



Industria y Comercio
SUPERINTENDENCIA

SOLICITUD

PATENTE DE INVENCION

04-1188803

21. EXPEDIENTE N°

54. TÍTULO "METODO PARA EVALUACION DE MADUREZ DE SEGURIDAD"

51. CLASIFICACIÓN INTERNACIONAL G06F 1/00

71. SOLICITANTE SCHLUMBERGER OMNES, INC.

DOMICILIO HOUSTON, ESTADO DE TEXAS, ESTADO UNIDOS DE AMERICA

74. REPRESENTANTE LEGAL ALICIA LLOREDA RICAURTE
T.P. 53.215

22. BOGOTÁ, D.C. 25 NOV 2004

PETITORIO



SUPERINDUSTRIA Y COMERCIO
 Radicación : 04116863 20030008 Folios: 163
 Fecha (RD): 2004-11-25 16:18:01
 Trámite : 611 PCT-PATENT 379 FASE I/DCI 411 PRESENTE
 Dependencia: 2000 DIVISION DE NUEVAS CREACIONES

FORMULARIO UNICO DE SOLICITUD DE PATENTE PCT ENTRADA EN FASE NACIONAL

① **SOLICITUD DE:**
☒ Patente de Invención ☐ Patente de Modelo de Utilidad

☐ Capítulo I. ☒ Capítulo II.

② SOLICITANTE (71)	Nombre: SCHLUMBERGER OMNES, INC. Dirección: Suite 400, 5599 San Felipe, Houston, TX 77056, Estados Unidos de América. Nacionalidad o Domicilio: Houston, Estado de Texas, Estados Unidos de América. Lugar de Constitución: Teléfono: 3264270 Fax: 6069701 E-mail: jllcco@lloredacamacho.com	IDENTIFICACION C.C. ☐ NIT ☐ C.E. ☐ Otro ☐ Cual _____ Número _____
③ REPRESENTANTE O APODERADO	Nombre: ALICIA LLOREDA RICAURTE Dirección: Calle 72 No. 5-83 Piso 5º, Bogotá, Colombia Teléfono: 3264270 Fax: 6069701 E-mail: jllcco@lloredacamacho.com	C.C. ☒ NIT ☐ C.E. ☐ Otro ☐ Cual _____ Número <u>39.690.713</u> TP <u>53.215</u>
④ INVENTOR(ES) (72)	Nombre: BAUDOUIN, Claude R. y ELLIOTT, Collin, R. Dirección: 2319 McDuffie Street, Houston, TX 77019-6527 y 1 st Floor Flat, 12 Weatherby Gardens, London SW5 0JW. Nacionalidad o Domicilio: Estados Unidos de América y Gran Bretaña.	

⑤ **PCT (86)**
 Solicitud Internacional No. PCT/US2003/013298 Fecha: 28/04/03
 Publicación Internacional No. WO 2003/093960 A2 Fecha: 13/11/03

⑥ **Título (54) "MÉTODO PARA EVALUACIÓN DE MADUREZ DE SEGURIDAD"**

⑦ **Clasificación Internacional (51) G06F 1/00**

⑧ Prioridad SI ☒ NO ☐	(33) País de Origen US	(32) Fecha 29/04/02	(31) Número de Solicitud 10/134,815
--	---------------------------	------------------------	--

⑨ **Comprobante de Pago No. 04 - 83.996 Fecha: 28/10/04**

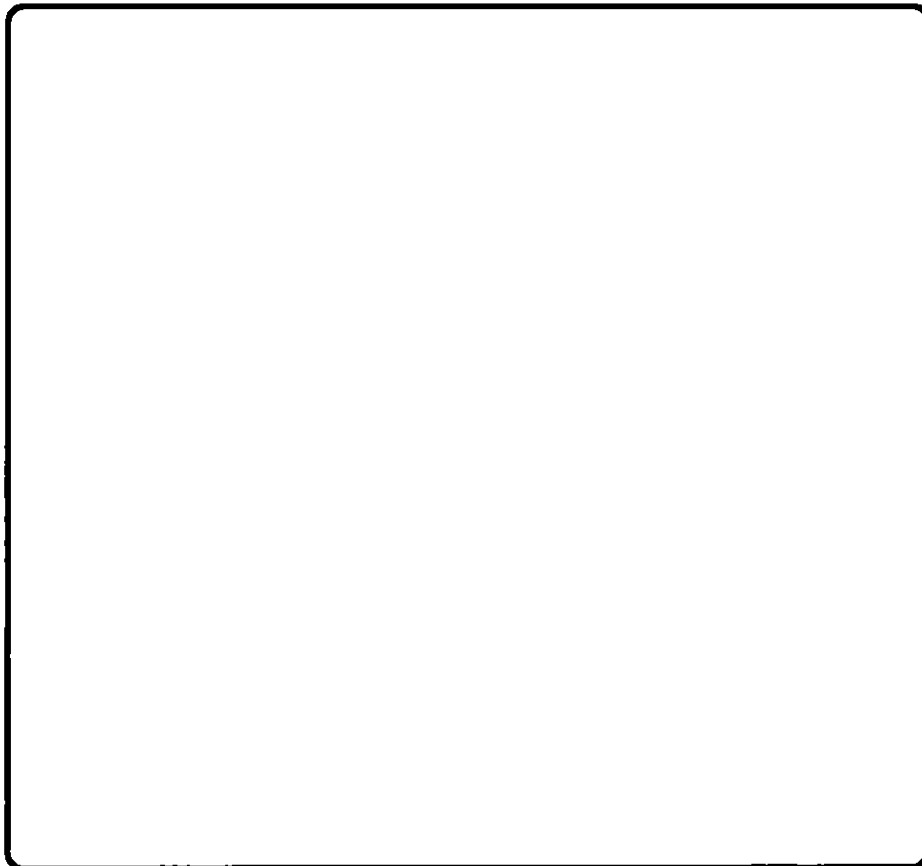
10

ANEXOS

- ☒ Comprobante de pago de la tasa de presentación de la solicitud.
- ☐ Documento que acredite la existencia y representación legal cuando el solicitante sea persona jurídica.
- ☐ Documento de Representación Legal.
- ☐ Documento de cesión de los Inventores.
- ☐ Declaraciones
- ☐ Copia de la solicitud internacional. (Resumen, descripción, reivindicaciones, dibujos)
- ☒ Traducción de la solicitud internacional al castellano. (Resumen, descripción, reivindicaciones, dibujos)
- ☐ Copia del examen preliminar internacional efectuado por la Autoridad Internacional de Examen Preliminar (IPEA).
- ☐ Traducción del examen preliminar internacional efectuado por la IPEA.
- ☐ De ser el caso, copia del contrato de acceso.
- ☐ De ser el caso, documento que acredite la licencia o autorización de uso de conocimientos tradicionales de las comunidades indígenas.
- ☐ Arte Final 12X12.
- ☐ De ser el caso, información sobre otras solicitudes de patente o títulos obtenidos en el extranjero por el mismo titular o su causante, relacionados parcial o totalmente con la invención de esta solicitud.
- ☐ De ser el caso, modificaciones efectuadas a la solicitud internacional.
- ☒ Otros: Reporte de Búsqueda Internacional con su traducción, Publicación con su traducción, Capítulo reivindicatorio originalmente presentado en Fase Internacional con su traducción, Notificación de Cambio de nombre de un inventor con su traducción, notificaciones de cambio de nombre del agente con sus traducciones y Anexo Explicativo de modificaciones a las reivindicaciones.

