquier análisis de coste-beneficio de la posible utilización de cifra (criptografía) de datos o de la adquisición de instalaciones de líneas de telecomunicación privadas. **Apreciar** lo razonable de las conclusiones de dichos análisis.

3. **Determinar**, en los casos en que se usa cifra en la red de informática distribuida de la organización, que el acceso a las declaraciones de procedimientos escritas pertinentes está adecuadamente protegido y que:

a. que a la persona que tiene asignada la responsabilidad de gestionar la responsabilidad y uso de la clave de cifra no se le han encomendado otras tareas que pudieran ser comprometedoras por implicar el tratamiento de datos en la red

b. el algoritmo utilizado para cifrar los datos es efectivo y, en particular, que los datos que se cifran bajo dicho algoritmo se hacen en función de un campo de datos variable de modo que el contenido o naturaleza de los datos cifrados no pueda deducirse a partir del conocimiento de la información no cifrada o de otros elementos cifrados del fichero de datos pertinente

c. cuando se utilizan equipos para cifrar los datos, éstos son capaces de procesarlos en un módulo físico totalmente seguro y a una tasa eficiente y que no revelará datos no cifrados como consecuencia de intentos de intrusión.

2.15 SEGURIDAD DE LA RED

* Objetivo de Control.

El Departamento de Informática debiera establecer procedimientos para mantener la seguridad física y lógica de la red

de informática distribuida de la organización.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos establecidos por el Departamento de Informática para mantener la seguridad física y lógica de la red de informática distribuida de la organización.

1. **Determinar**, mediante entrevistas al personal del Departamento de Informática responsable de la seguridad de la red de informática distribuida de la organización, que el tipo de dicha protección de seguridad puede calificarse como uno de los siguientes:

a. altamente distribuida: la seguridad está bajo control de los directivos de cada departamentos usuarios

b. distribuida: la seguridad está bajo control de los directivos de cada departamentos usuarios pero cumple directivas establecidas por el Departamento de Informática

c. mixta: la seguridad está bajo el control de los directivos de cada departamentos usuarios pero la responsabilidad general sobre la misma la retiene el Departamento de Informática

d. centralizada: la seguridad está bajo la dirección del Departamento de Informática, el cual sin embargo mantiene una estrecha relación con los directivos de los departamentos usuarios

e. altamente centralizada: la seguridad está bajo el control completo del Departamento de Informática.

2. **Verificar** que el tipo de protección de seguridad en la red de informática distribuida de la organización es adecuado para su configuración actual y **asegurarse**, en particular, que no se está aplicando un tipo de protección de seguridad altamente distribuida en una red altamente centralizada.

3. **Revisar** las declaraciones escritas de procedimientos tanto de Departamento de Informática cuanto de los departamentos usuarios pertinentes que se refieren a la seguridad de la red de informática distribuida de la organización y **determinar** si son:

a. adecuadas para proteger (1) las instalaciones físicas de la red, (2) la integridad de su logical de aplicación y (3) los datos —de entrada, salida y almacenados por el Departamento de Informática en las diversas instalaciones de los departamentos usuarios— de conformidad a la sensibilidad asignada o a las clasificaciones de seguridad.

b. revisadas periódicamente por la función de control de la Informática distribuida del Departamento de Informática o su grupo de garantía de calidad para asegurar que son adecuadas y están actualizadas.

2.16 REVISIONES DE SEGURIDAD DE LA RED

• **Objetivo de Control.**

El Departamento de Informática debiera establecer procedimientos para revisiones periódicamente por la dirección de los departamentos usuarios afectados por la red de informática distribuida de la organización.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos establecidos por el Departamento de Informática para revisiones periódicamente por la dirección de los departamentos usuarios para la seguridad de la red de informática distribuida de la organización.

1. **Determinar**, mediante entrevistas a miembros seleccionados de la plantilla de los departamentos usuarios responsables directamente de controlar la seguridad de la red de informática distribuida

PARTE II - 2. CONTROLES DE EXPLOTACION EN INFORMATICA DITRIBUIDA Y REDES

de la organización, que la seguridad de todas las instalaciones servidas por la red que ellos revisan la seguridad periódicamente de forma congruente, y que cualesquiera problemas detectados en el curso de tales revisiones se comunican oportunamente a la dirección.

2. **Evaluar** la adecuación de la respuesta de la dirección a dichos problemas.

3. **Verificar** que los procedimientos utilizados en las revisiones por los departamentos usuarios de la seguridad de la red de informática distribuida de la organización incluyen: (1) un examen de todo el material, sistemas operativos, operadores de transacciones y datos, de explotación y comunicaciones, (2), una revisión de toda la documentación de seguridad pertinente, para determinar si está actualizada, y (3) una prueba de la concienciación de los usuarios individuales acerca de las políticas y procedimientos de seguridad pertinentes.

4 **Verificar** que se producen oportunamente y se distribuyen a la dirección de todos los departamentos usuarios afectados informes consolidados de los resultados de las revisiones por los departamentos usuarios de la red de informática distribuida de la organización.

2.17 DOCUMENTACIÓN Y FORMACIÓN DEL PERSONAL DE OPERACIÓN DE LA RED

• **Objetivo de Control.**

El Departamento de Informática debiera establecer procedimientos para brindar documentación y formación suficientes a los usuarios de la red de informática distribuida de la organización.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos establecidos por el Departamento de Informática para brindar documentación y formación adecuadas a los usuarios de la red de informática distribuida de la organización.

1. **Revisar** la documentación y los planes de formación que se han desarrollado

en las instalaciones de los usuarios seleccionados en la red de informática distribuida de la organización. **Verificar** que la documentación está actualizada y es completa y que toda la formación solicitada se imparte oportunamente.

2. **Verificar** que los departamentos que utilizan la red de informática distribuida de la organización han recibido instrucciones escritas sobre la fijación de parámetros u opciones estándar para los dispositivos de transmisión de datos que están utilizando y los procedimientos a ser empleados para identificar problemas en la red. **Examinar** los registros disponibles sobre problemas operativos de la red para **determinar** qué proporción de los mismos puede ser atribuida a una inadecuada formación de los usuarios.

3. **Verificar** la precisión de los registros usados por los miembros de la plantilla del Departamento de Informática que explotan la red de informática distribuida de la organización, para identificar problemas de explotación de la red. **Comparar** la correlación entre nombres lógicos de dispositivos y etiquetas externas de los dispositivos con las definiciones de dispositivos de la red usadas para generar el método de acceso de telecomunicaciones usado por la red a fin de **determinar** la precisión de este tipo de registros.

4. **Verificar** que los cables, modems, unidades de control y otros componentes físicos de la red de informática distribuida de la organización tienen etiquetas externas adecuadas. Un sistema de etiquetado externo inadecuado conducirá posiblemente a debilidades en la rápida identificación y resolución de fallos.

2.18 REVISIÓN POST-IMPLANTACIÓN DE LA RED

• **Objetivo de Control.**

El Departamento de Informática debiera establecer procedimientos para efectuar una revisión post-implantación de la red de informática distribuida de la organiza-

ción para asegurar que su estructura y funcionamiento son conformes con las especificaciones de los departamentos usuarios.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos establecidos por el Departamento de Informática para efectuar una revisión post-implantación de la red de informática distribuida de la organización que asegure que su estructura y funcionamiento son conformes con las especificaciones de los departamentos usuarios.

1. **Determinar**, mediante entrevistas a las personas del Departamento de Informática responsables de la implantación de la red de informática distribuida de la organización, y examinando la información pertinente, debe llevarse a cabo una revisión técnica de la red después de su implantación.

2. **Determinar**, mediante entrevistas con la dirección de departamentos usuarios seleccionados, si la implantación de la red de informática distribuida de la organización es conforme con sus especificaciones de uso de dicha red.

3. **Revisar** los resultados de la revisión post-implantación. **Verificar** que aquellas especificaciones de diseño y funcionamiento de la red que no han sido satisfechas han sido programadas en un calendario para su implantación oportuna. **Determinar** las prioridades establecidas para satisfacer especificaciones individuales no satisfechas.

4. **Determinar**, mediante entrevistas al personal del Departamento de Informática responsable de la implantación de la red de informática distribuida de la organización y con directivos de departamentos usuarios seleccionados, la naturaleza y razones de cualesquiera diferencias entre los costes y tiempos estimados y reales de implantación de la red.

6. **Asegurarse**, una vez transcurrido un período de tiempo adecuado, que la red de informática distribuida de la

organización está cumpliendo los objetivos de funcionamiento especificados.

2.19 CONTROL DE FUNCIONAMIENTO DE LA RED

• **Objetivo de Control.**

El Departamento de Informática debiera establecer procedimientos adecuados para controlar y medir el funcionamiento del sistema de sistema de informática distribuida de la organización.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos establecidos por el Departamento de Informática para controlar y medir el funcionamiento del sistema de informática distribuida de la organización.

1. **Determinar**, mediante entrevistas a los miembros del Departamento de Informática responsables de controlar el funcionamiento de la red de informática distribuida de la organización, y mediante un examen de la documentación de las especificaciones de la red por los usuarios, que se han establecido criterios adecuados de funcionamiento del material y de la explotación.

2. **Revisar** los registros producidos por los mecanismos de control y optimización de funcionamiento de la red de informática distribuida de la organización para **determinar** si:

a. existe una estructura que asegure que la explotación de máxima prioridad se lleva a cabo y se transmite en primer lugar

b. se han desarrollado o adquirido procedimientos automáticos para resolver cierres del sistema, también denominados abrazos mortales.

c. los controles de material y logical no degradan significativamente el funcionamiento general de la red

d. se utiliza periódicamente un monitor de logical para medir las eficiencias de la red y su explotación

PARTE II - 2. CONTROLES DE EXPLOTACION EN INFORMATICA DITRIBUIDA Y REDES

e. existe una rutina de antigüedad para mejorar el estado de explotación o transmisión de baja prioridad en función del tiempo en que la tarea ha estado en la cola.

3. Revisar los registros generados por cualquier mecanismo de nivelado de cargas que exista en la red de informática distribuida de la organización para determinar si:

a. la capacidad de la instalación central del Departamento de Informática puede ser asignada dinámicamente y controlada respecto a demandas concurrentes conflictivas

b. existen medidas para aplicar cualquier nivelado de instalaciones de explotación de cargas requerido, tales como transferir datos al procesador o transferir el procesador a los datos.

4. **Verificar** que en la red de informática distribuida de la organización existen mecanismos que controlan los tiempos de respuesta de la red y el número y duración de sus fallos de operación.

5. **Verificar** que todos los procesadores de red en la red de informática distribuida de la organización son controlados regularmente para determinar el nivel y eficacia de sus actividades de proceso. **Determinar** si se emiten regularmente informes generales de funcionamiento de la red, cubriendo aspectos tales como disponibilidad de la misma, cumplimiento de calendarios, tiempos de respuesta, eficiencias de las diversas instalaciones de explotación y problemas de funcionamiento.

6. **Determinar** que los departamentos que utilizan la red de informática distribuida de la organización presentan regularmente informes de funcionamiento al Departamento de Informática, para su análisis y consolidación y que se distribuyen copias de los informes de funcionamiento consolidados a los directivos de los departamentos usuarios.

2.20 PLANES DE CONTINGENCIA DE EXPLOTACIÓN DE LA RED

• **Objetivo de Control.**

El Departamento de Informática debiera establecer procedimientos que provean a la oportuna restauración de la red de informática distribuida de la organización una vez que haya tenido lugar una interrupción de sus operaciones o un desastre.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos establecidos por el Departamento de Informática para proveer a la oportuna restauración de la red de informática distribuida de la organización cuando tiene lugar una interrupción en su explotación o un desastre.

1. **Determinar** que el Departamento de Informática ha emitido declaraciones escritas de procedimientos relativos a la restauración de la informática distribuida de la organización una vez que ha tenido lugar una interrupción de su explotación o un desastre. **Cerciorarse** de que dichas declaraciones están actualizadas y **verificar** que, cuando menos, prescriben:

a. las condiciones bajo las que tales procedimientos deben aplicarse

b. la persona o personas, indicando su nombre, función o cargo que será responsable de ejecutar partes específicas de los procedimientos

c. los nombres y números de teléfono de programadores, operadores y personal de soporte de la red a quienes hay que identificar y la aplicación de los procedimientos

d. la situación de y los procedimientos para acceder al equipo a ser empleado durante el procedimientos de restauración de la red

e. las fuentes de los suministros necesarios para la restauración

f. los procedimientos para notificar a los directivos de los departamentos usuarios de la red que se están ejecutando los procedimientos de recuperación de desastres.

4. **Verificar** que los procedimientos para restauración de la red de informática distribuida de la organización se aprueban periódicamente y que se aplican las medidas de seguridad exigidas en el local o instalación que será utilizado durante el período de restauración de la explotación.

PARTE II: CONTROLES ESPECÍFICOS DE CIERTAS TECNOLOGÍAS

CONTROLES SOBRE EL INTERCAMBIO ELECTRÓNICO DE DATOS

CONTENIDO

3 CONTROLES SOBRE EL INTERCAMBIO ELECTRÓNICO DE DATOS	II-3-1
3.1 OBJETIVOS DE GESTIÓN	II-3-1
3.2 ANÁLISIS COSTE-BENEFICIO	II-3-1
3.3 SELECCIÓN DE SUMINISTRADORES DE SERVICIOS	II-3-2
3.4 TÉRMINOS CONTRACTUALES	II-3-2
3.5 IDENTIFICACIÓN Y VERIFICACIÓN DE USUARIOS	II-3-4
3.6 CONTROLES DE PROTECCIÓN DE PROGRAMAS	II-3-5
3.7 CONTROLES SOBRE EL LOGICAL DE APLICACIÓN	II-3-5
3.8 MANUAL DE USUARIO	II-3-6
3.9 FACTURAS POR EL SERVICIO	II-4-1

* * *

PARTE II - 3. CONTROLES SOBRE EL INTERCAMBIO ELECTRONICO DE DATOS

1 CONTROLES SOBRE EL INTERCAMBIO ELECTRÓNICO DE DATOS

La dirección debiera asegurar que la dependencia de la organización respecto del uso compartido de tecnología de la información mantenida en parte, o en su totalidad, por otra organización, se controla, gestiona y evalúa cuidadosamente.

La dirección debería también asegurar que la utilización por la organización de intercambio electrónico de datos e basa en consideraciones de coste-beneficio y demuestra un nivel satisfactorio coherente de seguridad y control.

En los acuerdos entre los socios comerciales de un intercambio electrónico de datos deberían incluirse prácticas específicas de Auditoría Informática y de control. Entre los temas que deberían contemplarse figuran el no rechazo de las actividades de los socios comerciales, la necesidad de registros de transmisión, el uso de firmas electrónicas como acuse de recibo de textos legales, la cifra (criptografía) y descifrado de texto, el mantenimiento de la integridad de las bases de datos compartidas y el archivo de los registros de transmisión.

3.1 OBJETIVOS DE GESTIÓN

- **Objetivo de Control.**

La alta dirección de la organización debiera emitir una declaración escrita de los objetivos y beneficios a alcanzar por la participación de la organización en relaciones de intercambio electrónico de datos, con proveedores y clientes adecuados.

- **Directiva de Auditoría.**

Debe examinarse la declaración escrita por la alta dirección de la organización de los objetivos y beneficios a alcanzar por la participación de la organización en relaciones de intercambio electrónico de datos, con proveedores y clientes adecuados.

1. **Verificar**, mediante entrevistas y una revisión de las declaraciones escritas emitidas por la alta dirección, que los objetivos y beneficios establecidos para la participación de la organización en relaciones comerciales de intercambio electrónico de datos son alcanzables y razonables.

2. **Determinar** que la dirección de los departamentos legales, de seguros, y de riesgos de la organización y los departamentos usuarios afectados por este acuerdo de participación han desempeñado un papel significativo en el establecimiento de dichos objetivos y en su realización.

3. **Determinar** que la alta dirección de la organización entiende los aspectos de teoría y control asociados con la participación e intercambio electrónico de datos y que reconoce el papel que los costes juegan en la relación satisfactoria de dichos aspectos.

3.2 ANÁLISIS COSTE-BENEFICIO

- **Objetivo de Control.**

La alta dirección de la organización debiera exigir que se efectúen periódicamente análisis coste-beneficio de su participación en diversas relaciones comerciales del intercambio electrónico de datos.

- **Directiva de Auditoría.**

Deben realizarse los análisis coste-beneficio de la participación de la organización en diversas relaciones comerciales de intercambio electrónico de datos.

1. **Verificar** que se llevan a cabo periódicamente análisis coste-beneficio adecuados de las diversas relaciones comerciales de intercambio electrónico de datos de la organización y apreciar lo razonable de las conclusiones extraídas de tales análisis.

3.3 SELECCIÓN DE SUMINISTRADORES DE SERVICIOS

• **Objetivo de Control.**

La alta dirección debiera establecer criterios basados en funcionamiento y en costes para mantener las relaciones de la organización con un suministrador de servicios de intercambio electrónico de datos.

• **Directiva de Auditoría.**

Deben revisarse los criterios establecidos por la alta dirección para mantener la relación de la organización con un suministrador de servicios de intercambio electrónico de datos.

1. **Verificar** que la alta dirección ha establecido criterios razonables, basados en funcionamiento y costes, para el mantenimiento de las relaciones de la organización con suministradores de servicios de intercambio electrónico de datos.

3.4 TÉRMINOS CONTRACTUALES

• **Objetivo de Control.**

La alta dirección debiera establecer, mediante acuerdos o contratos escritos, los términos y condiciones para el establecimiento y mantenimiento de relaciones con socios comerciales y suministradores de servicios de intercambio electrónico de datos.

• **Directiva de Auditoría.**

Deben revisarse los términos y condiciones de los contratos o acuerdos escritos con los socios comerciales o suministradores de servicios de intercambio electrónico de datos establecidos por la alta dirección de la organización.

1. **Determinar**, a partir de una revisión de los contratos y acuerdos escritos que han sido establecidos por la alta dirección de la organización por los socios comerciales o suministradores de servicios de intercambio electrónico de datos cuán razonable y adecuados son sus términos y condiciones.

2. **Verificar** para los acuerdos establecidos por la alta dirección de la organización con sus socios comerciales de intercambio electrónico de datos que:

a. el socio comercial ha acordado cumplir con los formatos y mensajes de transacción y los procedimientos de verificación y autenticación establecidas por la asociación Industrial de la organización de establecimiento de estándares pertinente

b. se han contemplado los aspectos legales relacionados por (1) el significado de 'escribir', la función desempeñada por las firmas electrónicas, y (2) el no-rechazo de mensajes electrónicos y otros aspectos del tratamiento de mensajes, en concreto los relativos a cantidades, precio o coste, y calidad de lo productos

c. Se han establecido controles que afectan a (1) la transmisión de datos en binario, tales como la de gráficos, (2) a los pedidos pendientes de servirse o a productos sustituidos, (3) el almacenamiento provisional de los productos, generalmente en un almacén o entorno de productos semi-elaborados y (4) un interfaz con el inventario justo a tiempo o aplicaciones de fabricación informatizada en las que los datos son modificables

d. La responsabilidad de los impuestos sobre el valor añadido y otros generados a partir de las transacciones surgidas desde el acuerdo ha sido definida y acordados.

3. **Verificar**, para los contratos que la alta dirección de la organización ha establecido con sus suministradores de intercambio electrónico de datos que:

a. el contrato distingue entre y define adecuadamente las relaciones y las obligaciones, incluyendo (1) una cobertura de seguro de responsabilidad frente a terceros y una fianza de fidelidad, (2) las responsabilidades del suministrador de los servicios sus agentes y subcontratistas y (3) las responsabilidades de la organización

b. se han determinado la frecuencia de los cambios en el logical utilizado para el tratamiento de dichas transacciones y la distribución de los costes de tales cambios

c. se han resuelto los aspectos con la propiedad y confidencialidad de los datos y los medios utilizados para evitar tanto que dichos datos se revelen por los empleados por el suministrador de servicio, sus administradores, o subcontratistas como la escucha no autorizada de los datos durante su transmisión

d. se han provisto los medios para la identificación de los usuarios del sistema, para la evaluación y resolución de anomalías en los registros y en el flujo de registros de transacciones de datos a fin de ayudar a corregir discrepancias de proceso, evitar resultados espurios y detectar actividades fraudulentas

e. se ha limitado efectivamente el desvelado por el suministrador de servicio a tercero de los nombres, números de teléfono, cargos y otra información sobre aquellos empleados de información que participan en el intercambio electrónico de datos

f. el contrato establece que el suministrador de servicio brindará capacidades de explotación alternativas para permitir la rápida restauración del proceso de intercambio electrónico de datos una vez acaecido un desastre.

4. **Determinar**, mediante entrevistas con usuarios seleccionados y una revisión de las determinaciones del contrato establecido con los suministradores del servicio electrónico de datos:

a. se registran informáticamente las transacciones completas y se retienen copias de archivo de dichos registros por un número específico de años, y que están disponibles a efectos de revisión, auditoría o respaldo, a un

coste razonable y en un plazo razonable

b. están definidos los cargos por acceso a la red, transmisión de transacciones, y actividades similares de utilización del sistema y éstos se reconcilian rutinariamente con los volúmenes de transacción

c. los usuarios del sistema pueden interrogarle en tiempo real para determinar el estado actual de una transacción en concreto

d. se han definido el fuero, la legislación, y las prácticas empresariales que rigen en el supuesto de que surja una desavenencia

e. se manejan con eficacia los procesos de cifra, descifrado y gestión de claves

f. el logical de traducción para convertir formatos de ficheros se mantiene a largo plazo.

5. **Determinar**, mediante entrevistas, con usuarios seleccionados y a partir de una revisión de las determinaciones en el contrato con los suministradores de servicios de intercambio electrónico de datos que los siguientes criterios operativos de funcionamiento y sus correspondientes penalizaciones económicas han sido definidos y se ejecutan.

a. controles adecuados sobre la seguridad de acceso a la red y sobre los datos para cuyo proceso se utiliza la red

b. una tasa aceptable de errores de proceso

c. una adecuada disponibilidad de la red definida en términos del tiempo que está disponible y en términos de respuesta, efectuándose ajustes a la facturación para reflejar cualquier interrupción o degradación del servicio

PARTE II - 3. CONTROLES SOBRE EL INTERCAMBIO ELECTRONICO DE DATOS

d. la adecuada corrección y borrado de registros del fichero maestro, registros de transacción y ficheros de datos

e. una eficaz compatibilidad para el almacenamiento y remisión ('store and forward') de mensajes, incluyendo el uso opcional de controles de integridad a nivel de mensaje - tales como códigos de autenticación o totales lógicos cifrados - para desanimar las suplantación por individuos que logren acceso no autorizado al sistema

f. transmisión de mensajes numerados por el sistema de forma coherente, para evitar errores en el reconocimiento o recepción de mensajes y el problema de repetición de mensajes cuando han tenido lugar o errores o los mensajes han sido alterados o mutilados y deben ser retransmitidos

g. el mantenimiento actualizado de un plan adecuado de recuperación de desastres cuyo coste está incluido en la tarifa básica de servicio del suministrador.

h. la inspección rutinario del contenido de las transmisiones para identificar la posible presencia de virus informáticos y problemas similares con el código o con los datos

i. la transmisión automática a los usuarios del sistema de los registros de transacciones procesadas sin éxito a fin de facilitar la resolución a tiempo de los defectos y la retransmisión de los registros

j. una adecuada vigilancia de cualesquiera empleados del suministrador de servicio, de sus agentes o sus subcontratistas que actúa como un solucionador de problemas y ha sido autorizado con privilegios de sobreseimiento (esta vigilancia debiera asegurar que los registros de las actividades de esta persona se revisen a diario por un representante de la organización y que todos los problemas identificados se resuelven de forma razonable)

k. la recopilación autorizada de datos económicos y de mercado por el suministrador del servicio de forma coherente e imparcial a partir de los registros de transacciones generados a través del acuerdo comercial de intercambio electrónico de datos.

6. **Verificar**, para los contratos con suministradores de intercambio electrónico de datos, que se lleven a cabo auditorías periódicas por terceros independientes de las operaciones del suministrador. Apremiar la frecuencia, ámbito, actualidad, oportunidad y adecuación de dichas revisiones.

3.5 IDENTIFICACIÓN Y VERIFICACIÓN DE USUARIOS

* **Objetivo de Control.**

La alta dirección de la organización debiera establecer controles adecuados sobre el uso del sistema del intercambio electrónico de datos.

* **Directiva de Auditoría.**

Debe revisarse la adecuación de los controles sobre el uso del intercambio electrónico de datos establecidos por la alta dirección de la organización.

1. **Verificar**, a partir de una revisión de la documentación, de procedimientos pertinentes y de una observación del uso del sistema electrónico de datos, que los controles que la alta dirección de la organización ha establecido sobre dicho uso:

a. delimitan la habilidad de los usuarios para iniciar actividades específicas sensibles -- incluyendo la segregación entre la iniciación y transacciones de alto volumen y alto riesgo

b. Exigen autorización humana o mediación en los casos en que las transacciones se inician como respuesta a un evento del sistema, tal como un cambio en los proveedores o la recepción de un lote de productos específico

c. utilizan palabras de paso y mecanismos de identificación comparables, como parte del procedimiento de apertura ('sign on') del sistema

d. brindan un mecanismo para devolver la llamada para identificar la autenticidad de la instalación del usuario ante el sistema y el socio comercial ante el usuario

e. asegurar que un número predeterminado de fallos consecutivos en la apertura desconectarán la instalación del usuario del sistema y exigirán una aprobación verificada por el supervisor antes de poder volver a establecer la conexión.

3.6 CONTROLES DE PROTECCIÓN DE PROGRAMAS

• **Objetivo de Control.**

La alta dirección de la organización debiera establecer controles adecuados sobre el uso del sistema de intercambio electrónico de datos.

• **Directiva de Auditoría.**

Debe revisarse la adecuación de los controles sobre el uso del intercambio de datos establecidos por la alta dirección de la organización.

1. **Verificar**, a partir de una revisión de la documentación de procedimientos pertinente y observación del uso del sistema de intercambio electrónico de datos, que los controles establecidos por la alta dirección sobre dicho uso.

a. registran las instrucciones de llamada a programas generada durante la rutina de apertura

b. establecen que tales instrucciones de llamada programas se revisen periódicamente para determinar la hora, fecha, iniciador, y propósito de dicha actividad.

2. **Determinar** que los procedimientos requieren la comparación programa de

los cambios hechos con los registros que autorizan tales cambios para permitir, poner de manifiesto y resolver cualquier cambio no autorizado.

3.7 CONTROLES SOBRE EL LOGICAL DE APLICACIÓN

• **Objetivo de Control.**

La alta dirección de la organización debiera establecer controles adecuados sobre los procesos de entrada y salida y el logical de aplicación utilizado en el sistema de intercambio electrónico de datos.

• **Directiva de Auditoría.**

Debe revisarse la adecuación de los controles sobre los procesos de entrada y salidas y el logical de aplicación utilizado en el sistema de intercambio de datos, establecidos, por la alta dirección de la organización.

1. **Verificar**, a partir de una revisión estructurada de la documentación de procedimientos pertinente y de la observación del uso del sistema de intercambio electrónico de datos, que los controles establecidos por la alta dirección sobre las transacciones de entrada y salida del sistema y el mantenimiento de los ficheros maestros aseguran que las mismas están autorizados, y son completas, precisas, seguras y están sometidas a procedimientos de corrección de errores.

2. **Determinar** que la identidad del emisor y receptor de los mensajes son validados por el sistema.

3. **Determinar** que la topología del sistema enlaza los ficheros de datos y las corrientes de datos de los socios comerciales y del suministrador del servicio.

4. **Determinar** que la integridad de los mecanismos de formateo de la aplicación, los protocolos de comunicaciones y otras funciones del sistema están asegurada.

5. **Determinar** que funcionan los diagramas de encaminamiento o bifurcación

PARTE II - 3. CONTROLES SOBRE EL INTERCAMBIO ELECTRONICO DE DATOS

("branching") de mensajes que han sido aprobados entre los socios comerciales.

3.8 MANUAL DE USUARIO

- **Objetivo de Control.**

La alta dirección de la organización debiera de producir una declaración escrita o un manual que estableciese los procedimientos autorizados para el uso del sistema de intercambio electrónico de datos

- **Directiva de Auditoría.**

Debe revisarse la declaraciones escritas producida por la alta dirección de la organización que establece los procedimientos autorizados para el uso del sistema de intercambio electrónico de datos.

1. **Determinar**, a partir de una revisión de la declaraciones escritas o del manual que establece los procedimientos autorizados para el uso del sistema de intercambio electrónico de datos, que éste define los procedimientos a ser seguidos para hacer cosas tales como:

- a. obtener acceso al sistema
- b. iniciar y terminar transacciones
- c. resolver errores en la transmisión y recepción de mensajes.
- d. responder a la degradación o interrupción de las operaciones del sistema

3.9 FACTURAS POR EL SERVICIO

- **Objetivo de Control.**

La alta dirección de la organización debiera asegurar que las facturas emitidas por el suministrador del servicio de intercambio electrónico de datos son conformes con las provisiones del contrato y se reconcilian con los registro de la organización de uso del sistema de la organización, y que no dan lugar a pagos innecesarios.

- **Directiva de Auditoría.**

Deben revisarse los procedimientos establecidos por la alta dirección de la organización para asegurar que las facturas emitidas por el suministrador del servicio de intercambio electrónico de datos son conformes con las provisiones del contrato y se reconcilian con los registros de uso del sistema de la organización, y que no dan lugar a pagos innecesarios.

1. **Determinar**, a partir de una revisión de facturas seleccionadas emitidas por el suministrados deservicio de intercambio electrónico de datos a la organización que:

- a. son conformes con las provisiones del contrato de la organización con el suministrador
- b. se comparan con los registros del uso del servicio por la organización
- c. no se están efectuando pagos innecesarios.

2. **Determinar** que la organización está siendo adecuadamente compensada por el suministrador por cualquier degradación o interrupción en la calidad del servicio suministrado.

PARTE II: CONTROLES ESPECÍFICOS DE CIERTAS TECNOLOGÍAS

CONTENIDO

4	CONTROLES EN LAS OPERACIONES EN LAS OFICINAS DE SERVICIOS	II-4-1
4.1	EL CONTRATO CON LA OFICINA DE SERVICIOS	II-4-1
4.2	MANUALES DE USUARIO	II-4-1
4.3	REVISIÓN POR TERCEROS	II-4-1
4.4	ESTABILIDAD FINANCIERA DE LA OFICINA DE SERVICIOS	II-4-2
4.5	EL PLAN DE RECUPERACIÓN DE DESASTRES INFORMÁTICOS DE LOS USUARIOS	II-4-2

* * *

PARTE II - 4. CONTROLES DE EXPLOTACION EN OFICINAS DE SERVICIOS.

4 CONTROLES EN LAS OPERACIONES EN LAS OFICINAS DE SERVICIOS

Un usuario de una oficina de servicios informáticos debiera ser capaz de obtener garantías razonables de que los controles aportados por dicha organización son adecuados.

4.1 EL CONTRATO CON LA OFICINA DE SERVICIOS

- **Objetivo de Control.**

Debiera cumplimentarse un contrato detallando los derechos y obligaciones del proveedor del servicio.

- **Directiva de Auditoría.**

Debe obtenerse y examinarse el contrato entre el proveedor del servicio y el usuario.

1. **Revisar** el contrato para determinar si están definidos los costes de diseño del sistema, de programación, de tiempo de ordenador, de informes periódicamente, de informes especiales y de otros materiales.

2. **Revisar** el contrato para asegurar que están definidas las responsabilidades del usuario en cosas tales como la preparación de lotes de entrada, la entrada de datos, y el cuadro.

3. **Revisar** la responsabilidad de la oficina de servicios en cosas tales como la revisión de la precisión de las salidas del proceso, la resolución de problemas identificados, y el re-proceso.

4. **Asegurar** que están estipulados la duración del contrato y las condiciones para su terminación

5. **Verificar** que el contrato exige a la oficina de servicios que proporcione anualmente una revisión por un tercero de sus procedimientos de control.

6. **Determinar** si el contrato permite a los auditores internos y externos del usuario llevar a cabo una auditoría de las operaciones de la oficina de servicios, si fuera necesario.