11

FIGURA CARACTERISTICA:



12

Solicito la concesión de la patente,

NOMBRE: ALICIA LLOREDA RICAURTE

FIRMA:

C.C. 39.890.713 Usaquén T.P. 53.215

INDUSTRIA Y CIENCIA
Radicación : 04116363 00000000 Folios: 163
NET : 300174089- Fecha (R2): 2004-11-25 16:10:01
Trámite : 011 FCT-PATENT 379 FASE NACI 411 PRESENTA
Dependencia: 2020 DIVISION DE PEQUEÑAS EMPRESAS

RECIBO OFICIAL DE CAJA : 04 - \$3,996
FECHA : OCTUBRE 26 DE 2004

***** CONSIGNACION *****

DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	Vr. PAGO
LLOPEJA Y CIA S. A	CONSIGNACION	BANCO POPULAR	050-00110-6	32106766	26/10/2004	\$,255,000.00

***** CONCEPTO *****

CANT.	RENTISTICO	CONCEPTO	TOTAL CONCEPTO
1	50005-01-01	SOLICITUDES	
1		TRAMITES DE SOL. DE PATENTE DE IN	422,000.00
		TOTAL :	\$ 422,000.00

SOM: CUATROCIENTOS VEINTIDOS MIL PESOS

RESPONSABLE : _____

RECIBO DE CAJA APLICADO AL EXPEDIENTE No.  _____

Sentran felix 305
para el pub y target
20047
09-12-2004

Se notran felus 3a S
pca eto pub y target
2004
09-12-2004

TRATADO DE COOPERACION DE PATENTES
PCT
REPORTE DE BUSQUEDA INTERNACIONAL

(PCT Artículo 18 y Reglas 43 y 44)

Registro de referencia del solicitante o agente 09469/008WO1	PARA FUTURAS ACCIONES ver Notificación o Transmisión del Reporte de Búsqueda Internacional (Forma PCT/ISA/220) así como, donde aplique, el Item 5 a continuación.	
Solicitud internacional No. PCT/US 03/13298	Fecha de registro internacional (día/mes/año) 28/04/2003	Fecha de Prioridad (Primera) (día/mes/año) 29/04/2002
Solicitante SCHLUMBERGER OMNES, INC.		

Esta Autoridad de Búsqueda Internacional, en virtud del presente declara, conforme al Artículo 17(2) (a), que no se establecerá ningún reporte de Búsqueda Internacional en la solicitud internacional por las razones indicadas más adelante.

1. ☒ El objeto de la solicitud internacional se refiere a:

- a. ☐ teoría científica
- b. ☐ teorías matemáticas
- c. ☐ variedades de plantas.
- d. ☐ variedades de animales
- e. ☐ esencialmente procesos biológicos para la producción de plantas y animales, diferentes a los procesos microbiológicos y a los productos de dichos procesos.
- f. ☒ esquemas, reglas o métodos para hacer negocios
- g. ☐ esquemas, reglas o métodos para la realización de actos puramente mentales
- h. ☐ esquemas, reglas o métodos para juegos
- i. ☐ métodos para tratamiento de cuerpos humanos por cirugía o terapia
- j. ☐ métodos para tratamiento de cuerpos humanos por cirugía o terapia
- k. ☐ métodos de diagnóstico practicados en el cuerpo humano o animal
- l. ☐ más presentaciones de información
- m. ☐ programas de computador para los cuales esta Autoridad de Búsqueda Internacional no está dotada para buscar el arte anterior.

2. ☐ El incumplimiento de los requerimientos prescritos en cuanto a las siguientes partes previene que se realice una búsqueda importante de:

☐ la descripción ☒ las reivindicaciones ☐ los dibujos

3. ☐ El incumplimiento del estándar previsto en el Anexo C de las Instrucciones Administrativas en cuanto al listado de la secuencia nucleotídica y/o amino ácida previene que se realice una búsqueda importante de:

- ☐ no se ha suministrado la forma escrita o no cumple con el estándar.
- ☐ la forma legible por computador no se ha suministrado o no cumple con el estándar.

4. Otros comentarios: VER HOJA DE INFORMACION ADICIONAL

Nombre y dirección de la autoridad de búsqueda internacional
European Patent Office, P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk
Tel. No. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax No. (+31-70) 340-3016

Funcionario Autorizado
Jacinta Reddy

CONTINUACION DE INFORMACION ADICIONAL PCT/ISA/ 203

Las reivindicaciones se relacionan con la materia objeto para lo cual no se requiere búsqueda de conformidad con la Regla 39 del PCT. Dado que las reivindicaciones son formuladas en términos de dicha materia objeto o simplemente especifican características comunes relacionadas con su implementación tecnológica - por ejemplo: sistema de computador, procesador, memoria, medios de entrada, . . . - , el examinador de la búsqueda no podría establecer ningún problema técnico que potencialmente requiriera superar un paso inventivo. Por lo tanto, no fue posible llevar a cabo una búsqueda significativa en el estado de la técnica (Art. 17(2)(a)(i) y (ii) PCT; ver Lineamientos de Búsqueda Internacional del PCT, Capítulo VIII, ítems 1 a 3).

Se atrae la atención del solicitante al hecho de que no es necesario que las reivindicaciones relacionadas con invenciones respecto de las cuales no se ha establecido ningún reporte de búsqueda internacional sean el sujeto de un examen preliminar internacional (Regla 66.1(e) PCT). Se le notifica al solicitante que la política de la EPO al actuar como una Autoridad de Examen Preliminar Internacional normalmente no es llevar a cabo un examen preliminar en asuntos que no se han buscado. Este es el caso prescindiendo de si las reivindicaciones han sido enmendadas siguiendo el recibo del reporte de búsqueda o durante cualquier procedimiento del Capítulo II. Si la solicitud procede a la fase regional ante la EPO, se le recuerda al solicitante que puede llevarse a cabo una búsqueda durante el examen ante la EPO (ver Lineamientos de la EPO C-VI, 8.5), si se superan los problemas que llevaron a la declaración del Artículo 17(2).

PATENT COOPERATION TREATY

RECEIVED

SEP 02 2003

ROSENTHAL & OSHA L.L.P.

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

NOTIFICATION OF TRANSMITTAL OF
THE INTERNATIONAL SEARCH REPORT
OR THE DECLARATION

(PCT Rule 44.1)

To:

ROSENTHAL & OSHA L.L.P.
Attn. Rosenthal, Alan D.
1221 McKinney Street
Suite 2800
Houston, Texas 77010
UNITED STATES OF AMERICADate of mailing
(day/month/year) 26/08/2003

Applicant's or agent's file reference

09469/008W01

FOR FURTHER ACTION See paragraphs 1 and 4 below

International application No.

PCT/US 03/13298

International filing date
(day/month/year)

28/04/2003

Applicant

SCHLUMBERGER OMNES, INC.

- 1.
- ☐
- The applicant is hereby notified that the International Search Report has been established and is transmitted herewith.

Filing of amendments and statement under Article 19:

The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 48):

When? The time limit for filing such amendments is normally 2 months from the date of transmittal of the International Search Report; however, for more details, see the notes on the accompanying sheet. *Previously received*Where? Directly to the International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Facsimile No.: (41-22) 740.14.35

For more detailed instructions, see the notes on the accompanying sheet.

Action *Demand in chapter 2*
Base Date: *4/28/02*
Due Date: *11/29/03*
Deadline: *11/29/03*
Initial: *SR*

- 2.
- ☒
- The applicant is hereby notified that no International Search Report will be established and the declaration under Article 17(2)(a) to that effect is transmitted herewith.

- 3.
- ☐
- With regard to the protest against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. Further action(s): The applicant is reminded of the following:

Shortly after 18 months from the priority date, the International application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the International application, or of the priority claim, must reach the International Bureau as provided in Rules 80bis.1 and 80bis.3, respectively, before the completion of the technical preparations for International publication.

Within 18 months from the priority date, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later).

Within 30 months from the priority date, the applicant must perform the prescribed acts for entry into the national phase before all designated Offices which have not been elected in the demand or in a later election within 18 months from the priority date or could not be elected because they are not bound by Chapter II.

Name and mailing address of the International Searching Authority

European Patent Office, P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 851 epo nl,
Fax: (+31-70) 340-3018

Authorized officer

Jacinta Reddy

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under article 18. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the PCT Applicant's Guide, a publication of WIPO.

In these Notes, "Article", "Rule", and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the letter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only.

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When?

Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 48.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 48.2).

Where a demand for international preliminary examination has been/is filed, see below.

How?

Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Administrative Instructions, Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 18(1)" (see below, under "Statement under Article 18(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

NOTES TO FORM PCT/ISA/220 (continued)

The letter must indicate the differences between the claims as filed and the claims as amended. It must, in particular, indicate, in connection with each claim appearing in the international application (it being understood that identical indications concerning several claims may be grouped), whether

- (i) the claim is unchanged;
- (ii) the claim is cancelled;
- (iii) the claim is new;
- (iv) the claim replaces one or more claims as filed;
- (v) the claim is the result of the division of a claim as filed.