7. **Determinar** si el contrato establece una protección ante el desvelado o pérdida de los datos de los usuarios cuando están bajo control de la oficina de servicios.

8. **Determinar** si el contrato exige a la oficina de servicios a la presentación de sus cuentas anuales auditadas.

4.2 MANUALES DE USUARIO

- **Objetivo de Control.**

En la oficina de servicios debiera proporcionar manuales de usuarios y otra documentación de conversión. Dicha documentación debiera describir con precisión y de forma completa las acciones que los usuarios deben ejecutar.

- **Directiva de Auditoría.**

Deben revisarse los manuales de usuario y otra documentación de la oficina de servicios.

1. **Revisar** el manual de usuario de la oficina de servicios para hacerse una idea general de la entradas, salidas y procesos de la aplicación.

2. **Determinar** si se ha llevado a cabo programación adicional a la medida, por la oficina de servicios. Obtener copias de los manuales de usuario que describen este logical a medida.

3. **Verificar** si los manuales son exactos y completos mediante una indagación y observación del sistema en uso.

4.3 REVISIÓN POR TERCEROS

- **Objetivo de Control.**

Una entidad independiente debiera completar un informe de revisión por terceros de las operaciones pertinentes de la oficina de servicios, describiendo los puntos fuertes y débiles de control. Debiera ser efectuada anualmente.

PARTE II - 4. CONTROLES DE EXPLOTACION EN OFICINAS DE SERVICIOS.

• Directiva de Auditoría.

Debe obtenerse y revisarse una copia del informe de la última revisión por terceros de las operaciones pertinentes de la oficina de servicios. Si no estuviera disponible un informe así, debiera considerarse la expansión de la cobertura actual de la Auditoría Informática para incluir una revisión de las operaciones pertinentes de la oficina de servicios.

1. **Determinar** si el informe de revisión por terceros describe los puntos fuertes y débiles de control de las operaciones pertinentes de la oficina de servicios.

2. **Verificar** que durante la revisión por terceros cubierta por el informe se consideraron las disposiciones aplicables de esta publicación de *Objetivos de Control*.

3. **Determinar** qué controles son responsabilidad del usuario. **Verificar** que el usuario ha implantado tales controles de forma adecuada.

4. **Determinar** si la oficina de servicios ha sido objeto de una Auditoría Informática. **Revisar** la extensión del trabajo de auditoría llevado a cabo y las cualificaciones profesionales de los auditores que lo efectuaron.

4.4 ESTABILIDAD FINANCIERA DE LA OFICINA DE SERVICIOS

• Objetivo de Control.

La oficina de servicios debiera ser solvente desde un punto de vista financiero.

• Directiva de Auditoría.

Deben revisarse las cuentas anuales auditadas de la oficina de servicios.

1. **Obtener** y **revisar** las cuentas anuales de la oficina de servicios.

2. **Determinar** si la oficina de servicios goza de estabilidad financiera.

4.5 EL PLAN DE RECUPERACIÓN DE DESASTRES INFORMÁTICOS DE LOS USUARIOS

• Objetivo de Control.

El usuario debiera preparar un plan de recuperación de desastres informáticos que contemplara la posible pérdida temporal o permanente de capacidades de proceso de datos por la oficina de servicios.

• Directiva de Auditoría.

Debe obtenerse y revisarse el plan de recuperación de desastres informáticos preparado por el usuario.

1. **Obtener** una copia del plan de recuperación de desastres informáticos y **determinar** si las aplicaciones críticas tratadas por la oficina de servicios pueden ser restauradas antes de que las actividades del usuario sufran un impacto negativo.

2. **Determinar** si el plan de recuperación de desastres informáticos del usuario es probado y actualizado periódicamente.

3. **Determinar** si la utilización de oficina de servicios alternativas o de otras alternativas de tratamiento de datos han sido consideradas durante el proceso de establecimiento del plan de recuperación de desastres informáticos.

PARTE II - 5. CONTROLES SOBRE ORDENADORES PERSONALES.

PARTE II: CONTROLES ESPECÍFICOS DE CIERTAS TECNOLOGÍAS

CONTROLES SOBRE ORDENADORES PERSONALES

CONTENIDO

5 CONTROLES SOBRE ORDENADORES PERSONALES.	II-5-1
5.1 POLÍTICAS DE DIRECCIÓN.	II-5-1
5.2 CRITERIOS de ADQUISICIÓN DE ORDENADORES PERSONALES	II-5-2
5.3 DESARROLLO Y ADQUISICIÓN DE LOGICAL DE APLICACIÓN	II-5-3
5.4 DOCUMENTACIÓN DE LOS PROGRAMAS	II-5-4
5.5 BIBLIOTECA DE PROGRAMAS APLICACIÓN OBTENIDOS BAJO LICENCIA	II-5-5
5.6 FICHEROS DE DATOS	II-5-6
5.7 FICHEROS DE TRANSACCIONES	II-5-7
5.8 ACCESO A RECURSOS DE ORDENADORES PERSONALES.	II-5-7
5.9 DOCUMENTACIÓN DE LOS PROCESOS	II-5-8
5.10 CARACTERÍSTICAS DE CONTROL	II-5-8
5.11 TRANSMISIÓN DE DATOS CON ORDENADORES PERSONALES	II-5-8
5.12 RESPALDO Y SEGURIDAD DE PROGRAMAS Y DATOS	II-5-9
5.13 SEGURIDAD FÍSICA DE LOS EQUIPOS	II-5-9
5.14 OPERACIÓN DE LOS ORDENADORES PERSONALES	II-5-10
5.15 REVISIÓN POR LA DIRECCIÓN	II-5-11

* * *

PARTE II - 5. CONTROLES SOBRE ORDENADORES PERSONALES.

5 CONTROLES SOBRE ORDENADORES PERSONALES.

La adquisición, uso y seguridad de los ordenadores personales debiera ser planificada y controlada por la alta dirección de la organización y debiera basarse en consideraciones totalmente definidas de coste-beneficio. (El empleo de ordenadores personales en una organización establece un puente entre el proceso de datos convencional y el proceso de datos distribuido y presenta problemas de control de la informática de naturaleza singular. Los ordenadores personales, en general, son dispositivos aislados compuestos de un teclado o de otro dispositivo de entrada autocontenido, con algún tipo de memoria interna, una unidad central de proceso, un dispositivo de monitor de video y una impresora de salida. Normalmente los ordenadores personales son capaces de procesar cantidades significativas de datos por sí mismos y pueden utilizarse, en algunos casos, como terminales para comunicar con un ordenador central que posea capacidades de tratamiento de datos compatibles).

5.1 POLÍTICAS DE DIRECCIÓN.

* **Objetivo de Control.**

Los ordenadores personales y los datos para cuyo proceso se utilizan son activos cuya adquisición y utilización debieran ser objeto de atención y control por la alta dirección de la organización.

* **Directiva de Auditoría.**

La alta dirección de la organización debiera establecer políticas relativas a la adquisición y empleo de ordenadores personales. Dichas políticas debieran contemplar, cuando menos, el manejo de datos confidenciales, sensitivos e información protegida, así como la integridad, la exactitud, y lo completo de los datos procesados por los ordenadores personales.

Deben revisarse las políticas de la dirección relativas a la adquisición y empleo

de ordenadores personales en la organización.

1. **Determinar** si la alta dirección de la organización ha emitido declaraciones escritas de política relativas a la adquisición y empleo de ordenadores personales y que dichas declaraciones han sido comunicadas a la dirección de los departamentos usuarios.

2. **Determinar** si la alta dirección de la organización ha emitido declaraciones escritas de políticas que exigen que las aplicaciones de ordenadores personales se clasifiquen según el riesgo asociado a las mismas. Evaluar si la directiva relativas a la exigencia de clasificación por riesgos incluyen factores tales como:

a. el impacto de un fallo del sistema en la organización

b. la naturaleza y extensión de la dependencia de la dirección de la información producida por la aplicación

c. la confidencialidad de los datos dentro de la aplicación.

3. **Determinar** si la alta dirección de la organización ha emitido una declaración de política describiendo los tipos de controles que se exigen para las aplicaciones de ordenadores personales en las diversas categorías de riesgo. Evaluar si tales declaraciones de política exigen que las aplicaciones de ordenadores personales incorporen controles que son proporcionados a los riesgos asociados con ellos. **Evaluar** si dichas declaraciones de política incluyen determinaciones adecuadas para:

a. desarrollo y pruebas

b. documentación

c. controles de entradas, tratamientos y salidas

d. respaldo y recuperación de programas y datos

PARTE II - 5. CONTROLES SOBRE ORDENADORES PERSONALES.

e. la seguridad relativa a la custodia y empleo de los activos de ordenadores personales, incluyendo equipos, logical y datos.

4. **Determinar** si las declaraciones de política escritas para la adquisición de ordenadores personales emitidas por la alta dirección de la organización contemplan aspectos como:

a. la obtención de un inventario de material y logical de ordenador personal actualmente en uso por la organización

b. la clasificación de elementos del inventario en función de su valor crítico para la organización y de la confidencialidad de los datos exigida por la organización

c. desarrollo e implantación de un procedimiento para mantener actualizado el inventario de ordenadores personales de la organización

d. restricción de la utilización de ordenadores personales al logro de las metas y objetivos personales de la organización

e. prescripción del tipo de aplicaciones que se consideran adecuadas para ordenadores personales cuando estos se emplean de forma autónoma

f. prescripción de los tipos de aplicaciones que se consideran adecuadas para ordenadores personales cuando es necesario acceder a datos que son gestionados por explotación del Departamento de Informática de la organización

g. especificación del tipo de aprobación necesaria antes de que se permita dicho acceso.

5. **Evaluar** si se han diseñado formularios especiales u otra documentación para facilitar la propuesta de adquisición y la aprobación de las adquisiciones de ordenadores personales dentro de la organización.

5.2 CRITERIOS de ADQUISICIÓN DE ORDENADORES PERSONALES

• Objetivo de Control.

La alta dirección debiera establecer criterios de adquisición de ordenadores personales y pasar la aprobación de dichas adquisiciones en la exigencia de análisis de coste-beneficio.

• Directiva de Auditoría.

Deben revisarse los criterios de adquisición de ordenadores personales y los procedimientos de aprobación de las adquisiciones relacionados que haya establecido la alta dirección.

1. **Determinar** si la alta dirección ha comunicado criterios por escrito para la adquisición de ordenadores personales y ha proporcionado formularios u otra documentación para facilitar el proceso de aprobación de adquisiciones.

2. **Determinar** si las solicitudes de adquisición de ordenadores personales, exigidas por la alta dirección se basan, de forma rutinaria, en análisis coste-beneficio que incluyen la consideración de aspectos tales como:

a. cómo se determinaron las necesidades a satisfacer por el ordenadores personales

b. por qué dichas necesidades no podían ser satisfechas por recursos informáticos ya disponibles, tales como los proporcionados por explotación del Departamento de Informática

c. las especificaciones del sistema que han sido cumplidas

d. que se ha completado una revisión de equipos alternativos

e. que se han considerado los factores significativos de coste-beneficio.

3. **Establecer** si los procedimientos de la organización para solicitar la adquisición de ordenadores personales exigen que, cuando en la petición se ha mencionado una marca específica de ordenado-

res, quien prepara la solicitud ha de responder a las siguientes preguntas:

a. ¿son compatibles los ordenadores personales producidos por dicha compañía por otro material y logical informáticos actualmente en uso en la organización?

b. ¿produce la compañía logical de aplicación adecuado para su empleo con sus ordenadores personales?

c. ¿puede obtenerse mantenimiento adecuado para los ordenadores personales mencionados en la solicitud?

4. **Determinar** si existe una declaración escrita de política que trate de la adquisición de ordenadores personales a través del departamento de compras de la organización, de modo tal que las compras se beneficien de descuentos por volumen o de otros beneficios en función del número.

5.3 DESARROLLO Y ADQUISICIÓN DE LOGICAL DE APLICACIÓN

• **Objetivo de Control.**

La alta dirección debiera emitir una declaración escrita de política estableciendo directivas para el desarrollo o adquisición de logical de aplicación para ordenadores personales.

• **Directiva de Auditoría.**

Deben revisarse las directivas para el desarrollo o adquisición del logical de aplicación para ordenadores personales establecidas por la alta dirección.

1. **Determinar** si los procedimientos para desarrollar o adquirir logical de aplicación son conformes con la metodología de ciclo de vida del desarrollo de sistemas.

2. **Determinar** si la alta dirección ha emitido una declaración escrita de política que brinde directivas sobre las alternativas de desarrollar o comprar en el caso del logical de aplicación de

ordenadores, y que dicha declaración cubre por lo menos:

a. los estándares de análisis y documentación y de cumplimiento de la política

b. los requisitos legales a cumplir y la propiedad del código de los programas

c. el mantenimiento del material y logical

d. la documentación de las aplicaciones

3. **Determinar** si la alta dirección ha emitido una declaración escrita de política relativa a la adquisición de logical de aplicación a través del departamento de compras de la organización de modo que tales adquisiciones se beneficien de descuentos por volumen, contratos de licencia para una toda una oficina o de otros beneficios derivados de la compra en gran volumen.

4. **Establecer** si los procedimientos de adquisición de logical de aplicación para ordenadores personales de la organización exigen que, siempre que se haya mencionado el nombre específico en la solicitud de compra, quien prepara la orden de compra deba responder a las preguntas siguientes:

a. ¿es el paquete de logical compatible con otro logical de ordenadores personales y con los equipos usados por la organización?

b. ¿contiene el paquete de logical una declaración en cuanto a la integridad de los datos por la cual el vendedor del logical asume la responsabilidad de los errores del logical o de los daños que el logical pudiera ocasionar a otros sistemas?

c. ¿se tienen en vigor procedimientos para asegurar que el paquete de logical que se está adquiriendo es una copia legítima del logical y está libre

PARTE II - 5. CONTROLES SOBRE ORDENADORES PERSONALES.

de código de programas incluidos sin autorización?

5. **Determinar** si la alta dirección ha designado a miembros específicos de la plantilla para que desarrollen logical de aplicación para ordenadores personales y evalúen los programas de aplicación de ordenadores personales ofrecidos por los vendedores.

6. **Apreciar** el grado de implicación de la dirección de los departamentos usuarios en la determinación de si la organización debiera desarrollar logical de aplicación para ordenadores personales, o comprarlo.

7. **Determinar** si antes de que en la organización se decida si el logical de aplicación para ordenadores personales debe ser desarrollado o comprado se lleva a cabo un análisis coste-beneficio.

8. **Determinar** si las directivas de la organización para el desarrollo del logical de aplicación de ordenadores personales bajo contrato establecen:

a. una revisión y aprobación por la alta dirección de la solicitud de tales servicios

b. una seguridad de que el contratista satisface los estándares utilizados por el Departamento de Informática de la organización en cuanto a convenciones para nombrar ficheros de datos, documentación de programas y procedimientos de prueba

c. la determinación de que los servicios a prestar a —y el producto a entregar a— la organización por el contratista están claramente definidos y se llevan realmente a cabo

d. el asegurarse de que las cantidades pagadas al contratista están de acuerdo con la provisiones de su contrato con la organización y reflejan el trabajo realmente efectuado.

9. **Determinar** si se han establecido procedimientos para permitir que la dirección de los departamentos usuarios a-

pruebe y acepte el logical de aplicación para ordenadores personales desarrollado por el Departamento de Informática de la organización.

10. **Determinar** si se exige a los departamentos usuarios que aporten la documentación de los programas para su aprobación por la alta dirección antes de utilizar logical de aplicación para ordenadores personales que ha sido desarrollado por dicho departamento.

11. **Determinar** si la aprobación y aceptación requeridas por la dirección de los departamentos usuarios se ha recabado en casos en que personal del Departamento de Informática de la organización ha modificado paquetes de logical de aplicación para ordenadores personales.

12. **Determinar** si se ha recabado aceptación de la alta dirección antes de que paquetes de logical de aplicación para ordenadores personales sean modificados por los departamentos usuarios.

5.4 DOCUMENTACIÓN DE LOS PROGRAMAS

• **Objetivo de Control.**

La alta dirección debería establecer procedimientos para catalogar sus programas de aplicación para ordenadores personales y asegurar que se crean listas de tales programas y se mantienen actualizadas.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos de la organización para catalogar y preparar listas de sus programas de aplicación para ordenadores personales.