The following examples illustrate the manner in which amendments must be explained in the accompanying letter:

1. [Where originally there were 48 claims and after amendment of some claims there are 51]:
"Claims 1 to 29, 31, 32, 34, 35, 37 to 48 replaced by amended claims bearing the same numbers; claims 30, 33 and 36 unchanged; new claims 49 to 51 added."
2. [Where originally there were 15 claims and after amendment of all claims there are 11]:
"Claims 1 to 15 replaced by amended claims 1 to 11."
3. [Where originally there were 14 claims and the amendments consist in cancelling some claims and in adding new claims]:
"Claims 1 to 6 and 14 unchanged; claims 7 to 13 cancelled; new claims 15, 16 and 17 added." or
"Claims 7 to 13 cancelled; new claims 15, 16 and 17 added; all other claims unchanged."
4. [Where various kinds of amendments are made]:
"Claims 1-10 unchanged; claims 11 to 13, 16 and 18 cancelled; claims 14, 15 and 16 replaced by amended claim 14; claim 17 subdivided into amended claims 15, 16 and 17; new claims 20 and 21 added."

"Statement under article 18(1)" (Rule 46.4)

The amendments may be accompanied by a statement explaining the amendments and indicating any impact that such amendments might have on the description and the drawings (which cannot be amended under Article 18(1)).

The statement will be published with the international application and the amended claims.

It must be in the language in which the international application is to be published.

It must be brief, not exceeding 500 words if in English or if translated into English.

It should not be confused with and does not replace the letter indicating the differences between the claims as filed and as amended. It must be filed on a separate sheet and must be identified as such by a heading, preferably by using the words "Statement under Article 18(1)".

It may not contain any disparaging comments on the international search report or the relevance of citations contained in that report. Reference to citations, relevant to a given claim, contained in the international search report may be made only in connection with an amendment of that claim.

Consequence if a demand for international preliminary examination has already been filed

If, at the time of filing any amendments and any accompanying statement, under Article 18, a demand for international preliminary examination has already been submitted, the applicant must preferably, at the time of filing the amendments (and any statement) with the International Bureau, also file with the International Preliminary Examining Authority a copy of such amendments (and of any statement) and, where required, a translation of such amendments for the procedure before that Authority (see Rules 55.3(a) and 62.2, first sentence). For further information, see the Notice to the demand form (PCT/IPEA401).

Consequence with regard to translation of the international application for entry into the national phase

The applicant's attention is drawn to the fact that, upon entry into the national phase, a translation of the claims as amended under Article 18 may have to be furnished to the designated/elected Offices, instead of, or in addition to, the translation of the claims as filed.

For further details on the requirements of each designated/elected Office, see Volume II of the PCT Applicant's Guide.

PATENT COOPERATION TREATY

PCT

DECLARATION OF NON-ESTABLISHMENT OF INTERNATIONAL SEARCH REPORT

(PCT Article 17(2)(a), Rules 13ter.1(c) and Rule 39)

Applicant's or agent's file reference 09469/008W01	IMPORTANT DECLARATION	Date of mailing (day/month/year) 26/08/2003
International application No. PCT/US 03/13298	International filing date (day/month/year) 28/04/2003	(Earliest) Priority date (day/month/year) 29/04/2002
International Patent Classification (IPC) or both national classification and IPC G06F17/60		
Applicant SCHLUMBERGER OMNES, INC.		

This International Searching Authority hereby declares, according to Article 17(2)(a), that no international search report will be established on the international application for the reasons indicated below

1. ☒ The subject matter of the international application relates to:
 - a. ☐ scientific theories.
 - b. ☐ mathematical theories
 - c. ☐ plant varieties.
 - d. ☐ animal varieties.
 - e. ☐ essentially biological processes for the production of plants and animals, other than microbiological processes and the products of such processes.
 - f. ☒ schemes, rules or methods of doing business.
 - g. ☐ schemes, rules or methods of performing purely mental acts.
 - h. ☐ schemes, rules or methods of playing games.
 - i. ☐ methods for treatment of the human body by surgery or therapy.
 - j. ☐ methods for treatment of the animal body by surgery or therapy.
 - k. ☐ diagnostic methods practised on the human or animal body.
 - l. ☐ mere presentations of information.
 - m. ☐ computer programs for which this International Searching Authority is not equipped to search prior art.
2. ☐ The failure of the following parts of the international application to comply with prescribed requirements prevents a meaningful search from being carried out:

☐ the description
☒ the claims
☐ the drawings
3. ☐ The failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions prevents a meaningful search from being carried out:

☐ the written form has not been furnished or does not comply with the standard.
☐ the computer readable form has not been furnished or does not comply with the standard.
4. Further comments: **SEE FURTHER INFORMATION SHEET**

Name and mailing address of the International Searching Authority  European Patent Office, P.B. 6816 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fac. (+31-70) 340-3016	Authorized officer Jacinta Reddy
--	--

Form PCT/ISA/203 (July 1998)

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 283

The claims relate to subject matter for which no search is required according to Rule 39 PCT. Given that the claims are formulated in terms of such subject matter or merely specify commonplace features relating to its technological implementation - for example: computer system, processor, memory, input means, ... - , the search examiner could not establish any technical problem which might potentially have required an inventive step to overcome. Hence it was not possible to carry out a meaningful search into the state of the art (Art. 17(2)(a)(i) and (ii) PCT; see PCT International Search Guidelines, Chapter VIII, items 1 to 3).

The applicant's attention is drawn to the fact that claims relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure. If the application proceeds into the regional phase before the EPO, the applicant is reminded that a search may be carried out during examination before the EPO (see EPO Guideline C-VI, 8.5), should the problems which led to the Article 17(2) declaration be overcome.

(12) SOLICITUD INTERNACIONAL PUBLICADA SEGÚN EL TRATADO DE COOPERACION DE PATENTES (PCT)

(19) Organización Mundial de Propiedad Intelectual
Oficina Internacional



(43) Fecha de Publicación

13 de Noviembre de 2003 (13.11.2003)

PCT

(10) Número de Publicación Internacional

WO 2003/093960 A2

(51) Clasificación Internacional de Patentes⁷: G06F 1/00

(21) Número de Solicitud Internacional: PCT/US2003/013298

(22) Fecha de Registro Internacional: 28 de Abril de 2003
(28.04.2003)

(25) Idioma de registro: INGLES

(26) Idioma de Publicación: INGLES

(30) Información de Prioridad:
10/134,815 29 de Abril 2002 (29.04.2002) US

(71) Solicitante: SCHLUMBERGER OMNES, INC. [US/US];
Suite 400, 5599 San Felipe, Houston, TX 77056 (US).

(72) Inventores: BAUDOIN, Claude R.; 2319 McDuffie Street,
Houston, TX 77019-6527 (US). ELLIOTT, Collin, R.; 1st
Floor Flat, 12 Weatherby Gardens, London SW5 0JW (GB).

(74) Agente: ROSENTHAL, Alan, D. et al.; Rosenthal & Osha
L.L.P., Suite 2800, 1221 McKinney Street, Houston, TX
77010 (US).

(81) Estados Designados (nacionales): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,
DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR,
HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT,
LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM,
PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR,
TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Estados Designados (regionales): patente ARIPO (GH,
GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),
patente euroasiática (AM, AZ, BY, KG, KZ, MD, RU, TJ,
TM) patente europea (AT, BE, BG, CH, CY, CZ, DE,
DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL,
PT, RO, SE, SI, SK, TR) patente OAPI (BF, BJ, CF, CG,
CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaraciones bajo la Regla 4.17:

- en cuanto al derecho del solicitante de solicitar y que se le otorgue una patente (Regla 4.17(ii)) para todas las designaciones.
- en cuanto al derecho del solicitante a reivindicar la prioridad de la solicitud anterior (Regla 4.17(iii)) para todas las designaciones.

Publicado:

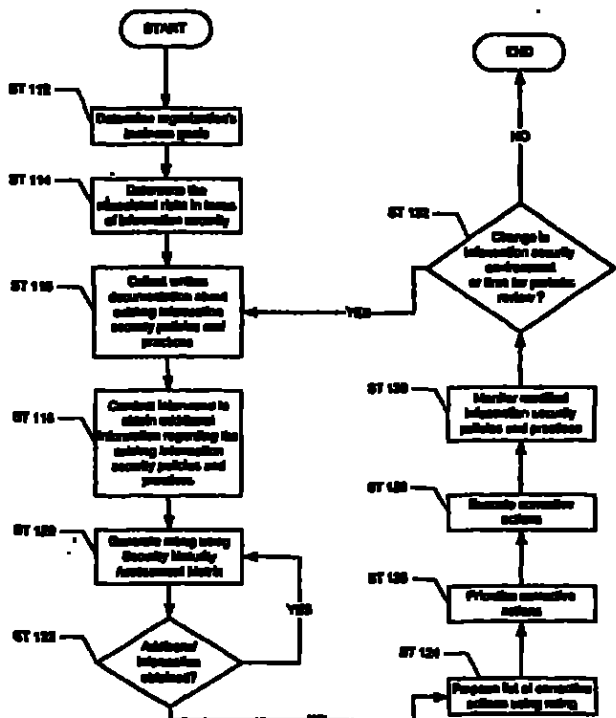
- sin reporte de búsqueda internacional y para ser publicado con la presentación de este reporte.