1. **Determinar** si la alta dirección ha designado a personas específicas de la plantilla para que cataloguen todos los programas de aplicación para ordenadores personales y para que reciban las listas de programas correspondientes.

2. **Apreciar**, cuando se usan programas de aplicación para ordenadores perso-

nales en aplicaciones informáticas que tienen acceso a datos gestionados por explotación del Departamento de Informática de la organización, si:

- a. la documentación del programa está actualizada
- b. dicha documentación se conserva a seguro en sitios no accesibles a los departamentos usuarios
- c. el logical de aplicación para ordenadores personales de uso frecuente está protegido respecto de modificaciones no detectadas
- d. los principales programas de aplicación para ordenadores personales están sujetos a controles formales de desarrollo.

3. **Determinar** si la documentación de programas de aplicación para ordenadores personales mantenida por la organización incluye:

- a. el nombre de la operación y la fecha de creación
- b. el autor o usuario del programa
- c. el nombre del programa
- d. la localización del programa
- e. el nombre del fichero de datos
- f. la localización del fichero de datos
- g. la estructura del fichero de datos
- h. la descripción de la operación
- i. la fecha de la documentación
- j. un listado del programa
- k. un flujograma

5.5 BIBLIOTECA DE PROGRAMAS APLICACIÓN OBTENIDOS BAJO LICENCIA

• **Objetivo de Control.**

En los casos en que se comparten, entre un número de usuarios diferentes, programas de aplicación para ordenadores personales, sujetos a un acuerdo de licencia con el creador del producto, debieran establecerse procedimientos por la alta dirección para registrar la actividad de los usuarios.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos establecidos por la alta dirección de la organización para registrar el uso de programas de aplicación para ordenadores personales compartidos, cuando éstos están bajo licencia.

1. **Determinar** si la alta dirección ha designado a un miembro específico de la plantilla para que actúe como bibliotecario de los programas de aplicación para ordenadores personales y para que registre la retirada y devolución de los programas específicos.

2. **Determinar** si se han establecido por la alta dirección procedimientos para asegurar que los programas de aplicación para ordenadores personales bajo licencia están protegidos contra copia o modificación.

3. **Determinar** si la alta dirección ha establecido procedimientos para asegurar el manejo y almacenamiento adecuados de los soportes magnéticos que contienen programas de aplicación para ordenadores personales bajo licencia.

4. **Determinar**, en el caso en que los programas de aplicación para ordenadores personales bajo licencia se utilizan para acceder a datos gestionados por explotación del Departamento de Informática de la organización, y cuando dichos programas de aplicación para ordenadores personales no estén protegidos contra copia o modificación, si:

PARTE II - 5. CONTROLES SOBRE ORDENADORES PERSONALES.

a. se han establecido procedimientos adecuados para identificar cualesquiera cambios que puedan haberse efectuado a un programa durante el período en que logical de aplicación ha retirado para su uso un usuario específico

b. el bibliotecario de programas de aplicación para ordenadores personales se cerciora de forma rutinaria de que el programa no ha sido modificado y que no ha sido copiado mientras era utilizado.

6. **Establecer** que, cuando se introducen cambios a programas de aplicación para ordenadores personales, dichos cambios han sido aprobados por todos los departamentos usuarios afectados de la organización, tanto antes como después de efectuar los cambios.

7. **Determinar** si se han establecido procedimientos en la organización para asegurar que no se conservan copias de programas de aplicación bajo licencia en los discos duros de los ordenadores personales equipados con los mismos.

5.6 FICHEROS DE DATOS

* **Objetivo de Control.**

Cuando se autoriza a ordenadores personales a acceder a datos que tiene explotación del Departamento de Informática o que han de ser empleados en aplicaciones autónomas, debieran establecerse por la alta dirección de la compañía procedimientos relativos a la creación y mantenimiento de ficheros de datos en dichos ordenadores personales.

* **Directiva de Auditoría.**

Deben revisarse los procedimientos de la organización para la creación y mantenimiento de ficheros de datos en ordenadores personales que, bien están autorizados a acceder a datos gestionados por el Departamento de Informática, bien han de ser utilizados en aplicaciones autónomas.

1. **Determinar** si se ha aprobado un formato de registro estándar para los ficheros de datos creados y utilizados en los ordenadores personales de la organización.

2. **Apreciar** si los procedimientos de conversión de datos utilizados en los ordenadores personales de la organización han sido documentados y son adecuados.

3. **Determinar** si en los ficheros de datos creados y utilizados en los ordenadores personales de la organización se han incorporado de forma rutinaria totales de control u otros controles programados.

4. **Apreciar** si los procedimientos de la organización para catalogar, almacenar y respaldar ficheros de datos de ordenadores personales por los departamentos usuarios son los adecuados.

5. **Determinar** si el Departamento de Informática utiliza controles tales como la fijación de una cadencia para regular la velocidad de transmisión de las transferencias de ficheros de datos de los ordenadores personales a explotación del Departamento de Informática para evitar sobrecargar las áreas de memoria asignadas a transmisión de datos (*buffers*) empleadas, lo que causaría una disminución de la velocidad de la red de comunicación de datos de la organización.

6. **Examinar** la frecuencia de vuelcos (copias de ficheros de explotación del Departamento de Informática a ordenadores personales seleccionados) y determinar la extensión de la redundancia de ficheros de datos y de la cantidad de proceso no directamente productivo creado por esta práctica. **Considerar** la viabilidad y el coste-eficacia del empleo por la organización de métodos alternativos de distribuir copias de ficheros de datos para ordenadores personales, como mediante un ordenador personal intermedio, una red de ordenadores personales o una transferencia de soportes magnéticos.

7. **Determinar** si los ficheros de datos sensibles o confidenciales creados y empleados por los ordenadores personales de la organización se cifran de forma rutinaria.

5.7 FICHEROS DE TRANSACCIONES

• **Objetivo de Control.**

Cuando los ordenadores personales están autorizados a acceder a datos gestionados en explotación del Departamento de Informática de la organización, o cuando han de usarse en tratamiento de aplicaciones autónomas, la alta dirección debiera establecer para dichos ordenadores personales procedimientos para iniciar, aprobar y verificar los datos de transacciones.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos establecidos para iniciar, aprobar y verificar datos de transacciones cuando hay ordenadores personales autorizados para acceder a datos gestionados por explotación del Departamento de Informática, o cuando han de usarse en tratamiento de aplicaciones autónomas.

1. **Determinar** si las transacciones se introducen empleando el ordenador personal como un terminal, que no se circunviene o se le busca las vueltas a los dispositivos de control que mantiene explotación del Departamento de Informática de la organización, tales como procedimientos de identificación de usuario y de palabras de paso.

2. **Determinar** que no se da responsabilidad para el desarrollo de programas de aplicación para ordenadores personales a aquellos individuos de los departamentos usuarios de la organización que inician transacciones mediante ordenadores personales.

3. **Evaluar** si las transacciones iniciadas a través de los ordenadores personales de la organización son adecuadamente documentadas y aprobadas.

4. **Determinar** si todas las transacciones creadas por los ordenadores personales de la organización quedan registradas e incluyen controles de totales, controles de totales lógicos, conteo de documentos o controles programados similares, y **evaluar** los procedimientos para establecer y comparar dichos totales.

5. **Determinar** si se retienen los registros de los totales de control creados por los ordenadores personales de la organización, a efectos de su posible seguimiento.

5.8 ACCESO A RECURSOS DE ORDENADORES PERSONALES.

• **Objetivo de Control.**

Cuando se autoriza a ordenadores personales a acceder a datos gestionados por explotación del Departamento de Informática de la organización, la alta dirección debiera establecer procedimientos para conseguir dicho acceso.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos establecidos por la alta dirección de la organización para permitir acceso desde ordenadores personales a datos gestionados por explotación de su Departamento de Informática.

1. **Determinar** si se requiere que la alta dirección apruebe a usuarios específicos u ordenadores personales específicos que solicitan acceso a datos almacenados en explotación del Departamento de Informática.

2. **Determinar** si para identificar a los usuarios autorizados de los ordenadores personales de la organización se utilizan códigos, palabras de paso u otros dispositivos o mecanismos y verificar que el acceso a los códigos o palabras de paso está restringido.

3. **Determinar** que está prohibido el uso de programas de comunicaciones que introducen la palabra de paso por el

PARTE II - 5. CONTROLES SOBRE ORDENADORES PERSONALES.

usuario de los ordenadores personales de la organización.

4. **Determinar** si para identificar el nivel de recursos a que está autorizado cada usuario autorizado de los ordenadores personales de la organización emplea códigos matrices u otros métodos.

5.9 DOCUMENTACIÓN DE LOS PROCESOS

• **Objetivo de Control.**

Cuando se autoriza a ordenadores personales para acceder a datos almacenados en explotación del Departamento de Informática o cuando los mismos han de usarse en aplicaciones autónomas, la alta dirección debiera establecer procedimientos para registrar la utilización de dichos ordenadores personales.

• **Directiva de Auditoría.**

Deben revisarse los registros de utilización de los ordenadores personales que tengan autorización para acceder a datos almacenados en explotación del Departamento de Informática o para ser empleados en aplicaciones autónomas.

1. **Determinar** que la organización registra la extensión, naturaleza y adecuación del uso de los ordenadores personales.

2. **Determinar** que se registran todas las transacciones procesadas por los ordenadores personales de la organización.

5.10 CARACTERÍSTICAS DE CONTROL

• **Objetivo de Control.**

La alta dirección de la organización debiera apreciar los riesgos asociados con el uso de ordenadores personales y analizar las consideraciones de coste-beneficio de los controles a emplear en esa utilización.

• **Directiva de Auditoría.**

Deben apreciarse los riesgos asociados con el uso de ordenadores personales

en la organización y las características de control utilizadas.

1. **Determinar** si los riesgos asociados con el empleo de ordenadores personales han sido evaluados mediante:

a. una clasificación de las aplicaciones de ordenadores personales por tipos: contabilidad, analíticas, tratamiento de textos y ofimática

b. una medida de la sensibilidad y vulnerabilidad de los datos usados en cada una de esas clasificaciones de aplicaciones.

2. **Determinar** si la organización ha llevado a cabo un análisis coste-beneficio de las características de control empleadas en sus aplicaciones sobre ordenadores personales.

3. **Apreciar** cuan razonables son las conclusiones alcanzadas por la alta dirección respecto a la evaluación de riesgos coste-beneficio del uso de ordenadores personales por la organización.

5.11 TRANSMISIÓN DE DATOS CON ORDENADORES PERSONALES

• **Objetivo de Control.**

La alta dirección de la organización debiera establecer procedimientos para controlar y registrar el movimiento de los registros de transacción y de los ficheros de datos entre sus ordenadores personales y los de otras organizaciones.

• **Directiva de Auditoría.**

Deben revisarse los procedimientos de la organización para controlar y registrar el movimiento de registros de transacción y de ficheros de datos entre sus ordenadores personales y los de otras organizaciones.

1. **Examinar** una selección de ficheros con protocolos de usuario para comunicaciones (script file) para **determinar** si son conformes con los procedimientos pertinentes de la organización.

2. **Determinar**, en aquellos casos en que algunos de los ordenadores personales

de la organización conectados a una red pública de comunicaciones se mantienen disponibles para recibir ficheros de datos de diversas procedencias, si dichas actividades se controlan adecuadamente mediante el uso de palabras de paso. **Verificar** que los ficheros de datos y los programas de aplicación almacenados en tales ordenadores personales no pueden ser modificados remotamente sin autorización adecuada y mediante cambios introducidos en los controles de transmisión de datos pertinentes.

5.12 RESPALDO Y SEGURIDAD DE PROGRAMAS Y DATOS

• **Objetivo de Control.**

La alta dirección de la organización debiera establecer directivas para el respaldo de programas de aplicación, ficheros de datos y la documentación asociada con ellos, de los programas de aplicación para ordenadores personales.

• **Directiva de Auditoría.**

Deben revisarse las directivas de la organización para el respaldo de sus programas de aplicación, ficheros de datos y la documentación relacionadas con ellos de sus ordenadores personales.

1. **Verificar** que la organización mantiene un inventario actualizado del contenido de todos los soportes magnéticos de todos los ordenadores personales de la organización.

2. **Determinar** si la alta dirección de la organización ha emitido directivas escritas adecuadas relativas al respaldo de sus programas de aplicación para ordenadores personales, ficheros de datos, y documentación asociada a los mismos.

3. **Apreciar** si la instalación usada para almacenar los programas de aplicación, ficheros de datos y documentación de

los ordenadores personales de la organización cumplen con los requisitos aplicables de protección contra el fuego.

4. **Determinar** que la organización conserva copias actualizadas de programas de aplicación para ordenadores personales ficheros de datos y su documentación adecuada en un emplazamiento remoto adecuado.

5. **Determinar** si los individuos que utilizan los ordenadores personales de la organización para procesar información crítica, protegida o sensible cierran de forma segura y de modo rutinario todos los diskettes pertinentes cuando se alejan del área en que está situado el ordenador personal.

6. **Determinar** que el plan de recuperación de desastres de la organización contempla el uso que esta hace de sus ordenadores personales.

7. **Verificar** que los programas o ficheros de datos confidenciales con información protegida o sensible empleados por los ordenadores personales de la organización están cifrados cuando se guardan en diskettes o discos fijos.

8. **Determinar** que los ficheros fuente, para los programas de aplicación para los ordenadores personales de la organización, están protegidos ante modificación no autorizada porque se mantienen en una versión protegida contra escritura.

9. **Evaluar** si el uso de los programas de aplicación y de utilidades del sistema para ordenadores personales de la organización se controla adecuadamente.

5.13 SEGURIDAD FÍSICA DE LOS EQUIPOS

• **Objetivo de Control.**

Debieran establecerse procedimientos adecuados para asegurar que los ordenadores personales de la organización no son objeto de robo o abuso.

PARTE II - 5. CONTROLES SOBRE ORDENADORES PERSONALES.

• Directiva de Auditoría.

Debe cerciorarse de la existencia de controles adecuados para prevenir el robo de o el vandalismo contra los ordenadores personales de la organización.

1. **Determinar** si las salas en que están situados los ordenadores personales de la organización se cierran con llave de forma rutinaria después de las horas rutinarias de trabajo y si los propios ordenadores personales están anclados a las mesas de dichas salas.
2. **Determinar** si los componentes de los ordenadores personales de la organización han sido marcados con un número de identificación único e indeleble para disuadir su robo.
3. **Determinar** que todos los números de identificación, números de serie y descripciones de equipos asociadas con los ordenadores personales de la organización están registrados y guardados en un sitio seguro.
4. **Determinar** que los ordenadores personales de la organización están protegidos de forma rutinaria con cubiertas contra el polvo cuando no están en uso.
5. **Determinar** que cada uno de los ordenadores personales de la organización está protegido contra sobre-intensidades eléctricas mediante un limitador adecuado y que los ordenadores personales críticos han sido dotados de un suministro no interrumpido de energía eléctrica.
6. **Verificar** que cerca de cada uno de los ordenadores personales de la organización está situado un extintor de incendios adecuado.
7. **Verificar** que existe un procedimiento adecuado de registro y firma para los ordenadores personales que se retiran de las oficinas de la organización.

5.14 OPERACIÓN DE LOS ORDENADORES PERSONALES

• Objetivo de Control.

La alta dirección debiera establecer procedimientos para la explotación regular de los ordenadores personales de la organización.

• Directiva de Auditoría.

Debe cerciorarse de la existencia de procedimientos para la explotación regular de los ordenadores personales de la organización.

1. **Determinar** si los individuos que manejan los ordenadores personales de la organización han recibido la formación adecuada.
2. **Verificar** que hay más de un individuo familiarizado con el manejo de cada una de las aplicaciones críticas o sensibles sobre los ordenadores personales de la organización.
3. **Determinar** que se llevan a cabo procedimientos básicos de mantenimiento de forma regular sobre todos los ordenadores personales de la organización.
4. **Verificar** que en los discos fijos de los ordenadores personales de la organización solo se conservan programas y ficheros de datos autorizados, que tales programas y ficheros de datos no pueden ser copiados o modificados sin autorización y que los ficheros de programas y datos no actualizados se retiran de forma rutinaria de dichos discos fijos.
5. **Determinar** que se ha establecido una convención estándar para dar nombres a los ficheros de datos de los ordenadores personales de la organización.
6. **Determinar** si se lleva un calendario de operaciones para todos aquellos ordenadores personales de la organización que procesan nóminas y programas de aplicación cíclica similares.