(48) Fecha de la publicación correcta de esta versión:
21 de Mayo de 2004

(15) Información acerca de la corrección:
ver gaceta PCT No. 21/2004 de 21 de Mayo de 2004,
Sección II

Para los códigos de dos letras y otras abreviaturas,
refiérase a "Las Notas Guías sobre Códigos y
Abreviaturas" que aparecen al comienzo de cada
emisión regular de la Gaceta PCT.

(54) Título: "MÉTODO PARA EVALUACIÓN DE MADUREZ DE SEGURIDAD"



(57) Resumen: Un método para evaluar la política y práctica de seguridad de la información en una organización, incluyendo la determinación del riesgo asociado con la política y práctica de seguridad de la información, recogiendo información acerca de la política y práctica de seguridad de la información, generando una clasificación usando una matriz de evaluación de maduración de la seguridad, la información obtenida y el riesgo asociado con la política y práctica de seguridad de la información, generando una lista de acciones correctivas usando la clasificación, ejecutando la lista de acciones correctivas para crear una nueva política y práctica de seguridad de la información y monitorear la nueva política y práctica de seguridad de la información.

CORRECTED VERSION

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
13 November 2003 (13.11.2003)

PCT

(10) International Publication Number
WO 2003/093960 A2

(51) International Patent Classification: G06F 1/00

R.; 1st Floor Flat, 12 Weatherby Gardens, London SW5
0JW (GB).

(21) International Application Number:
PCT/US2003/013298

(74) Agents: ROSENTHAL, Alan, D. et al.; Rosenthal & Osha
L.L.P., Suite 2800, 1221 McKinney Street, Houston, TX
77010 (US).

(22) International Filing Date: 28 April 2003 (28.04.2003)

(25) Filing Language: English

(81) Designated States (national): AE, AG, AL, AM, AT, AU,
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,
CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GH, GI,
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,
LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,
MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE,
SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC,
VN, YU, ZA, ZM, ZW.

(26) Publication Language: English

(30) Priority Data:
10/134,815 29 April 2002 (29.04.2002) US

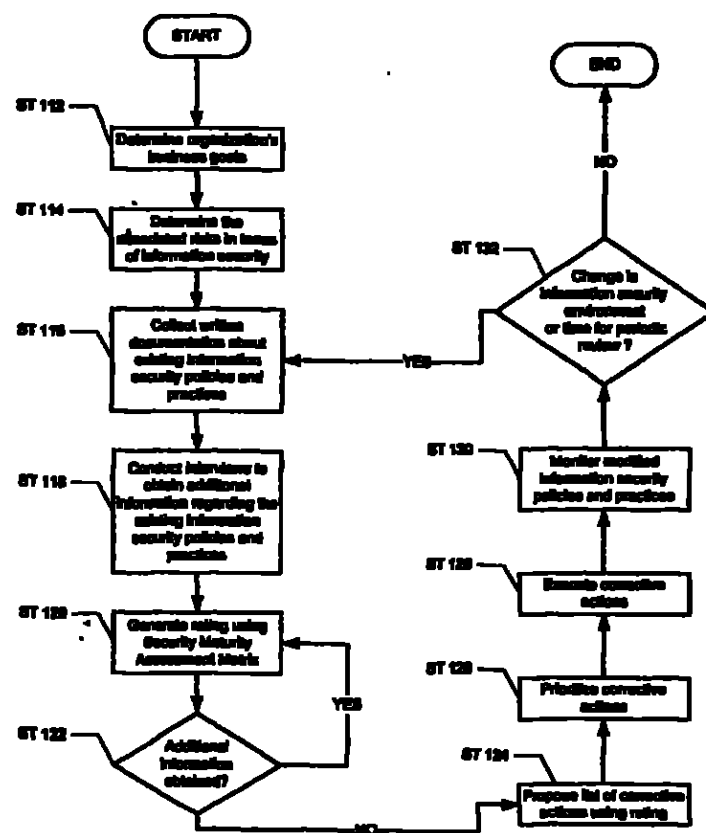
(71) Applicant: SCHLUMBERGER OMNES, INC.
[US/US]; Suite 400, 5599 San Felipe, Houston, TX 77056
(US).

(72) Inventors: BAUDOUIN, Claude, R.; 2319 McDuffie
Street, Houston, TX 77019-6527 (US). ELLIOTT, Colin,

(84) Designated States (regional): ARIPO patent (GH, GM,
KE, LS, MW, MZ, SD, SI, SZ, TZ, UG, ZM, ZW),
European patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: SECURITY MATURITY ASSESSMENT METHOD



(57) Abstract: A method for assessing an information security policy and practice of an organization, including determining a risk associated with the information security policy and practice, collecting information about the information security policy and practice, generating a rating using a security maturity assessment matrix, the collected information, and the risk associated with the information security policy and practice, generating a list of corrective action using the rating, executing the list of corrective actions to create a new security information policy and practice, and monitoring the new security information policy and practice.

WO 2003/093960 A2



European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished upon receipt of that report

(48) Date of publication of this corrected version:

21 May 2004

Declarations under Rule 4.17:

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for all designations
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations

(15) Information about Correction:

see PCT Gazette No. 21/2004 of 21 May 2004, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

PCT

De la OFICINA INTERNACIONAL

**NOTIFICACION DE REGISTRO
DE UN CAMBIO**

(Regla 92 bis. 1 del PCT e
Instrucciones Administrativas, Sección 422)

Fecha de envío por correo (día/mes/año) 23 de Diciembre de 2003 (23.12.2003)
Archivo de referencia del solicitante o agente 09469/008WO1
Solicitud Internacional No. PCT/US03/13298

Para:

ROSENTHAL, Alan, D.
Rosenthal & Osha L.L.P.
Suite 2800
1221 McKinney Street
Houston, TX 77010
Estados Unidos de América

NOTIFICACION IMPORTANTE

Fecha de registro internacional (día/mes/año)
28 de Abril de 2003 (28.04.03)

1. Las siguientes indicaciones aparecieron en el registro en relación con:

☐ el solicitante ☒ el inventor ☐ el agente ☐ el representante común

Nombre y Dirección BAUDON, Claude, R.	País de Nacionalidad	País de Residencia
	No. Teléfono	
	No. Facsímil	
	No. Teleprinter	

2. La Oficina Internacional por el presente notifica al solicitante que el siguiente cambio se ha registrado en relación con:

☐ la persona ☒ el nombre ☐ la dirección ☐ la nacionalidad ☐ la residencia

Nombre y Dirección BAUDOIN, Claude, R.	País de Nacionalidad	País de Residencia
	No. Teléfono	
	No. Facsímil	
	No. Teleprinter	

3. Otras observaciones, si fuese necesario:

4. Se ha enviado una copia de esta notificación a:

☒ la Oficina que recibe ☒ las Oficinas designadas relacionadas
☐ la Autoridad de Búsqueda Internacional ☐ las Oficinas seleccionadas relacionadas
☐ la Autoridad de Examen Preliminar Internacional ☐ otros:

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsímil No.: (41-22) 338.70.90	Funcionario autorizado Sun LEE Teléfono No.: (41-22) 338 8710
--	---

51
14

PCT

NOTIFICATION OF THE RECORDING
OF A CHANGE
(PCT Rule 92bis.1 and
Administrative Instructions, Section 422)

From the INTERNATIONAL BUREAU

To:

ROSENTHAL, Alan, D.
Rosenthal & Osha L.L.P.
Suite 2800
1221 McKinney Street
Houston, TX 77010
United States of America

Date of mailing (day/month/year)
23 December 2003 (23.12.03)

Applicant's or agent's file reference
09469/008WO1

International application No.
PCT/US03/13298

International filing date (day/month/year)
28 April 2003 (28.04.03)

IMPORTANT NOTIFICATION

1. The following indications appeared on record concerning:

☐ the applicant ☒ the inventor ☐ the agent ☐ the common representative

Name and Address
BAUDON, Claude, R.

EPO - DG 1

02.01.2004

(104)

State of Nationality

State of Residence

Telephone No.

Facsimile No.

Teleprinter No.

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

☐ the person ☒ the name ☐ the address ☐ the nationality ☐ the residence

Name and Address
BAUDOIN, Claude, R.