5.15 REVISIÓN POR LA DIRECCIÓN

- **Objetivo de Control.**

La alta dirección debiera revisar periódicamente el uso de los ordenadores personales de la organización.

- **Directiva de Auditoría.**

Debe cerciorarse de la existencia de revisiones periódicas por la alta dirección del uso de los ordenadores personales de la organización.

1. **Determinar** si se preparan informes periódicos del uso de los ordenadores personales de la organización para la alta dirección y se existen procedimientos adecuados para identificar y resolver cualesquiera problemas identificados en dichos informes.

2. **Determinar** si el riesgo asociado con el uso de ordenadores personales por la organización se revisa periódicamente por la alta dirección.

PARTE II - 5. CONTROLES SOBRE ORDENADORES PERSONALES.

PARTE II: CONTROLES ESPECÍFICOS DE CIERTAS TECNOLOGÍAS

CONTROLES SOBRE REDES DE ÁREA LOCAL

CONTENIDO

6 CONTROLES SOBRE REDES DE ÁREA LOCAL	11-6-1
6.1 POLÍTICAS SOBRE GESTIÓN DE REDES	11-6-1
6.2 SEGURIDAD LÓGICA DE LA RED	11-6-1
6.3 SEGURIDAD FÍSICA LA RED	11-6-2
6.4 SOPORTE Y GESTIÓN LA RED	11-6-2
6.5 CONTROL DE CAMBIOS EN LA RED	11-6-3

* * *

PARTE II - 6. CONTROLES SOBRE REDES DE AREA LOCAL.

6 CONTROLES SOBRE REDES DE ÁREA LOCAL

La dirección debiera asegurar que cualquier red de área local usada por la organización está adecuadamente diseñada y que su uso se controla adecuadamente.

6.1 POLÍTICAS SOBRE GESTIÓN DE REDES

*** Objetivo de Control.**

La alta dirección debiera establecer políticas que contemplen la selección, adquisición e instalación de redes de área local. Específicamente, dichas políticas debieran contemplar:

- a. los estándares en vigor en la organización relativos a la arquitectura de redes
- b. los procedimientos a seguir para diseñar, seleccionar y asegurar los costes y beneficios de una arquitectura de red de área local
- c. los procedimientos a seguir en la instalación de una red de área local que aseguren que se contemplan cosas tales como las convenciones acerca de nombres y las especificaciones de seguridad de los datos.

*** Directiva de Auditoría.**

Deben revisarse las políticas de la dirección relativas a selección, adquisición e instalación de una red de área local.

1. **Determinar** si la alta dirección de la organización ha emitido declaraciones escritas de política que prescriben los procedimientos a seguir en la selección, adquisición e instalación de redes de área local.
2. **Determinar** si la alta dirección de la organización ha emitido declaraciones escritas de política describiendo las arquitecturas de red que serán soportadas.

3. **Determinar** si la alta dirección de la organización ha emitido declaraciones de política escritas esbozando las directivas para el diseño y el análisis coste-beneficio de una instalación de red de área local propuesta. Dichas directivas debieran considerar, como mínimo:

- a. el análisis de las opciones de topografía de la red de área local
- b. la lógica seguida para la selección de los medios de transmisión empleados
- c. la selección del sistema operativo de la red de área local
- d. la revisión y aprobación de la propuesta de red de área local

4. **Determinar** si la alta dirección de la organización ha escrito declaraciones de política esbozando las directivas a seguir en la instalación de una red de área local. Apremiar si las mismas incluyen especificaciones para:

- a. una revisión del proceso para asegurar que se cumplen las convenciones en cuanto a nombres de la organización
- b. la documentación de la instalación real de la red de área local, incluyendo:

-mapas de red

-los parámetros seleccionados en el sistema operativo de la red de área local

5. **Determinar** si dichas declaraciones de política se han distribuido a los niveles de dirección adecuados dentro de la organización.

6.2 SEGURIDAD LÓGICA DE LA RED

*** Objetivo de Control.**

La alta dirección de la organización debiera establecer procedimientos que

PARTE II - 6. CONTROLES SOBRE REDES DE AREA LOCAL.

asegure que la adición, cambio o borrado de capacidades de acceso en una red de área local se basan en las necesidades de información de los usuarios de la red.

• Directiva de Auditoría.

Debe revisarse la política de la alta dirección de la organización respecto a la adición, cambio o borrado de capacidades de acceso en una red local.

1. **Determinar** que la alta dirección de la organización ha prescrito el uso de una forma estándar de documentar las solicitudes de adición, cambio o borrado de las capacidades de acceso de redes de área local. (Los procedimientos establecidos para el uso de este formulario de petición debieran asegurar que el proceso de revisión y aprobación se completa antes de que se lleven a cabo los cambios en cuestión).

2. **Determinar** que se ha establecido un proceso adecuado de gestión de la seguridad que soporte los cambios en los perfiles de acceso por usuarios a la red de área local.

3. **Determinar** que puede revisarse una matriz de perfiles de acceso para asegurar que los privilegios de acceso concedidos se han basado en la necesidad-de-conocer de los usuarios de la red de área local.

6.3 SEGURIDAD FÍSICA LA RED

• Objetivo de Control.

Debieran establecerse controles adecuados para asegurar que la seguridad de una red de área local no se pone en compromiso por amenazas físicas.

• Directiva de Auditoría.

Debe revisarse la adecuación de los controles establecidos por la alta dirección de la organización para asegurar que la seguridad de una red de área local no se pone en compromiso por amenazas físicas.

1. **Determinar** que los medios de transmisión utilizados por la red de área local están adecuadamente protegidos.

2. **Verificar** que el servidor de la red de área local ha sido objeto de medidas de seguridad y no pueden acceder a él individuos no autorizados.

3. **Determinar** que el servidor de la red de área local está protegido de daños resultantes de sobre-intensidades y puntas en el suministro de energía eléctrica.

4. **Determinar** que hay un sistema de suministro ininterrumpido de energía eléctrica conectado al servidor de la red de área local si ésta soporta aplicaciones que procesan informaciones críticas.

6.4 SOPORTE Y GESTIÓN LA RED

• Objetivo de Control.

Debieran brindarse gestión y soportes suficientes para asegurar la operación fiable e ininterrumpida de una red de área local.

• Directiva de Auditoría.

Debe revisarse la adecuación de la gestión y el soporte brindados a la operación de la red de área local.

1. **Determinar** que se han establecido procedimientos adecuados para revisiones periódicas de la capacidad de una red de área local y para asegurar que a los usuarios de la red se les ofrecen tiempos de respuesta adecuados y capacidades de almacenamiento en disco suficientes.

2. **Determinar** que los usuarios de red de área local tienen a su disposición soporte técnico adecuado para ayudarles a la resolución de problemas.

3. **Verificar** que los procedimientos en vigor de mantenimiento de las red de área local incluyen evaluaciones periódicas del funcionamiento de la red y **asegurar** que los problemas se resuelven

antes de que afecten al funcionamiento de la red.

6.5 CONTROL DE CAMBIOS EN LA RED

- **Objetivo de Control.**

La alta dirección de la organización debiera establecer controles de cambios a la configuración de una red de área local que aseguren su funcionamiento satisfactorio continuado.

- **Directiva de Auditoría.**

Debe revisarse la adecuación de los controles establecidos por la alta dirección de la organización sobre los cambios a la configuración de una red de área local .

1. **Determinar** que los procesos empleados para cambiar la configuración de una red de área local están documentados.

2. **Verificar** que se han considerado disposiciones para cualquier respaldo necesario antes de llevarse a cabo un cambio en una red de área local.

3. **Determinar** que se avisa adecuadamente a los usuarios de la red de área local antes de que se lleve a cabo un cambio en la configuración de la red.

PARTE II - 6. CONTROLES SOBRE REDES DE AREA LOCAL.

PARTE II: CONTROLES ESPECÍFICOS DE CIERTAS TECNOLOGÍAS

CONTROLES SOBRE SISTEMAS EXPERTOS

CONTENIDO

7. CONTROLES SOBRE SISTEMAS EXPERTOS

7.1 SELECCIÓN DE LA APLICACIÓN	II-7-1
7.2 DISEÑO	II-7-1
7.3 ADQUISICIÓN DEL CONOCIMIENTO	II-7-2
7.4 PRUEBAS	II-7-2
7.5 MANTENIMIENTO	II-7-2
7.6 FORMACIÓN Y SUPERVISIÓN LOS USUARIOS	II-7-3
7.7 ACCESO	II-7-3

* * *

PARTE II - 7. CONTROLES SOBRE SISTEMAS EXPERTOS.

7 CONTROLES SOBRE SISTEMAS EXPERTOS

Puede haber sistemas expertos en muchas aplicaciones de tratamiento de la información de tamaño medio y grande. Pueden usarse como ayuda a la toma de decisiones o pueden guiar a un individuo a través de un trabajo rutinario complejo. Debieran estar sometidos al mismo tipo de controles de desarrollo de la aplicación, mantenimiento y uso que se usan para todos los demás sistemas de información de la organización.

7.1 SELECCIÓN DE LA APLICACIÓN

• Objetivo de Control.

La alta dirección de la organización debiera emitir una declaración escrita que exija que la decisión de seleccionar una aplicación para la cual debe desarrollarse o implantarse un sistemas expertos debiera ser congruente con la estrategia general de proceso de datos de la organización y con la naturaleza de la aplicación seleccionada.

• Directiva de Auditoría.

La declaración escrita por la alta dirección de la organización exigiendo que la decisión de seleccionar una aplicación para la cual vaya a desarrollarse e implantarse un sistemas expertos debiera ser congruente con la estrategia general de proceso de datos de la organización y con la naturaleza de la aplicación seleccionada.

Debe revisarse la declaración escrita por la alta dirección de la organización exigiendo que la decisión de seleccionar una aplicación para la cual vaya a desarrollarse e implantarse un sistemas expertos debiera ser congruente con la estrategia general de proceso de datos de la organización y con la naturaleza de la aplicación seleccionada.

1. **Determinar** que la declaración emitida por la organización acerca del desarrollo e implantación de sistemas expertos se cumple.

2. **Verificar** que la aplicación a ser revisada es adecuada para su utilización como un sistema experto, cerciorándose de que el sistema satisface los siguientes criterios:

- a. la aplicación requiere el uso de juicio o criterio discrecionales
- b. hay disponibles expertos en el área de la aplicación y son capaces describir su conocimiento en un formulario en forma de una serie de reglas generales o ejemplos a seguir que es adecuado como base para el desarrollo de un sistemas expertos
- c. el consejo aportado por el sistemas expertos será probablemente de utilidad y valor para usuarios relativamente carentes de experiencia en el campo en que se ha desarrollado la aplicación.

3. **Determinar** que el uso de un sistemas expertos está adecuadamente soportado por el Departamento de Informática de la organización V<, de que:

- a. se dispone de equipos con suficiente capacidad para procesar el sistemas expertos
- b. el personal del Departamento incluye individuos con la experiencia y habilidad necesaria para mantener un sistemas expertos.

7.2 DISEÑO

• Objetivo de Control.

La alta dirección de la organización debiera establecer una metodología estructurada para el diseño de sistemas expertos que asegure que el producto final del diseño es lógico, razonable y que responde a las necesidades de los individuos que lo utilicen.

• Directiva de Auditoría.

Debe revisarse la metodología de diseño estructurado establecida por la alta dirección de la organización para ase-

PARTE II - 7. CONTROLES SOBRE SISTEMAS EXPERTOS.

gurar que los sistemas expertos son lógicos y razonables.

1. **Verificar** que la metodología establecida por la alta dirección de la organización para el desarrollo de sistemas expertos establece que dicho desarrollo se haga de forma lógico considerando la necesidad de:

- a. recoger y mantener actualizado el conocimiento experto
- b. aceptar entradas de usuarios de un sistema tal relativas a las circunstancias disponibles
- c. suministrar a esas personas consejo basado en el conocimiento experto.

7.3 ADQUISICIÓN DEL CONOCIMIENTO

• **Objetivo de Control.**

La metodología estructurada de diseño de sistemas expertos establecida por la alta dirección de la organización debería disponer que se entreviste a expertos cualificados de forma efectiva para ayudar a desarrollar reglas útiles que emulen el proceso de toma de decisiones del experto.

• **Directiva de Auditoría.**

Debe revisarse el proceso de entrevistas al experto que forma parte de la metodología estructurada de diseño de sistemas expertos establecida por la alta dirección de la organización.

1. **Evaluar** los registros del desarrollo del sistemas expertos de la organización y Verificar que:

- a. los expertos entrevistados estaban cualificados
- b. que el método para entrevistar a los expertos era efectivo
- c. que la traducción de los resultados de las entrevistas en la base de datos de conocimiento era adecuada.

7.4 PRUEBAS

• **Objetivo de Control.**

La metodología estructurada de diseño de sistemas expertos establecida por la alta dirección de la organización debería determinar que debe verificarse el funcionamiento del sistema por expertos humanos antes de usarlo en un entorno de producción y que a partir de ese momento debe revisarse periódicamente.

• **Directiva de Auditoría.**

Debe revisarse el grado de cumplimiento con los requisitos de la metodología estructurada de diseño de sistemas expertos establecida por la alta dirección de la organización. En particular, se debe cerciorar de que el funcionamiento del sistema se verificará por expertos humanos antes de usarlo en un entorno de producción y de que en adelante será revisado periódicamente.

1. **Verificar** mediante entrevistas y una revisión de la documentación pertinente que los requisitos de la metodología estructurada de diseño de sistemas expertos establecida por la alta dirección de la organización se han cumplido. En particular, **asegurarse** de que el funcionamiento del sistema será revisado por expertos humanos.

2. **Determinar**, a partir de una revisión de la documentación de los procedimientos de prueba del sistema experto y de los resultados obtenidos de ellos, que el funcionamiento de tales sistemas es fiable y produce resultados comparables a los que se producirían por expertos humanos bajo similares circunstancias.

7.5 MANTENIMIENTO

• **Objetivo de Control.**

La metodología estructurada de diseño de sistemas expertos establecida por la alta dirección de la organización debería determinar que el componente de base de datos del conocimiento del sistema se actualizará periódicamente a

fin de ajustar el funcionamiento del sistema de modo que se minimicen las decisiones inadecuadas.

• **Directiva de Auditoría.**

Debe determinarse el grado de cumplimiento con los requisitos de la metodología estructurada de diseño de sistemas expertos que establecen que el componente de base de datos del conocimiento del sistema se actualizará periódicamente para ajustar el funcionamiento del sistema de modo que minimice decisiones inadecuadas.

1. **Verificar** que los sistemas expertos de la organización son objeto de los procedimientos de control de cambios y de respaldo que también se aplican a los demás sistemas de información.
2. **Revisar** las disposiciones de la metodología de desarrollo de sistemas expertos de la organización y verificar que:

a. la frecuencia del mantenimiento refleja el ritmo de cambio en el entorno de la aplicación y el nivel de satisfacción del usuario con el funcionamiento del sistema

b. los expertos que brindan información para la actualización de la base de datos de conocimiento están cualificados para llevar a cabo dicha tarea

c. el funcionamiento del sistemas expertos, y especialmente la frecuencia y temática de las decisiones inadecuadas en combinación con su utilización, se controlan y evalúan para brindar una guía para el mantenimiento del sistema

7.6 FORMACIÓN Y SUPERVISIÓN LOS USUARIOS

• **Objetivo de Control.**

La metodología estructurada de diseño de sistemas expertos establecida por la alta dirección de la organización debería disponer que los usuarios de estos

sistemas deben ser formados y supervisados adecuadamente.

• **Directiva de Auditoría.**

Debe determinarse el grado de cumplimiento de los requisitos de la metodología estructurada de diseño de sistemas expertos establecida por la alta dirección de la organización de que los usuarios de tales sistemas sean formados y supervisados adecuadamente.