State of Nationality

State of Residence

Telephone No.

Facsimile No.

Teleprinter No.

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

☒ the receiving Office ☒ the designated Offices concerned
☐ the International Searching Authority ☐ the elected Offices concerned
☐ the International Preliminary Examining Authority ☐ other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Authorized officer

Sun LEE

Facsimile No. (41-22) 338-70-80

Telephone No. (41-22) 338 8710

17

TRATADO DE COOPERACION DE PATENTES

PCT

De la OFICINA INTERNACIONAL

**NOTIFICACION DE REGISTRO
DE UN CAMBIO**

(Regla 92 bis. 1 del PCT e
Instrucciones Administrativas, Sección 422)

Para:

ROSENTHAL, Alan, D.
Osha & May L.L.P.
Suite 2800
1221 McKinney Street
Houston, TX 77010
Estados Unidos de América

Fecha de envío por correo (día/mes/año)
04 de Junio de 2004 (04.06.2004)

Archivo de referencia del solicitante o agente
09469/008WO1

NOTIFICACION IMPORTANTE

Solicitud Internacional No.
PCT/US2003/013298

Fecha de registro internacional (día/mes/año)
28 de Abril de 2003 (28.04.03)

1. Las siguientes indicaciones aparecieron en el registro en relación con:

☐ el solicitante ☐ el inventor ☒ el agente ☐ el representante común

Nombre y Dirección
ROSENTHAL, Alan, D.
Osha Novak & May L.L.P.
Suite 2800
1221 McKinney Street
Houston, TX 77010
Estados Unidos de América

País de Nacionalidad	País de Residencia
No. Teléfono (713) 228-8600	
No. Facsímile (713) 228-8778	
No. Teleprinter	

2. La Oficina Internacional por el presente notifica al solicitante que el siguiente cambio se ha registrado en relación con:

☐ la persona ☐ el nombre ☒ la dirección ☐ la nacionalidad ☐ la residencia

Nombre y Dirección
ROSENTHAL, Alan, D.
Osha & May L.L.P.
Suite 2800
1221 McKinney Street
Houston, TX 77010
Estados Unidos de América

País de Nacionalidad	País de Residencia
No. Teléfono (713) 228-8600	
No. Facsímile (713) 228-8778	
No. Teleprinter	

3. Otras observaciones, si fuese necesario:

4. Se ha enviado una copia de esta notificación a:

☒ la Oficina que recibe ☒ las Oficinas designadas relacionadas
☐ la Autoridad de Búsqueda Internacional ☐ las Oficinas seleccionadas relacionadas
☐ la Autoridad de Examen Preliminar Internacional ☐ otros:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsímile No.: (41-22) 338.70.90

Funcionario autorizado
KI-Nam HA

Teléfono No.: (41-22) 338 8031

PCT

From the INTERNATIONAL BUREAU

NOTIFICATION OF THE RECORDING
OF A CHANGE

(PCT Rule 92bis.1 and
Administrative Instructions, Section 422)

To:

ROSENTHAL, Alan, D.
Osha & May L.L.P.
Suite 2800
1221 McKinney Street
Houston, TX 77010
United States of America

Date of mailing (day/month/year) 04 June 2004 (04.06.2004)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference 09489/008WO1	
International application No. PCT/US2003/013298	International filing date (day/month/year) 28 April 2003 (28.04.2003)

1. The following indications appeared on record concerning: ☐ the applicant ☐ the inventor ☒ the agent ☐ the common representative								
Name and Address ROSENTHAL, Alan, D. Osha Novak & May L.L.P. Suite 2800 1221 McKinney Street Houston, TX 77010 United States of America	State of Nationality	State of Residence						
	Telephone No. (713) 228-8600							
	Facsimile No. (713) 228-8778							
	Teleprinter No.							
2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning: ☐ the person ☐ the name ☒ the address ☐ the nationality ☐ the residence								
Name and Address ROSENTHAL, Alan, D. Osha & May L.L.P. Suite 2800 1221 McKinney Street Houston, TX 77010 United States of America	State of Nationality	State of Residence						
	Telephone No. (713) 228-8600							
	Facsimile No. (713) 228-8778							
	Teleprinter No.							
3. Further observations, if necessary: EPO-DG 1 11 06 2004 37								
4. A copy of this notification has been sent to: <table><tr><td>☒ the receiving Office</td><td>☒ the designated Offices concerned</td></tr><tr><td>☐ the International Searching Authority</td><td>☐ the elected Offices concerned</td></tr><tr><td>☐ the International Preliminary Examining Authority</td><td>☐ other:</td></tr></table>			☒ the receiving Office	☒ the designated Offices concerned	☐ the International Searching Authority	☐ the elected Offices concerned	☐ the International Preliminary Examining Authority	☐ other:
☒ the receiving Office	☒ the designated Offices concerned							
☐ the International Searching Authority	☐ the elected Offices concerned							
☐ the International Preliminary Examining Authority	☐ other:							

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 28, Switzerland Facsimile No. (41-22) 338.70.90	Authorized officer KI-Nam HA Telephone No. (41-22) 338 8031
--	---

TRATADO DE COOPERACION DE PATENTES

PCT

De la OFICINA INTERNACIONAL

NOTIFICACION DE REGISTRO
DE UN CAMBIO

(Regla 92 bis. 1 del PCT e
Instrucciones Administrativas, Sección 422)

Para:

ROSENTHAL, Alan, D.
Osha Novak & May L.L.P.
Suite 2800
1221 McKinney Street
Houston, TX 77010
Estados Unidos de América

Fecha de envío por correo (día/mes/año)
28 de Mayo de 2004 (28.05.2004)

Archivo de referencia del solicitante o agente
09469/008WO1

NOTIFICACION IMPORTANTE

Solicitud Internacional No.
PCT/US2003/013298

Fecha de registro internacional (día/mes/año)
28 de Abril de 2003 (28.04.03)

1. Las siguientes indicaciones aparecieron en el registro en relación con:

☐ el solicitante ☐ el inventor ☒ el agente ☐ el representante común

Nombre y Dirección
ROSENTHAL, Alan, D.
Rosenthal & Osha L.L.P.
Suite 2800
1221 McKinney Street
Houston, TX 77010
Estados Unidos de América

País de Nacionalidad	País de Residencia
No. Teléfono (713) 228-8600	
No. Facsímile (713) 228-8778	
No. Teleprinter	

2. La Oficina Internacional por el presente notifica al solicitante que el siguiente cambio se ha registrado en relación con:

☐ la persona ☐ el nombre ☒ la dirección ☐ la nacionalidad ☐ la residencia

Nombre y Dirección
ROSENTHAL, Alan, D.
Osha Novak & May L.L.P.
Suite 2800
1221 McKinney Street
Houston, TX 77010
Estados Unidos de América

País de Nacionalidad	País de Residencia
No. Teléfono (713) 228-8600	
No. Facsímile (713) 228-8778	
No. Teleprinter	

3. Otras observaciones, si fuese necesario:

4. Se ha enviado una copia de esta notificación a:

☒ la Oficina que recibe	☒ las Oficinas designadas relacionadas
☐ la Autoridad de Búsqueda Internacional	☐ las Oficinas seleccionadas relacionadas
☐ la Autoridad de Examen Preliminar Internacional	☐ otros:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 338.70.90

Funcionario autorizado
Sun LEE

Teléfono No.: (41-22) 338 8710

Previously Docketed

PCT/US2003/013298

Action:	NA-2744	Docketing	30MC
Base Date:	4/29/02	Base Date:	4/29/02
Due Date:	7/29/04	Due Date:	10/29/04
Deadline:	7/29/04	Deadline:	10/29/04
Initials:	bb	Initials:	PCT
Atty/Buc. Initials:		Atty/Buc. Initials:	

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

RECEIVED
JUN 09 2004

OSHA & MAY LLP.

ROSENTHAL, Alan, D.
Osha Novak & May L.L.P.
Suite 2800
1221 McKinney Street
Houston, TX 77010
United States of America

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and
Administrative Instructions, Section 422)

Date of mailing (day/month/year) 26 May 2004 (26.05.2004)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference 09469/008WO1	
International application No. PCT/US2003/013298	International filing date (day/month/year) 28 April 2003 (28.04.2003)

1. The following indications appeared on record concerning:

☐ the applicant ☐ the inventor ☒ the agent ☐ the common representative

Name and Address

ROSENTHAL, Alan, D.
Rosenthal & Osha L.L.P.
Suite 2800
1221 McKinney Street
Houston, TX 77010
United States of America

State of Nationality

State of Residence

Telephone No.

(713) 228-8600

Facsimile No.

(713) 228-8778

Teleprinter No.

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

☐ the person ☐ the name ☒ the address ☐ the nationality ☐ the residence

Name and Address

ROSENTHAL, Alan, D.
Osha Novak & May L.L.P.
Suite 2800
1221 McKinney Street
Houston, TX 77010
United States of America

State of Nationality

State of Residence

Telephone No.

(713) 228-8600

Facsimile No.

(713) 228-8778

Teleprinter No.

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

☒ the receiving Office ☒ the designated Offices concerned
☐ the International Searching Authority ☐ the elected Offices concerned
☐ the International Preliminary Examining Authority ☐ other:

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Sun LEE
Facsimile No. (41-22) 338.70.90	Telephone No. (41-22) 338.8710

Form PCT/IB/308 (March 1994)

008298427

**CAPITULO REIVINDICATORIO COMO FUE
ORIGINALMENTE PRESENTADO EN FASE
INTERNACIONAL JUNTO CON SU
TRADUCCION**

Claims

- [c1] A method for assessing an information security policy and practice of an organization, comprising:
determining a risk associated with the information security policy and practice;
collecting information about the information security policy and practice;
generating a rating using a security maturity assessment matrix, the collected information, and the risk associated with the information security policy and practice;
generating a list of corrective actions using the rating;
executing the list of corrective actions to create a new security information policy and practice; and
monitoring the new security information policy and practice.
- [c2] The method of claim 1, further comprising:
generating a new rating using the security capability assessment matrix when there is a change in an information security environment of the organization.
- [c3] The method of claim 1, further comprising:
generating a graphical assessment of the rating.
- [c4] The method of claim 3, wherein the graphical assessment of the rating is generated by a security maturity assessment reporting tool.
- [c5] The method of claim 4, wherein the security maturity assessment reporting tool comprises functionality to track the rating of the security information policy and practice over time.
- [c6] The method of claim 4, wherein the security maturity assessment reporting tool comprises functionality to graphically compare the rating to a rating goal.

- 21
- [c7] The method of claim 1, the collecting information comprising collection of documentation detailing the information security policy and practice of the organization.
- [c8] The method of claim 1, the security assessment matrix comprising a matrix in which each of a plurality of columns denote a maturity level and each of a plurality of rows denote a particular information security feature such that the intersection of one of the plurality of columns with one of the plurality of rows is a capability maturity level.
- [c9] The method of claim 8, wherein each of the plurality of rows is a grouping of British Standards Institution 7799 items.
- [c10] The method of claim 8, wherein each of the plurality of rows is a grouping of a set of controls outlining best mode practices in information security.
- [c11] The method of claim 8, wherein each of the plurality of rows is a grouping of International Organization for Standardization 17799 items.
- [c12] The method of claim 8, wherein each of the plurality of columns is a maturity level defined in accordance with the Capability Maturity Model of the Software Engineering Institute.
- [c13] The method of claim 9, the grouping of British Standards Institution 7799 items comprising a British Standards Institution 7799 category.
- [c14] The method of claim 11, the grouping of International Organization for Standardization 17799 items comprising an International Organization for Standardization 17799 category.
- [c15] The method of claim 1, the generating the list of corrective actions comprising comparing a description of a current maturity level of an organization for each of a plurality of information security items in the security assessment matrix
- 24

with a description of a desired maturity level for each of the plurality of information security items.

[c16] An apparatus for assessing an information security policy and practice of an organization, comprising:

means for determining a risk associated with the information security policy and practice;

means for collecting information about the information security policy and practice;

means for generating a rating using a security maturity assessment matrix, the collected information, and the risk associated with the information security policy and practice;

means for generating a list of corrective actions using the rating;

means for executing the list of corrective actions to create a new security information policy; and

means for monitoring the new security information policy.

[c17] The apparatus of claim 16, further comprising:

means for generating a new rating using the security maturity assessment matrix if there is a change in the information security environment of the organization.

[c18] A computer system for assessing an information security policy and practice of an organization, comprising:

a processor;

a memory;

an input means; and

software instructions stored in the memory for enabling the computer system under control of the processor, to perform:

determining a risk associated with the information security policy and practice;

collecting information about the information security policy and practice
using the input means;
generating a rating using a *security maturity assessment matrix*, the
collected information, and the risk associated with the
information security policy and practice;
generating a list of corrective actions using the rating;
executing the list of corrective actions to create a new security
information policy and practice; and
monitoring the new security information policy and practice.

[c19] The computer system of claim 18, further comprising:

software instructions to perform generating a new rating using the security
maturity assessment matrix if there is a change in the information
security environment of the organization.

REIVINDICACIONES

1. Un método para estimar o evaluar una política y práctica de seguridad de información de una organización, caracterizado porque comprende: determinar un
5 riesgo asociado con la política y práctica de seguridad de información; capturar información respecto a la política y práctica de seguridad de información; generar una calificación utilizando una matriz de evaluación de madurez de seguridad, la información capturada y el riesgo
10 asociado con la política y práctica de seguridad de información; generar una lista de acciones correctivas utilizando la calificación; ejecutar la lista de acciones correctivas para crear una nueva política y práctica de información de seguridad; y supervisar la nueva política
15 y práctica de información de seguridad.

2. El método de conformidad con la reivindicación 1, caracterizado porque además comprende: generar una nueva calificación utilizando la matriz de evaluación de capacidad de seguridad, cuando hay un cambio en un
20 biente de seguridad de información de la organización.

3. El método de conformidad con la reivindicación 1, caracterizado porque además comprende generar una evaluación gráfica de la calificación.

4. El método de conformidad con la reivindicación 3, caracterizado porque la evaluación gráfica de la calificación se genera por una herramienta para reporte de evaluación de madurez de seguridad.

5 5. El método de conformidad con la reivindicación 4, caracterizado porque la herramienta para reporte de evaluación de madurez de seguridad comprende funcionalidad para dar seguimiento a la calificación de la política y práctica de información de seguridad con el tiempo.
10 po.

6. El método de conformidad con la reivindicación 4, caracterizado porque la herramienta para reporte de evaluación de madurez de seguridad comprende funcionalidad para comparar gráficamente la calificación con una
15 meta de calificación.

7. El método de conformidad con la reivindicación 1, caracterizado porque la recolección de información comprende recolectar documentación que detalla la política y práctica de seguridad de información de la organización.
20

8. El método de conformidad con la reivindicación 1, caracterizado porque la matriz de evaluación de seguridad comprende una matriz en donde cada una de una pluralidad de columnas denota un nivel de madurez y cada
25 una de una pluralidad de hileras denota una característi-

ca de seguridad de información particular de manera tal que la intersección de una de la pluralidad de columnas con una pluralidad de hileras es un nivel de madurez de capacidad.

- 5 9. El método de conformidad con la reivindicación 8, caracterizado porque cada una de la pluralidad de hileras es un agrupamiento de los ítems de la Institución de Normas Británica 7799 (British Standard Institution 7799).
- 10 10. El método de conformidad con la reivindicación 8, caracterizado porque cada uno de la pluralidad de hileras es un agrupamiento de un conjunto de controles que establecen las prácticas de mejor modo en seguridad de información.
- 15 11. El método de conformidad con la reivindicación 8, caracterizado porque cada uno de la pluralidad de hileras es un agrupamiento de los ítems de la Organización Internacional para Normalización 17799 (International Organization for Standardization 17799).
- 20 12. El método de conformidad con la reivindicación 8, caracterizado porque cada una de la pluralidad de columnas es un nivel de madurez definido de acuerdo con el Modelo de Madurez de Capacidad (Capability Maturity Model) del Instituto de Ingeniería de Soporte Lógico
- 25 (Software Engineering Institute).

27

13. El método de conformidad con la reivindicación 9, caracterizado porque el agrupamiento de los ítems de la Institución de Normas Británica 7799 (British Standard Institution 7799) comprende una categoría de la
5 Institución de Normas Británica 7799 (British Standard Institution 7799).

14. El método de conformidad con la reivindicación 11, caracterizado porque el agrupamiento de los ítems de la Organización Internacional para Normalización
10 17799 (International Organization for Standardization 17799) comprende una categoría de la Organización Internacional para Normalización 17799 (International Organization for Standardization 17799).

15. El método de conformidad con la reivindicación 1, caracterizado porque generar la lista de acciones correctivas, comprende comparar una exclusión de un nivel de madurez actual de una organización por cada uno de una pluralidad de ítems de seguridad de información en la matriz de evaluación de seguridad, con una descripción
20 de un nivel de madurez deseado por cada uno de la pluralidad de ítems de seguridad de información.