1. **Verificar**, mediante entrevistas y una revisión de la documentación pertinente, que los procedimientos de formación y supervisión de los usuarios de sistemas expertos de la organización son adecuados, y **cerciorarse**, en concreto, de que aquellas decisiones particularmente importantes o complejas, y posiblemente inadecuadas, se remiten a expertos humanos para su verificación.

7.7 ACCESO

• **Objetivo de Control.**

La metodología estructurada de diseño de sistemas expertos establecida por la alta dirección de la organización debería determinar que el acceso al sistema se restrinja con relación al valor y sensibilidad del conocimiento contenido en el mismo.

• **Directiva de Auditoría.**

Debe revisarse el grado de cumplimiento con las disposiciones sobre metodología estructurada de diseño de sistemas expertos, establecidas por la alta dirección de la organización, respecto a que el acceso al sistema se restrinja en relación con el valor y sensibilidad del conocimiento contenido en el mismo.

1. **Determinar**, mediante entrevistas y una revisión de la documentación pertinente, que el acceso por usuarios a los sistemas expertos de la organización, a sus bases de datos de conocimiento, y a los programas de las conchas del sistema se restringen adecuadamente.

ÍNDICE ANALÍTICO

- acceso a bases de datos B-iii
- acceso físico I-3-15, B-vi
- aceptación v, I-1-2, I-2-ii, I-2-7, I-2-9, I-2-16, I-2-24, I-2-25, I-3-3, II-2-1, II-2-2, II-5-4, B-i
- acompañamiento de visitas vii, I-3-i, I-3-15, B-viii
- acreditación de seguridad iii, I-1-i, I-1-7, I-1-8, II-2-9, B-vii
- acuerdo sobre nivel de servicio B-iv
- adecuado I-1-5, I-1-10, I-1-11, I-1-14, I-1-16, I-2-9, I-2-10, I-2-11, I-2-12, I-2-14, I-2-16, I-2-21, I-2-22, I-2-24, I-3-1, I-3-3, I-3-4, I-3-5, I-3-8, I-4-3, I-4-4, I-4-6, II-2-5, II-2-8, II-2-11, II-2-13, II-3-4, II-5-3, II-5-9, II-5-10, II-6-2, II-7-1, B-i
- administración de la seguridad B-vii
- agrupaciones de equipos II-2-7
- almacenamiento I-2-12, I-3-22, I-3-23, II-2-7, II-3-2, II-5-5, II-6-2, B-vii
- almacenamiento y remisión II-3-4
- alta dirección I, II, III, V, I-1-1, I-1-2, I-1-3, I-1-3, I-1-4, I-1-5, I-1-6, I-1-14, I-1-15, I-2-1, I-2-2, I-2-8, I-2-9, I-2-15, I-2-15, I-3-1, I-3-4, I-3-5, I-3-6, I-3-7, I-3-8, I-3-14, I-3-18, I-4-1, I-4-12, II-1-4, II-2-1, II-2-8, II-2-10, II-3-1, II-3-2, II-3-4, II-3-5, II-3-5, II-3-6, II-5-1, II-5-2, II-5-3, II-5-4, II-5-5, II-5-6, II-5-7, II-5-8, II-5-9, II-5-11, II-6-1, II-6-2, II-6-3, II-7-1, II-7-2, II-7-2, II-7-3
- anotar II-2-2
- apagar B-viii
- apertura I-2-20, II-3-5, B-vii
- aportados II-4-1, B-vi
- apreciar B-i
- asediadores II-2-9
- asegurar I-1-1, I-1-3, I-1-5, I-1-6, I-1-7, I-1-8, I-1-9, I-1-11, I-1-13, I-1-14, I-1-15, I-1-16, I-2-2, I-2-5, I-2-11, I-2-12, I-2-13, I-2-15, I-2-19, I-2-25, I-2-26, I-3-2, I-3-3, I-3-4, I-3-5, I-3-7, I-3-8, I-3-9, I-3-10, I-3-12, I-3-14, I-3-15, I-3-16, I-3-17, I-3-19, I-3-22, I-4-1, I-4-2, I-4-3, I-4-4, I-4-6, I-4-7, I-4-8, I-4-9, I-4-10, I-4-12, I-4-13, I-4-15, I-4-16, II-1-1, II-1-2, II-1-3, II-1-4, II-1-5, II-1-6, II-2-2, II-2-4, II-2-5, II-2-6, II-2-7, II-2-8, II-2-11, II-2-13, II-3-1, II-3-4, II-3-5, II-3-6, II-4-1, II-5-3, II-5-4, II-5-5, II-5-6, II-5-9, II-6-1, II-6-2, II-7-2, B-i, B-iii
- autenticación II-3-2, II-3-4
- autorización vii, I-2-4, I-2-11, I-2-13, I-2-22, I-2-25, I-3-13, I-3-17, I-4-i, I-4-1, I-4-2, I-4-3, I-4-5, I-4-6, II-1-4, II-3-4, II-5-4, II-5-8, II-5-9, II-5-10, B-i
- biblioteca de soportes magnéticos vi, I-3-i, I-3-8, B-v
- bibliotecario de soportes magnéticos B-v
- bifurcación II-3-5
- capacidad vi, V, I-2-3, I-2-11, I-2-23, I-3-i, I-3-2, I-3-3, I-3-11, I-3-21, II-2-5, II-2-14, II-6-2, II-7-1, B-i
- centralizado B-i
- centro de cálculo vii, I-3-i, I-3-17, B-iii
- cerciorarse I-2-1, I-2-5, I-2-6, I-2-7, I-2-8, I-3-3, I-3-5, I-3-6, I-3-7, I-3-9, I-3-11, I-3-13, I-3-16, I-3-19, I-3-21, I-4-1, I-4-2, I-4-5, I-4-6, I-4-7, I-4-10, I-4-11, I-4-16, II-1-1, II-1-5, II-2-14, II-5-10, II-5-11, II-7-3, B-i
- ciclo de vida del desarrollo de sistemas iv, III, V, I-2-i, I-2-1, I-2-2, I-2-3, I-2-4, I-2-5, I-2-6, I-2-7, I-2-8, I-2-9, I-2-10, I-2-11, I-2-12, I-2-13, I-2-14, I-2-15, I-2-16, I-2-17, I-2-18, I-2-19, I-2-20, I-2-21, I-2-22, I-2-23, I-2-24, I-2-25, I-2-28, I-2-29, II-2-2, II-5-3, B-v
- cierre B-vii
- cierres del sistema II-2-13
- cifra ix, II-2-i, II-2-10, II-3-1, B-iii
- cifrado B-iii

ÍNDICE ANALÍTICO

- cifrado de datos B-ii
- clasificación I-4-16, II-2-5, II-5-1, II-5-2, II-5-8, B-ii
- comité de dirección I-1-1, I-2-3, I-2-15, I-2-28, I-3-1, B-vii
- comparación I-1-9, I-3-11, II-3-5, B-ii
- conciencia de seguridad I-4-16, B-vii
- concienciación vii, I-3-1, I-3-14, I-3-18, II-2-12
- conciliación de totales de campos B-ii
- confidencialidad I-4-16, II-1-2, II-3-3, II-5-1, II-5-2, B-ii
- confidencialidad de los datos II-3-3, II-5-1, II-5-2, B-ii
- confirmar I-1-4, I-1-6, I-1-16, I-2-15, II-2-4, B-ii
- congruente I-1-3, I-1-8, I-1-10, I-2-1, I-2-25, I-3-3, I-3-8, I-3-14, I-4-1, I-4-3, II-2-3, II-2-12, II-7-1, B-ii
- conjunto de datos B-iii
- conjuntos de datos I-2-12, II-2-2, II-2-4, II-2-5, II-2-9
- consolidación II-2-4, II-2-14
- contabilidad de costes de trabajos vi, I-3-1, I-3-7, B-iv
- contabilidad de trabajos I-3-2, B-iv
- contingencia ix, I-2-8, I-2-19, I-2-23, II-2-i, II-2-14, B-ii
- contrato ix, I-2-19, I-3-21, II-3-2, II-3-3, II-3-6, II-4-i, II-4-1, II-5-4, B-ii
- control 1, i, iii, v, vi, vii, viii, ix, x, I, II, III, I-1-1; I-1-2, I-1-3, I-1-4, I-1-5, I-1-6, I-1-7, I-1-8, I-1-9, I-1-10, I-1-11, I-1-12, I-1-13, I-1-14, I-1-15, I-1-16, I-1-17, I-2-i, I-2-ii, I-2-1, I-2-2, I-2-3, I-2-4, I-2-5, I-2-6, I-2-7, I-2-8, I-2-9, I-2-10, I-2-11, I-2-12, I-2-13, I-2-14, I-2-15, I-2-16, I-2-17, I-2-18, I-2-19, I-2-20, I-2-21, I-2-22, I-2-23, I-2-24, I-2-25, I-2-26, I-2-27, I-2-28, I-2-29, I-3-i, I-3-1, I-3-2, I-3-3, I-3-4, I-3-5, I-3-6, I-3-7, I-3-8, I-3-9, I-3-10, I-3-11, I-3-12, I-3-13, I-3-14, I-3-15, I-3-16, I-3-17, I-3-18, I-3-19, I-3-20, I-3-21, I-3-22, I-3-23, I-3-24, I-4-i, I-4-1, I-4-2, I-4-3, I-4-4, I-4-5, I-4-6, I-4-7, I-4-8, I-4-9, I-4-10, I-4-11, I-4-12, I-4-13, I-4-14, I-4-15, I-4-16, II-1-i, II-1-1, II-1-2, II-1-3, II-1-4, II-1-5, II-2-i, II-2-1, II-2-2, II-2-3, II-2-4, II-2-5, II-2-6, II-2-7, II-2-8, II-2-9, II-2-10, II-2-11, II-2-12, II-2-13, II-2-14, II-3-1, II-3-2, II-3-4, II-3-5, II-3-6, II-4-1, II-4-2, II-4-i, II-5-ii, II-5-1, II-5-2, II-5-3, II-5-4, II-5-5, II-5-6, II-5-7, II-5-8, II-5-9, II-5-10, II-5-11, II-6-i, II-6-1, II-6-2, II-6-3, II-7-1, II-7-2, II-7-3, B-ii, B-v
- control de cambios vii, x, I-2-26, I-3-i, I-3-12, I-3-13, II-1-1, II-1-5, II-6-i, II-6-3, II-7-3, B-ii
- controlar I-2-1, I-2-11, I-2-25, I-3-9, I-3-10, I-4-8, I-4-11, I-4-14, I-4-16, II-1-4, II-2-4, II-2-5, II-2-6, II-2-8, II-2-10, II-2-11, II-2-13, II-5-8
- controles correctores I-2-14, B-ii
- controles detectores I-2-14, I-4-6, I-4-8, B-iii
- controles preventivos I-2-14, I-4-6, B-vi
- conversión v, viii, I-2-ii, I-2-7, I-2-23, I-2-24, I-4-i, I-4-4, I-4-5, II-2-1, II-2-2, II-4-1, II-5-6, B-ii
- corrección B-iii
- corrección de errores I-4-4, I-4-7, I-4-8, II-2-8, II-3-5
- corregir II, I-2-13, I-4-10, I-4-11, I-4-14, II-3-3, B-iii
- coste-beneficio vi, vii, ix, I-2-ii, I-2-7, I-2-14, I-2-24, I-2-28, I-3-i, I-3-11, I-4-6, II-2-1, II-2-10, II-3-i, II-3-1, II-5-1, II-5-2, II-5-4, II-5-8, II-6-1, B-ii
- creación de datos vii, I-4-i, I-4-1, I-4-4, II-1-2, B-ii
- cuadrar I-4-12
- cuadre I-4-6
- cumplimiento ii, iv, vi, II, I-1-ii, I-1-4, I-1-6, I-1-13, I-2-ii, I-2-1, I-2-15, I-2-16, I-2-28, I-3-4, I-3-14, I-3-18, I-4-4, I-4-13, II-1-3, II-2-14, II-5-3, II-7-2, II-7-3, B-ii
- daño II, I-3-14, B-ii
- datos de prueba I-2-16, I-2-22, I-2-23, B-viii
- datos fuente v, I-2-i, I-2-13, I-4-5, I-4-13, B-vii
- datos sensibles I-2-14, II-2-5, II-2-10, II-5-7, B-vii
- declaración I-2-1, I-2-2, I-2-17, I-2-19, I-3-14, I-4-3, I-4-9, II-2-3, II-2-8, II-3-1, II-3-6, II-5-1, II-5-3, II-7-1, B-vii
- definiciones de datos II-2-4

- demandas concurrentes conflictivas II-2-14
- departamento de informática iii, iv, vi, vii, IV, V, I-1-i, I-1-ii, I-1-1, I-1-2, I-1-3, I-1-4, I-1-5, I-1-6, I-1-7, I-1-8, I-1-9, I-1-10, I-1-11, I-1-12, I-1-13, I-1-14, I-1-15, I-1-16, I-1-17, I-2-1, I-2-2, I-2-3, I-2-4, I-2-5, I-2-7, I-2-8, I-2-15, I-2-18, I-2-19, I-2-20, I-2-21, I-2-22, I-2-23, I-2-24, I-2-25, I-2-26, I-2-28, I-2-29, I-3-i, I-3-ii, I-3-1, I-3-2, I-3-3, I-3-4, I-3-5, I-3-6, I-3-7, I-3-8, I-3-9, I-3-10, I-3-11, I-3-12, I-3-13, I-3-14, I-3-15, I-3-16, I-3-17, I-3-18, I-3-19, I-3-20, I-3-21, I-3-22, I-3-23, I-3-24, I-4-5, I-4-9, I-4-12, I-4-13, I-4-15, II-2-2, II-2-3, II-2-4, II-2-5, II-2-6, II-2-7, II-2-8, II-2-9, II-2-10, II-2-11, II-2-12, II-2-13, II-2-14, II-5-2, II-5-4, II-5-5, II-5-6, II-5-7, II-5-8, II-7-1, B-iv
- departamentos usuarios vii, I-1-1, I-1-2, I-1-4, I-1-5, I-1-6, I-1-10, I-1-14, I-2-1, I-2-2, I-2-3, I-2-4, I-2-5, I-2-7, I-2-8, I-2-12, I-2-13, I-2-15, I-2-16, I-2-18, I-2-21, I-2-22, I-2-23, I-2-24, I-2-25, I-2-26, I-2-29, I-3-ii, I-3-6, I-3-7, I-3-8, I-3-16, I-3-17, I-3-20, I-3-24, I-4-1, I-4-5, I-4-7, I-4-8, I-4-11, I-4-12, I-4-13, I-4-15, I-4-16, II-2-1, II-2-2, II-2-3, II-2-4, II-2-5, II-2-6, II-2-7, II-2-8, II-2-9, II-2-10, II-2-11, II-2-12, II-2-13, II-2-14, II-2-15, II-3-1, II-5-1, II-5-4, II-5-5, II-5-6, II-5-7, B-viii
- desactivar B-iii
- desarrollo de logical B-vii
- desarrollo de sistemas iv, III, V, I-1-6, I-2-i, I-2-1, I-2-2, I-2-3, I-2-4, I-2-5, I-2-6, I-2-7, I-2-8, I-2-9, I-2-10, I-2-11, I-2-12, I-2-13, I-2-14, I-2-15, I-2-16, I-2-17, I-2-18, I-2-19, I-2-20, I-2-21, I-2-22, I-2-23, I-2-24, I-2-25, I-2-26, I-2-28, I-2-29, I-3-1, II-2-2, II-5-3, II-7-2, II-7-3, B-v, B-viii
- descentralizado II-2-1, B-iii
- despedida y desconexión B-v
- determinar III, I-1-1, I-1-2, I-1-3, I-1-4, I-1-5, I-1-6, I-1-7, I-1-8, I-1-9, I-1-10, I-1-11, I-1-12, I-1-13, I-1-14, I-1-15, I-1-16, I-2-1, I-2-2, I-2-3, I-2-4, I-2-5, I-2-6, I-2-7, I-2-8, I-2-9, I-2-10, I-2-11, I-2-12, I-2-13, I-2-14, I-2-15, I-2-16, I-2-17, I-2-18, I-2-19, I-2-20, I-2-21, I-2-22, I-2-23, I-2-24, I-2-25, I-2-26, I-2-27, I-2-28, I-2-29, I-3-1, I-3-2, I-3-3, I-3-4, I-3-5, I-3-6, I-3-7, I-3-8, I-3-9, I-3-10, I-3-11, I-3-12, I-3-13, I-3-14, I-3-15, I-3-16, I-3-17, I-3-18, I-3-19, I-3-20, I-3-21, I-3-22, I-3-23, I-3-24, I-4-1, I-4-2, I-4-3, I-4-4, I-4-5, I-4-6, I-4-7, I-4-8, I-4-9, I-4-10, I-4-11, I-4-12, I-4-13, I-4-14, I-4-15, I-4-16, II-1-1, II-1-3, II-1-4, II-1-5, II-2-1, II-2-2, II-2-3, II-2-4, II-2-5, II-2-6, II-2-7, II-2-8, II-2-9, II-2-10, II-2-11, II-2-12, II-2-13, II-2-14, II-3-1, II-3-2, II-3-3, II-3-5, II-3-6, II-4-1, II-4-2, II-4-i, II-5-1, II-5-2, II-5-3, II-5-4, II-5-5, II-5-6, II-5-7, II-5-8, II-5-9, II-5-10, II-5-11, II-6-1, II-6-2, II-6-3, II-7-1, II-7-2, II-7-3, B-iii
- diario I-2-23, I-3-4, I-4-7, I-4-9, I-4-10, I-4-13, II-1-4, II-3-4, B-v
- diccionario de datos II-1-1, II-1-3, II-1-4, B-ii
- directiva de auditoría B-i
- discutir I-3-1, I-3-20, I-4-14, II-2-7, B-iii
- disposición I-2-16, I-2-20, I-4-13, II-6-2
- distribución viii, I-1-4, I-2-20, I-2-25, I-2-26, I-3-2, I-3-3, I-3-15, I-4-i, I-4-4, I-4-9, I-4-12, I-4-13, I-4-14, I-4-16, II-2-i, II-2-2, II-2-3, II-3-3, B-iv
- documento ii, II, III, I-1-11, I-1-14, I-3-12, I-4-1, I-4-3, I-4-5, I-4-7, B-vi, B-viii
- documento circulante I-4-5, B-viii
- emergencia vii, I-3-ii, I-3-17, I-3-18, I-3-19, I-3-21, B-iii
- emplazamiento remoto I-3-20, II-5-9, B-v
- en línea vii, viii, I-2-13, I-3-i, I-3-5, I-3-6, I-3-17, I-4-i, I-4-5, I-4-8, I-4-11, I-4-12, I-4-13, I-4-14, I-4-16, II-2-7, II-2-9, B-v
- encender B-viii
- encuesta I-3-6, B-viii
- entrevistar I-1-1, I-1-2, I-1-3, I-1-5, I-1-6, I-1-7, I-1-8, I-1-9, I-1-10, I-1-11, I-1-12, I-1-14, I-3-2, I-3-5, I-3-6, I-3-7, I-3-8, I-3-10, I-3-14, I-3-19, I-3-22, II-2-3, II-2-4, II-7-2, B-iv
- especificaciones iv, v, vi, V, I-1-ii, I-1-12, I-1-13, I-1-17, I-2-i, I-2-ii, I-2-1, I-2-3, I-2-5, I-2-6, I-2-7, I-2-8, I-2-10, I-2-11, I-2-12, I-2-13, I-2-14, I-2-15, I-2-16, I-2-17, I-2-21,