16. Un aparato para estimar una política y práctica de seguridad de información de una organización, caracterizado porque comprende: medios para determinar un
25 riesgo asociado con la política y práctica de seguridad

30

de información; medios para recolectar información respecto a la política y práctica de seguridad de información; medios para generar una calificación utilizando una matriz de evaluación de madurez de seguridad, la información recolectada y el riesgo asociado con la política y práctica de seguridad de información; medios para generar una lista de acciones correctivas utilizando la calificación; medios para ejecutar la lista de acciones correctivas para crear una nueva política de información de seguridad; y medios para supervisar la nueva política de información de seguridad.

17. El aparato de conformidad con la reivindicación 16, caracterizado porque además comprende: medios para generar una nueva calificación utilizando la matriz de evaluación de madurez de seguridad si hay un cambio en el ambiente de seguridad de información de la organización.

18. Un sistema de computadora para estimar una política y práctica de seguridad de información de una organización, caracterizado porque comprende: un procesador; una memoria; medios de alimentación; e instrucciones de soporte lógico almacenadas en la memoria para permitir que el sistema de computadoras bajo el control del procesador, realice: determinar un riesgo asociado con la política y práctica de seguridad de información; recolectar

información respecto a la política y práctica de seguridad de información utilizando los medios de alimentación; generar una calificación utilizando una matriz de evaluación de madurez de seguridad, la información recolectada y el riesgo asociado con la política y práctica de seguridad de información; generar una lista de acciones correctivas utilizando la calificación; ejecutar la lista de acciones correctivas para crear nuevas política y práctica de información de seguridad; y supervisar las nuevas política y práctica de información de seguridad.

19. El sistema de computadora de conformidad con la reivindicación 18, caracterizado porque además comprende instrucciones de soporte lógico para realizar la generación de una nueva calificación utilizando la matriz de evaluación de madurez de seguridad si hay un cambio en el ambiente de seguridad de información de la organización.

ANEXO EXPLICATIVO DE MODIFICACIONES A LAS REIVINDICACIONES

En ejercicio del derecho conferido por el Artículo 28 numeral 1 del Tratado de Cooperación en materia de Patentes PCT, atentamente me permito Informar a ese Despacho que el capítulo reivindicatorio tal como fue presentado originalmente en Fase Internacional ha sido modificado.

Las modificaciones realizadas se encuentran plenamente sustentadas en la descripción de la presente Invención y en este sentido, no configuran una ampliación del invento o de la divulgación contenida en la solicitud presentada.

MÉTODO PARA EVALUACIÓN DE MADUREZ DE SEGURIDAD

RESUMEN-OBJETO Y FINALIDAD DE LA INVENCION

5 Un método para estimar política y práctica de
seguridad de información de una organización, que incluye
determinar un riesgo asociado con la política y práctica
de seguridad de información, recolectar información res-
pecto a la política y práctica de seguridad de informa-
10 ción, generar una calificación utilizando una matriz de
evaluación de una madurez de seguridad, la información
recolectada y el riesgo asociado con la política y prác-
tica de seguridad de información, generar una lista de
acciones correctivas utilizando la calificación, ejecutar
15 la lista de acciones correctivas para crear unas nuevas
política y práctica de información de seguridad y super-
visar las nuevas política y práctica de información de
seguridad.

20

25

MÉTOD PARA EVALUACIÓN DE MADUREZ DE SEGURIDAD

ANTECEDENTES DE LA INVENCION

[0001] La seguridad de información abarca la protección de información contra descripción, transferencia, modificación o destrucción, no autorizadas, ya sea
5 accidentales o intencionales. La seguridad de información se ha vuelto una consideración predominante para organizaciones, como resultado de las tendencias hacia el comercio electrónico, los negocios electrónicos, el acceso a la red y correo electrónico por la red y correo
10 electrónico universal, y explotaciones de seguridad bien publicadas. Como resultado, las organizaciones intentan aplicar principios de seguridad de información en un marco pragmático.

15 [0002] Para permitir a las organizaciones aplicar principios de seguridad de información en un marco pragmático, se han desarrollado una cantidad de normas y herramientas de información. Una norma ampliamente reconocida, BS7799/ISO17799, se desarrolló por la Institu-
20 ción de Normas Británica (BSI = British Standards Institution) y adoptó por la Organización Internacional para Estandarización (ISO = International Organization for Standardization). La norma BS7799/ISO17799 es un conjunto completo o extenso de controles que establecen las
25 prácticas de mejor modo en seguridad de información. El

objetivo de BS7799/ISO17799 es servir como un solo punto de referencia para determinar la apropiada política de seguridad de información para una variedad de sistemas de organizaciones. La norma BS7799/ISO17799 incluye 10 secciones, cada una que está dirigida a un área específica de seguridad de información. Ver, "ISO17799 Security Standard: ISO 17799 Compliance & Positioning" (Norma de seguridad ISO17799: Cumplimiento y ubicación ISO 17799) <http://www.securityauditor.net/iso17799/>.

10 [0003] El proceso de manejar el cumplimiento con BS7799/ISO17799 no es una tarea trivial. Como resultado, una cantidad de productos de administración de riesgo y análisis de riesgo, se han desarrollado para ayudar a organizaciones a cumplir con la norma

15 BS7799/ISO17799. Un producto es COBRA, que fue desarrollado por C & A Systems, Inc. COBRA se utiliza para semi-automatizar el proceso de evaluación. COBRA utiliza una serie de cuestionarios en línea para obtener información respecto a la política de seguridad actual. Utili-

20 zando las respuestas a partir de los cuestionarios, COBRA crea reportes que proporcionan información respecto a la posición de cumplimiento actual de la organización, en una base de pasa/falla, con respecto a cada sección de la norma BS7799/ISO17799.

[0004] Otra herramienta que se ha desarrollado para permitir a organizaciones aplicar principios de seguridad de información en un marco pragmático, es el modelo de Madurez de Capacidad en Ingeniería de Seguridad de Sistemas (SSE-CMM = Systems Security Engineering Capability Maturity Model). El SSE-CMM se deriva de conceptos del modelo de madurez de capacidad del Instituto de Ingeniería de Soporte Lógico (SEI = Software Engineering Institute) inicialmente creado para desarrollos de soporte lógico. SSE-CMM describe las características esenciales de un proceso de ingeniería en seguridad de organización que debe existir para asegurar buena ingeniería de seguridad. SSE-CMM no determina o receta un proceso o norma tal como BS7799/ISO17799, sino más bien utiliza un modelo que captura prácticas generalmente observadas en la industria. Adicionalmente, SSE-CMM se basa en un modelo de madurez que define metas específicas y prácticas para todo el ciclo de vida de una organización. Además, SSE-CMM define un proceso y reglas de evaluación total para ingeniería de seguridad dentro de una organización. Ver "System Security Engineering Capability Maturity Model-Model & Appraisal Method Summary April 1999," (Método de Evaluación y Modelo- modelo de madurez de capacidad de Ingeniería de Seguridad de Sistemas, compendio abril 1999) <http://www.sse-cmm.org/>. La evaluación resultante

obtenida de aplicar SSE-CCM típicamente no se asocia con una herramienta de reporte para el nivel de madurez.

COMPENDIO DE LA INVENCION

[0005] En general, en un aspecto, la invención
5 se refiere a un método para evaluar una política y práctica de seguridad de información de una organización, que comprende determinar un riesgo asociado con la práctica y política de seguridad de información, capturar información respecto a la práctica y política de seguridad de
10 información, generar una calificación utilizando una matriz de evaluación de madurez de seguridad, la información capturada, y el riesgo asociado con la práctica y política de seguridad de información, generar una lista de acciones correctivas utilizando la calificación, ejecutar la lista de acciones correctivas para crear una
15 nueva política y práctica de información de seguridad, y supervisar las nuevas políticas y prácticas de información de seguridad de información.

[0006] En general, en un aspecto, la invención
20 se refiere a un aparato para estimar una política y práctica de seguridad de información de una organización, que comprende medios para determinar un riesgo asociado con la política y práctica de seguridad de información, medios para capturar información respecto a la política y
25 práctica de seguridad de información, medios para generar

una calificación utilizando una matriz de evaluación de de seguridad, la información capturada y el riesgo asociado con la política y práctica de seguridad de información, medios para generar una lista de acciones correctivas utilizando la calificación, medios para ejecutar la lista de acciones correctivas para crear una nueva política de información de seguridad y medios para supervisar la nueva política de información de seguridad.