ÍNDICE ANALÍTICO

- I-2-26, I-2-27, I-2-28, I-3-1, I-3-2, I-3-3, I-3-11, II-2-1, II-2-5, II-2-7, II-2-13, II-5-2, II-6-1, B-vii
- estudio de viabilidad v, V, I-2-i, I-2-6, I-2-7, I-2-9, B-iii
- evaluación iv, v, vi, I, II, I-1-i, I-1-4, I-1-5, I-1-6, I-1-9, I-1-12, I-2-ii, I-2-9, I-2-14, I-2-16, I-2-23, I-2-24, I-2-25, I-2-26, I-2-27, I-2-28, I-2-29, I-3-4, I-3-11, II-3-3, II-5-8, B-i
- evaluar I-1-3, I-1-4, I-1-5, I-1-7, I-1-10, I-2-1, I-2-2, I-2-4, I-2-28, I-3-3, I-3-6, I-3-7, I-3-8, I-4-3, B-iii
- examinar II, III, I-1-6, I-2-3, I-2-9, I-2-23, I-3-3, I-3-9, I-3-20, II-2-3, II-2-12, II-5-6, II-5-8, B-iii
- excepción I-4-11, B-iii
- explorar I-1-2, B-iii
- explotación vi, I-1-6, I-1-9, I-1-15, I-3-i, I-3-10, II-2-13, II-5-8, B-ii, B-vi, B-vii
- exposición B-iii
- facturación a usuarios vi, I-3-i, I-3-8, B-viii
- fallo I-2-20
- fallo de logical B-vii
- fichero de datos rechazados I-4-8, I-4-11, B-viii
- fijación de parámetros u opciones II-2-12
- flujograma I-2-17, II-5-5, B-iv
- formación II, III, IV, v, vii, ix, x, I-1-i, I-1-ii, I-1-7, I-1-9, I-1-11, I-1-16, I-2-ii, I-2-1, I-2-7, I-2-20, I-2-21, I-2-24, I-3-i, I-3-ii, I-3-4, I-3-11, I-3-18, I-3-19, II-1-2, II-2-i, II-2-4, II-2-5, II-2-12, II-5-10, II-7-i, II-7-3, B-viii
- formación del usuario B-viii
- formato B-iv
- fuego I-3-8, I-3-18, II-5-9, B-iii
- generación de mensajes de ayuda del terminal B-vi
- gestión de proyectos I-1-11, B-vi
- gestión del calendario I-3-2, B-vii
- gestión interna I-3-8, B-iv
- grupo de control I-4-5, I-4-9, I-4-12, I-4-13, II-2-2, B-ii
- identificación del usuario I-3-16, I-4-11, II-2-8, B-v
- identificar III, IV, V, I-1-1, I-1-2, I-1-3, I-1-6, I-1-7, I-1-13, I-1-17, I-2-4, I-2-9, I-3-2, I-3-3, I-3-10, I-3-11, I-3-12, I-3-13, I-3-14, I-3-15, I-3-16, I-3-17, I-3-20, I-4-1, I-4-2, I-4-4, I-4-5, I-4-8, I-4-9, I-4-11, I-4-15, II-1-1, II-1-2, II-2-7, II-2-9, II-2-12, II-2-14, II-3-4, II-3-5, II-5-6, II-5-7, II-5-8, II-5-11, B-iv
- imputabilidad I-1-11, I-1-14, I-4-5, I-4-7, B-i
- indagar I-4-11, II-1-5
- independencia II, I-1-5, I-1-14, I-1-15, II-1-2, B-iv
- informar II, I-1-15, I-2-25, I-2-26, I-3-6, I-4-14
- informática distribuida viii, II-2-i, II-2-1, II-2-2, II-2-3, II-2-4, II-2-5, II-2-6, II-2-7, II-2-8, II-2-9, II-2-10, II-2-11, II-2-12, II-2-13, II-2-14, II-2-15
- inspeccionar I-1-3, B-viii
- instalación vii, I-2-1, I-2-25, I-3-i, I-3-2, I-3-7, I-3-9, I-3-11, I-3-12, I-3-13, II-1-1, II-2-6, II-2-9, II-2-10, II-2-14, II-2-15, II-3-5, II-5-9, II-6-1, B-ii, B-iii, B-iv
- intercambio de datos II-3-5
- intercambio electrónico de datos ix, IV, II-3-i, II-3-1, II-3-2, II-3-3, II-3-4, II-3-5, II-3-6
- interfaz VI, B-iv
- interrupción I-3-18, I-3-19, I-3-21, II-2-6, II-2-8, II-2-14, II-3-3, II-3-6, B-iv
- intimidad I-1-8, I-1-17, I-2-8, I-2-11, I-2-12, I-3-14, B-vi
- logical v, vi, vii, viii, ix, IV, I-2-i, I-2-1, I-2-2, I-2-7, I-2-15, I-2-16, I-2-18, I-2-19, I-2-20, I-2-21, I-3-i, I-3-1, I-3-2, I-3-3, I-3-4, I-3-6, I-3-7, I-3-9, I-3-10, I-3-11, I-3-12, I-3-13, I-3-19, I-4-i, I-4-6, I-4-7, I-4-9, I-4-10, I-4-14, II-1-1, II-1-3, II-1-4, II-1-5, II-2-i, II-2-1, II-2-3, II-2-5, II-2-6, II-2-7, II-2-8, II-2-11, II-2-13, II-3-i, II-3-3, II-3-5, II-4-1, II-5-ii, II-5-2, II-5-3, II-5-4, II-5-5, II-5-6, B-i, B-ii, B-v, B-vii
- logical de aplicación v, viii, ix, IV, I-2-i, I-2-18, I-4-i, I-4-9, I-4-10, II-2-11, II-3-i, II-3-5, II-5-ii, II-5-3, II-5-4, II-5-5, II-5-6, B-i

logical de control I-4-14, B-ii
 logical de ordenador personal I-4-6, I-4-7, II-5-2, B-v
 logical de sistema vi, vii, ix, I-3-1, I-3-9, I-3-10, I-3-11, I-3-12, I-3-13, II-2-i, II-2-8, B-v
 mantenimiento preventivo vi, I-3-i, I-3-4, I-3-5, II-2-7, B-vi
 manual de explotación I-2-19, B-vii
 manual de usuario v, ix, I-2-ii, I-2-20, II-3-i, II-3-6, II-4-1, B-viii
 material vi, I-3-i, I-3-4, B-iv
 material fungible II-2-7, B-vii
 material fungible fraccionado B-vii
 mensaje de ayuda del terminal B-vi
 metodología de ciclo de vida del desarrollo de sistemas de la organización I-2-1,
 I-2-2, I-2-3, I-2-4, I-2-5, I-2-6, I-2-7, I-2-8, I-2-9, I-2-10, I-2-11, I-2-12, I-2-13,
 I-2-14, I-2-15, I-2-16, I-2-17, I-2-18, I-2-19, I-2-20, I-2-21, I-2-22, I-2-23, I-2-24,
 I-2-25, I-2-28, I-2-29, II-2-2, B-v
 modem B-v
 muestreo B-vii
 necesidad-de-conocer II-6-2
 nivelado de cargas II-2-14
 objetivo de control B-ii
 obligatorio B-v
 obtener I-1-3, I-1-7, I-1-11, I-1-15, I-2-3, I-2-15, I-2-23, I-3-1, I-3-2, I-3-4, I-3-11, I-3-12,
 I-3-15, I-3-17, II-3-6, II-4-1, II-4-2, II-4-i, B-v
 ofimática II-5-8, B-v
 operaciones v, vii, ix, I-1-4, I-1-5, I-1-11, I-1-13, I-1-17, I-2-ii, I-2-1, I-2-2, I-2-18, I-2-19,
 I-2-21, I-3-ii, I-3-3, I-3-4, I-3-8, I-3-11, I-3-12, I-3-20, I-3-22, I-3-23, I-4-4, I-4-5,
 I-4-9, II-2-3, II-2-6, II-2-7, II-2-14, II-3-4, II-3-6, II-4-i, II-4-1, II-4-2, II-5-10, B-ii, B-vi
 oportuno I-2-26, I-3-9, I-4-8, B-viii
 ordenador personal IV, B-v
 palabras de paso vii, I-1-8, I-3-i, I-3-13, I-3-15, I-3-16, I-4-5, II-2-9, II-3-5, II-5-7, II-5-9, B-v
 pertinente I-2-20, I-4-3, II-2-4, II-2-10, II-2-12, II-2-13, II-3-2, II-3-5, II-7-2, II-7-3, B-vi
 pista de auditoría I-4-7, I-4-9, II-1-4
 pistas de auditoría v, I-2-i, I-2-10, I-2-11, I-2-14, I-2-22, I-2-23, I-2-27, I-4-12, II-2-3
 plan de contingencia I-2-8, I-2-23, B-ii
 plan de recuperación de desastres vii, ix, I-3-ii, I-3-19, I-3-20, I-3-21, I-3-22, I-3-23,
 I-3-24, II-4-i, II-5-9, B-iii
 política de seguridad I-3-14, B-vii
 post-implantación vi, ix, V, I-2-ii, I-2-26, I-2-27, I-2-28, I-2-29, II-2-i, II-2-12, II-2-13, B-vi
 presupuesto vi, I-3-i, I-3-1, I-3-4, B-i
 privilegios de sobreseimiento II-3-4
 probar I-4-4, I-4-14
 procedimiento operativo B-v
 procedimientos sensibles B-vii
 procesar B-vi
 proceso I-3-3, II-3-3, B-vi
 proceso de identificación del usuario I-3-16, B-v
 producción II-1-4, II-7-2, B-ii, B-vi
 programación B-vii
 programación de aplicaciones II-1-5, B-i
 programación del calendario de carga de trabajo B-viii
 propiedad II-1-2, II-1-4, II-2-4, II-3-3, II-5-3
 propietario II-1-4
 protección de registros B-v
 proteger I-3-8, I-3-10, I-3-14, I-3-23, I-4-16, II-2-10, II-2-11, B-vii
 prototipo I-2-10, B-vi
 provisiones I-2-10, I-2-11, II-3-6, II-5-4

ÍNDICE ANALÍTICO

- proyecto de desarrollo o modificación de sistemas de información I-2-9, I-2-10, I-2-11, I-2-12, I-2-13, I-2-14, I-2-16, I-2-18, I-2-19, I-2-20, I-2-21, I-2-22, I-2-23, I-2-25, B-iv
- prueba v, I-2-ii, I-2-16, I-2-21, I-2-22, I-2-23, I-2-24, I-3-3, I-3-7, I-3-12, I-3-23, II-2-2, II-2-9, II-2-12, II-5-4, II-7-2, B-iii, B-v, B-viii
- prueba en paralelo I-2-24, B-v
- pruebas v, vii, x, I-1-3, I-1-11, I-1-12, I-1-13, I-2-i, I-2-ii, I-2-9, I-2-16, I-2-18, I-2-19, I-2-20, I-2-21, I-2-22, I-2-23, I-2-24, I-2-26, I-3-ii, I-3-3, I-3-5, I-3-7, I-3-12, I-3-19, I-3-21, I-3-23, I-3-24, I-4-6, I-4-13, II-1-5, II-2-1, II-2-2, II-5-1, II-7-i, II-7-2, B-vii
- pruebas de carga punta B-vii
- punteo B-i
- puntos de control I-2-20, B-ii
- puntual B-viii
- rearranque I-2-20, I-3-10, B-vi
- recuperación vii, viii, ix, I-2-23, I-2-27, I-3-ii, I-3-10, I-3-18, I-3-19, I-3-20, I-3-21, I-3-22, I-3-23, I-3-24, I-4-3, I-4-7, II-1-i, II-1-4, II-1-5, II-2-6, II-2-15, II-3-4, II-4-i, II-5-1, II-5-9, B-iii, B-vi
- recursos de ordenador vii, I-3-ii, I-3-3, I-3-5, I-3-7, I-3-8, I-3-14, I-3-15, I-3-16, I-3-17, I-3-18, I-3-20, B-ii
- red conmutada I-3-21, II-2-9, B-iii
- red de área local II-6-1, II-6-2, II-6-3
- red de informática distribuida II-2-1, II-2-2, II-2-3, II-2-4, II-2-5, II-2-6, II-2-7, II-2-8, II-2-9, II-2-10, II-2-11, II-2-12, II-2-13, II-2-14, II-2-15
- redes de área local x, II-6-i, II-6-1, II-6-2
- registro I-4-14, B-vi
- remoto I-3-20, I-3-22, II-2-7, II-5-9, B-v, B-vi
- rendimiento iv, I-1-ii, I-1-10, I-1-16, I-3-2, B-vi
- respaldo vii, ix, x, I-2-23, I-2-27, I-3-ii, I-3-18, I-3-20, I-3-21, I-3-22, I-3-24, I-4-15, II-1-5, II-2-i, II-2-1, II-2-3, II-2-6, II-2-7, II-3-3, II-5-ii, II-5-1, II-5-9, II-6-3, II-7-3, B-i
- resumen I-1-14, I-2-7, II-2-4
- revelación II-2-10, B-iii
- revisar II, I-1-1, I-1-2, I-1-3, I-1-4, I-1-5, I-1-6, I-1-7, I-1-8, I-1-9, I-1-10, I-1-11, I-1-12, I-1-13, I-1-14, I-2-1, I-2-2, I-2-3, I-2-4, I-2-6, I-2-7, I-2-8, I-2-9, I-2-10, I-2-11, I-2-12, I-2-13, I-2-14, I-2-15, I-2-17, I-2-18, I-2-19, I-2-22, I-2-26, I-3-1, I-3-4, I-3-5, I-3-6, I-3-7, I-3-9, I-3-10, I-3-11, I-3-12, I-3-13, I-3-14, I-3-15, I-3-16, I-3-17, I-3-18, I-3-19, I-3-20, I-3-21, I-3-22, I-3-23, I-3-24, I-4-4, I-4-8, I-4-10, I-4-11, I-4-12, I-4-14, II-1-1, II-1-5, II-1-6, II-2-1, II-2-2, II-2-3, II-2-4, II-2-6, II-2-8, II-2-9, II-2-10, II-2-11, II-2-12, II-2-13, II-2-14, II-4-1, II-4-2, II-5-11, II-7-3, B-vi
- riesgo I-2-2, I-2-8, I-3-16, I-3-20, I-4-16, II-2-2, II-3-4, II-5-1, II-5-11, B-iii, B-vii
- riesgo de pérdidas I-3-20, B-vii
- sala B-ii, B-iii
- seguimiento ii, I-2-26, I-3-2, I-3-5, I-3-6, I-4-1, I-4-2, I-4-8, I-4-11, I-4-12, II-5-7, B-iv, B-v
- seguridad física x, I-3-13, II-2-10, II-2-11, II-5-ii, II-5-9, II-6-i, II-6-2, B-vi
- seguridad lógica vii, x, I-3-i, I-3-13, I-3-14, II-6-i, II-6-1, B-v
- seguro I-3-8, II-2-8, II-2-10, II-3-2, II-5-5, II-5-10, B-iv
- separación de funciones iii, I-1-i, I-1-6, I-2-2, I-2-25, I-3-17, I-4-2, I-4-4, I-4-6, I-4-8, B-vii
- servidor II-6-2
- sistema de gestión de bibliotecas de soportes magnéticos B-v
- sistema de informática distribuida II-2-13
- sistema operativo vi, ix, I-2-23, I-3-i, I-3-10, I-3-17, II-2-i, II-2-8, II-2-9, II-6-1, B-v
- sobreseimiento II-3-4
- sólo lectura B-vi
- suplantación II-3-4
- telecomunicaciones I-2-1, I-2-8, I-3-21, II-2-7, II-2-12, B-viii
- tiempo de respuesta II-2-1, II-2-7, B-vi

tiempo que está disponible II-3-3
 tiempo real II-3-3, B-vi
 total del lote I-4-13
 totales de control I-2-11, I-2-14, I-2-20, I-4-4, I-4-5, I-4-7, I-4-9, I-4-10, I-4-12, II-5-6, II-5-7,
 B-ii
 trabajo IV, VI, III, IV, V, I-1-ii, I-1-11, I-1-14, I-1-16, I-1-17, I-2-3, I-2-4, I-2-5, I-2-6, I-2-8,
 I-2-9, I-2-15, I-2-18, I-2-19, I-2-21, I-3-1, I-3-2, I-3-3, I-3-4, I-3-5, I-3-6, I-3-7,
 I-3-12, I-4-4, I-4-8, I-4-9, II-4-2, II-5-4, II-5-10, II-7-1, B-iv, B-viii
 transmisión x, IV, I-3-1, I-4-1, I-4-16, II-2-2, II-2-8, II-2-12, II-2-14, II-3-1, II-3-2, II-3-3, II-3-4,
 II-3-6, II-5-ii, II-5-6, II-5-8, II-5-9, II-6-1, II-6-2, B-i, B-viii
 tratamiento por lotes B-i
 traza B-i
 vacaciones I-3-4, B-viii
 validación v, viii, I-2-i, I-2-12, I-2-16, I-2-22, I-4-i, I-4-6, I-4-7, I-4-10, I-4-11, B-viii
 validar I-3-6, I-4-7, I-4-10
 verificar I-1-2, I-1-11, I-1-12, I-1-13, I-1-14, I-2-2, I-2-5, I-2-7, I-2-8, I-2-19, I-2-20, I-2-21,
 I-2-22, I-2-24, I-2-26, I-2-28, I-2-29, I-3-2, I-3-3, I-3-5, I-3-6, I-3-7, I-3-9, I-3-10,
 I-3-12, I-3-13, I-3-15, I-3-16, I-3-17, I-3-18, I-3-22, I-3-23, I-3-24, I-4-1, I-4-2, I-4-3,
 I-4-9, I-4-10, I-4-11, I-4-13, II-2-2, II-2-3, II-2-4, II-2-5, II-2-6, II-2-7, II-2-8, II-2-9,
 II-2-10, II-2-11, II-2-12, II-2-13, II-2-14, II-2-15, II-3-1, II-3-2, II-3-4, II-3-5, II-4-1,
 II-4-2, II-5-7, II-5-9, II-5-10, II-6-2, II-6-3, II-7-1, II-7-2, II-7-3, B-viii
 vigilancia I-3-15, II-3-4, B-viii

* * *

ÍNDICE ANALÍTICO

ÍNDICE ANALÍTICO

APÉNDICE A

CONTRIBUYENTES A ESTA PUBLICACIÓN

El contenido de esta publicación es un compendio y cúmulo de los conocimientos y experiencia de numerosos Auditores Informáticos. Reconocemos, con agradecimiento, las contribuciones a la expansión y perfeccionamiento de su profesión por tantas personas. A continuación relacionamos alfabéticamente, con indicación de su lugar de residencia, los nombres de aquéllos contribuyentes de los que tenemos constancia. Lamentamos cualesquiera omisiones, errores en los nombres, o de cualquier otro tipo, y agradeceríamos se no informase de las correcciones necesarias, a fin de que la próxima versión de esta lista sea más exacta.

John J. Anderson, St. Louis MO	Paul C. Hostall, Washington DC
Rick Barrow, Richmond VA	Rita Hull, Richmond VA
David Barton, Lancaster SC	Ray Irvin, Plainfield IN
Linda Ludean Beasley, Salinas CA	David Johnston, Charlotte NC
A. Faye Borthick, Knoxville TN	David F. Kent, Washington DC
James Brennan, Charlotte NC	Robert Klenk, Philadelphia PA
John Brilliant, Jr., Richmond VA	Gary L. Kreigh, Indianapolis IN
Paul Burch, Indianápolis IN	Glenn Lane, San Francisco CA
Peter S. Cluck, Philadelphia PA	Keith Lawler, London United Kingdom
Edward DeLanis, Concord CA	Cheryl A. Little, Oakland CA
Michael Donahue, Washington DC	George E. Love, Richmond VA
John Fattes, Washington DC	Daniel P. Lubas, Blue Bell PA
Samantha Fordyce, New York NY	Richard R. Lynch, Richmond VA
George J. Freuhan, San Francisco CA	Richard M. Martin, San Francisco CA
David Goodyear, Blacksburg VA	Elichi Matsubara, Tokyo Japan
Timothy A. Gudeman, Indianapolis IN	Ronald Matthews, Vancouver Canada
Steven Hass, Philadelphia PA	James E. Metcalfe, Seattle WA
William S. Hancock, Cincinnati OH	Carol Moulton, Indianapolis IN
Gary Hardy, London United Kingdom	Michael J. Murray, Seattle WA
Michael Hines, West Lafayette IN	Robert G. Parker, Victoria Canada

APÉNDICES

C. Grayling Pruitt, Nashville TN

Raymond E. Riegle, Richmond VA

John R. Robles, San Juan PR

Laurie Rohrer, Oakland CA

Zelia G. Ruthberg, Rockville MD

Dan Singel, Irving TX

Shellie Thomas, Indianapolis IN

Tim Wise, Washington DC

Greg Williamson, Minneapolis MN

APENDICE B

GLOSARIO

- A -

acceptance

accountability

accountable (documents, processes)

accounted for

application programming

application software

appropriate

ascertain (to)

assess (to)

assessment

assure (to)

audit guideline

audit trails

authorization

- B -

back-up

batch

batch procesing

budget

buffers

bypass

- C -

capacity

centralized

aceptación

imputabilidad

imputables a personas (documentos, procesos)

Imputados a personas

programación de aplicaciones

logical de aplicación

adecuado

cerciorarse

apreciar

evaluación

asegurar

directiva de auditoría

traza de auditoría

autorización

respaldo

lote

tratamiento por lotes

presupuesto

áreas de memoria asignadas a transmisión de datos

puenteo

capacidad

centralizado

APÉNDICES

change control
checkpoint controls
classification
compare (to)
comparison
compliance
computer facility
computer operation
computer resources
confidentiality
confirm (to)
consistent
contingency
contingency planning
contract
control software
control group
control totals
control objective
conversion
corrective controls
cost benefit
crossfooting

- D -

damage
data dictionary
data origination
data subject privacy
data encryption

control de cambios
puntos de control
clasificación
comparar
comparación
cumplimiento
instalación (o sala) de ordenadores
explotación / operaciones / producción
recursos de ordenador
confidencialidad
confirmar
congruente
contingencia
plan de contingencia
contrato
logical de control
grupo de control
totales de control
objetivo de control
conversión
controles correctores
coste-beneficio
conciliación de totales de campos

daño
diccionario de datos
creación de datos
confidencialidad de los datos
cifrado de datos (criptografía)

OBJETIVOS DE CONTROL, 1990.

database access
data processing site
dataset
decentralized
detective controls
determine (to)
dial-up
disable (to)
disaster recovery plan
disclosure
discuss (to)

- E -

edit (to)
editing
emergency
encrypted
encryption
ensure (to)
evaluate (to)
evidence
examine (to)
exception
explore (to)
exposure

- F -

facility
feasibility study
fire

acceso a bases de datos
centro de cálculo (o sala de ordenadores)
conjunto de datos (en bases de datos)
descentralizado
controles detectores
determinar
red conmutada
desactivar
plan de recuperación de desastres
revelación
discutir

corregir
corrección (acción o efecto de corregir)
emergencia
cifrado
cifra (criptografía)
asegurar
evaluar
prueba
examinar
excepción
explorar
exposición / riesgo

instalación
estudio de viabilidad
fuego

APÉNDICES

fire marshall

jefe de bomberos o autoridad con jurisdicción sobre normativa de protección de incendios

flowchart

flujograma

follow-up

seguimiento

- H -

hardware

material (equipos)

housekeeping

gestión interna (tareas domésticas)

- I -

identify (to)

identificar

independence

independencia

information services department

departamento de informática

information system development or modification project

proyecto de desarrollo o modificación de sistemas de información

insurance

seguro

installation

instalación

interface

interfaz (interficie)

interruption

interrupción

interview (to)

entrevistar

- J -

job

trabajo

job accounting

contabilidad de trabajos

job cost accounting

contabilidad de costes de trabajos

- K -

knowledge database

base de conocimientos

- L -

layout

formato (en pantallas, impresos, etc.) / distribución (en salas)

level of service agreement

acuerdo sobre nivel de servicio

locks

log

logging

logical security

log-off process

log-on process

- M -

mandatory

media librarian

media library

media library management system

microcomputer

microcomputer software

modem

monitoring

- O -

obtain (to)

off site

office automation

on line

operating procedure

operating system

operating system software

organization's system
development life cycle methodology

- P -

parallel testing

passwords

protección de registros

diario

anotaciones (o apuntes) a diarios

seguridad lógica

proceso de despedida y desconexión

proceso de identificación del usuario

obligatorio

bibliotecario de soportes magnéticos

biblioteca de soportes magnéticos

sistema de gestión de bibliotecas de
soportes magnéticos

ordenador personal

logical de ordenador personal

modem

control, seguimiento

obtener

emplazamiento remoto

ofimática

en línea

procedimiento operativo

sistema operativo

logical de sistema

metodología de ciclo de vida del desarrollo
de sistemas de la organización

prueba en paralelo

palabras de paso

APÉNDICES

performance

physical access

physical security

post-implementation

preventive controls

preventive maintenance

privacy

process (to)

processing

production

project management

prompt

prompting

prototype

provide

provided

provisions

- R -

read only

real time

record

record retention schedule

recovery

relevant

remote

response time

restart

review (to)

rendimiento

acceso físico

seguridad física

post-implantación

controles preventivos

mantenimiento preventivo

intimidación

procesar (tratar) datos

proceso (tratamiento) de datos

explotación (producción, operaciones)

gestión de proyectos

mensaje de ayuda del terminal

generación de mensajes de ayuda del terminal

prototipo

disponer (establecer)

aportados (suministrados)

disposiciones

sólo lectura

tiempo real

registro (magnético) / documento

calendario de retención de ficheros / documentos

recuperación

pertinente (apropiado, significativo)

remoto

tiempo de respuesta

rearranque

revisar

APÉNDICES

surveillance

survey

survey (to)

suspense file

system development

- T -

telecommunications

test data

timely

training

transmission

turnaround transmittal document

turn-off

turn-on

- U -

user billing and charge-back

user departments

user manual

user training

- V -

vacations

validation

verify (to)

visitor escort

- W -

workload scheduling

vigilancia

encuesta

inspeccionar

fichero de datos rechazados

desarrollo de sistemas

telecomunicaciones

datos de prueba

puntual / oportuno

formación

transmisión

documento circulante

apagar

encender

facturación a usuarios

departamentos usuarios

manual de usuario

formación del usuario

vacaciones

validación

verificar

acompañamiento de visitas

programación del calendario de carga de trabajo

.

OBJETIVOS DE CONTROL, 1990.

risk-of-loss
run book

- S -

sampling
scheduling

script file

secure (to)

security awareness

security clearance

security administration

security policy

sensitive data

sensitive procedures

separation of duties

sign-on

sign-off

software

software development

software failure

source data

specifications

staged supplies

statement

steering committee

storage

stress tests

supplies

riesgo de pérdidas
manual de explotación

muestreo

programación (de explotación) / gestión
del calendario

ficheros con protocolos de usuario para
comunicaciones

proteger

conciencia de seguridad

acreditación de seguridad

administración de la seguridad

política de seguridad

datos sensibles

procedimientos sensibles

separación de funciones

apertura (para su uso) de terminales

cierre (para su uso) de terminales

logical

desarrollo de logical

fallo de logical

datos fuente

especificaciones

material fungible fraccionado (en lugar y /
o tiempo)

declaración

comité de dirección

almacenamiento

pruebas de carga punta

material fungible (suministros)

risk-of-loss

run book

- S -

sampling

scheduling

script file

secure (to)

security awareness

security clearance

security administration

security policy

sensitive data

sensitive procedures

separation of duties

sign-on

sign-off

software

software development

software failure

source data

specifications

staged supplies

statement

steering committee

storage

stress tests

supplies

riesgo de pérdidas

manual de explotación

muestreo

programación (de explotación) / gestión del calendario

ficheros con protocolos de usuario para comunicaciones

proteger

conciencia de seguridad

acreditación de seguridad

administración de la seguridad

política de seguridad

datos sensibles

procedimientos sensibles

separación de funciones

apertura (para su uso) de terminales

cierre (para su uso) de terminales

logical

desarrollo de logical

fallo de logical

datos fuente

especificaciones

material fungible fraccionado (en lugar y / o tiempo)

declaración

comité de dirección

almacenamiento

pruebas de carga punta

material fungible (suministros)

APÉNDICES

surveillance

survey

survey (to)

suspense file

system development

- T -

telecommunications

test data

timely

training

transmission

turnaround transmittal document

turn-off

turn-on

- U -

user billing and charge-back

user departments

user manual

user training

- V -

vacations

validation

verify (to)

visitor escort

- W -

workload scheduling

vigilancia

encuesta

inspeccionar

fichero de datos rechazados

desarrollo de sistemas

telecomunicaciones

datos de prueba

puntual / oportuno

formación

transmisión

documento circulante

apagar

encender

facturación a usuarios

departamentos usuarios

manual de usuario

formación del usuario

vacaciones

validación

verificar

acompañamiento de visitas

programación del calendario de carga de trabajo

.