[0007] En general en un aspecto, la invención se refiere a un sistema de computadora para estimar una política y práctica de seguridad de información de una organización, que comprende un procesador, una memoria, medios de alimentación, e instrucciones de soporte lógico almacenadas en la memoria para permitir al sistema de computadora bajo control del procesador, realizar la determinación de un riesgo asociado con la política y práctica de seguridad de información, capturar información respecto a política y práctica de seguridad de información utilizando los medios de alimentación, generar una calificación utilizando una matriz de evaluación de madurez de seguridad, la información capturada y el riesgo asociado con la política y práctica de seguridad de información, generar una lista de acciones correctivas utilizando la calificación, ejecutar la lista de acciones correctivas para crear una nueva política y práctica de

información de seguridad y supervisar la nueva política y práctica de información de seguridad.

[0008] Otros aspectos y ventajas de la invención serán aparentes a partir de la siguiente descripción y reivindicaciones anexas.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0009] La Figura 1 ilustra un sistema de computadora típico.

[0010] La Figura 2 ilustra un diagrama de flujo que detalla el método de evaluación de madurez de seguridad, de acuerdo con una modalidad de la invención.

[0011] La Figura 3 ilustra una porción de un reporte de la herramienta de reporte de evaluación de madurez de seguridad, de acuerdo con una o más modalidades de la invención.

[0012] La Figura 4 ilustra un diagrama de flujo que detalla el método para evaluación de madurez de seguridad de acuerdo con otra modalidad de la invención.

DESCRIPCIÓN DETALLADA

[0013] Modalidades ejemplares de la invención se describirán con referencia a los dibujos acompañantes. Ítems semejantes se denotan con números de referencia semejantes a través de los dibujos, por consistencia.

[0014] En la siguiente descripción detallada de la invención, se establecen numerosos detalles especí-

ficos a fin de proporcionar una comprensión más completa de la invención. Sin embargo, será aparente para una persona con destreza ordinaria en la especialidad que la invención puede practicarse sin estos detalles específicos. En otras instancias, características bien conocidas no se han descrito en detalle para evitar oscurecer la invención.

[0015] La invención además se refiere a un método para estimar una madurez de seguridad de la organización. Además, la invención se refiere a estimar la madurez de seguridad de una organización utilizando una matriz de evaluación de seguridad. Además, la invención se refiere a basar la matriz de evaluación de seguridad en la norma BS7799/ISO17799 y el Modelo de Madurez de Capacidad (CMM = Capability Maturity Model). Además, la invención se refiere a un método para proporcionar resultados cuantitativos, orientados en acciones, utilizando la matriz de evaluación de seguridad. Además, la invención se refiere a un método para comparar la madurez de seguridad de una organización a una meta predeterminada o a la madurez de seguridad de la misma organización en otro punto en el tiempo, o al nivel de madurez de seguridad obligado por otra organización o autoridad.

[0016] La invención puede implementarse virtualmente en cualquier tipo de computadora independiente-

mente de la plataforma empleada. Por ejemplo, como se ilustra en la Figura 1, una computadora típica (28) incluye un procesador (30), memoria asociada (32), un dispositivo de almacenamiento (34), y numerosos otros elementos y funcionalidades típicos de las computadoras actuales (no mostrados). La computadora (48) también puede incluir medios de alimentación tales como un teclado (36) y un ratón (38), y medios de salida, tales como un monitor (40). Aquellos con destreza en la especialidad apreciarán que estos medios de alimentación y salida pueden tomar otras formas en un ambiente accesible.

[0017] El Método de Evaluación de Madurez de Seguridad (SMA = Security Maturity Assessment) involucra cinco etapas distintas: (1) conciencia y compromiso de administración, (2) evaluación de madurez de seguridad, (3) plan de acción correctiva (CAP = Corrective Action Plan), (4) ejecución de plan de acción correctiva (CAPE = Corrective Action Plan Execution), y (5) supervisión continua. Cada una de las etapas anteriormente mencionadas se explica a continuación con mayor detalle. Aquellos con destreza en la especialidad apreciarán que los nombres empleados para denotar las etapas pueden variar sin separarse de la invención.

[0018] La Figura 2 ilustra un diagrama de flujo que detalla el método SMA de acuerdo con una modalidad

de la invención. El método SMA se inicia al asegurar que una administración de una organización esté consciente y comprometida en mejorar las prácticas y políticas de seguridad de información de la organización (etapa 100).

- 5 Una entidad de evaluación (por ejemplo individuo/compañía que realiza la evaluación) luego estima las prácticas y políticas de seguridad de información de la organización (etapa 102). Utilizando la información lograda en la etapa 102, la entidad de evaluación desarrolla un plan de
- 10 acción correctiva (etapa 102). El plan de acción correctiva subsecuentemente se ejecuta (etapa 102). Si la organización desea una supervisión continua después de la ejecución del plan de acción correctiva (etapa 108), entonces la entidad de evaluación puede supervisar conti-
- 15 nuamente las políticas y prácticas de información revisadas de la organización (etapa 110). Viendo la supervisión continua, el método puede regresar a la etapa 100 para asegurar que la administración de la organización aún esté al tanto conciente y comprometida o proceda po-
- 20 tencialmente en forma directa a la etapa 102 si la administración de la organización continúa estando consciente y comprometida. Si la organización no desea tener supervisión continua después de la ejecución del plan de acción correctiva (etapa 108) entonces termina el método.

[0019] La etapa de conciencia y compromiso de administración es la primer etapa del método SMA y se utiliza para elevar conciencia dentro de la administración de la organización que se estima e iniciar captura de información. Específicamente, en la etapa de conciencia y compromiso de administración, una entidad de evaluación obtiene información para comprender las metas de negocios de la organización. Además, la entidad de evaluación recolecta información para comprender los riesgos asociados en términos de seguridad de información. Por ejemplo, si la organización está utilizando una red de área local (LAN = Local Area Network) inalámbrica, hay diferentes riesgos de seguridad de información para considerar que si la organización utiliza una LAN convencional, en donde todas las computadoras están conectadas mediante cable Ethernet. Adicionalmente, la entidad de evaluación crea conciencia en la organización al presentar la metodología y método de evaluación de madurez de seguridad. En una o más modalidades de la invención, la entidad de evaluación también puede proporcionar información adicional respecto a las normas subyacentes, por ejemplo la norma ISO. En una o más modalidades de la invención, la entidad de evaluación también puede proporcionar una explicación de un concepto del modelo de madurez como se aplica a la evaluación de seguridad.

[0020] La etapa de evaluación de madurez de seguridad se inicia por la entidad de evaluación que identifica participantes requeridos para realizar SMA. Adicionalmente, la entidad de evaluación, en conjunto con la organización, determina el efecto y costo a utilizar para realizar SMA. Una línea de tiempo, también se establece para permitir que la entidad de evaluación y la organización tengan un medio para dar seguimiento al avance de SMA. En este punto, en una o más modalidades de la invención, la entidad de evaluación puede solicitar que la organización firme un contrato de evaluación para asegurar compromisos por la organización a seguir con SMA. Una vez que se han completado las etapas anteriormente mencionadas, la entidad de evaluación procede a realizar SMA.

[0021] La entidad de evaluación inicia SMA al capturar documentos que detallan las políticas y prácticas de seguridad de información existentes de la organización. Después de revisar los documentos capturados, típicamente se obtiene información adicional mediante entrevistas con participantes identificados al inicio de esta etapa. Utilizando la información obtenida de los documentos recolectados y las entrevistas, se genera una calificación preliminar. La calificación preliminar detalla la madurez de las secciones individuales y el nivel

de madurez total de las prácticas y políticas de seguridad de información de la organización.

[0022] En una o más modalidades de la invención, la calificación preliminar se genera utilizando una

5 matriz de evaluación de seguridad (SAM). La SAM define cada nivel de madurez para cada ítem de seguridad de información. La SAM incluye 61 hileras que corresponden a los grupos de los sitios de seguridad de información de la norma BS7799/ISO17799 y cinco columnas que definen el

10 nivel de madurez. Los cinco niveles de madurez, dispuestos del menos maduro a más maduro, son inicial (nivel 1), repetible (nivel 2), definido (nivel 3), administrado (nivel 4) y optimización (nivel 5). Por cada intersección de hilera y columna, hay un párrafo que define un

15 nivel específico de "madurez de capacidad". Los párrafos contenidos en una hilera determinada del SAM representan niveles de madurez de capacidad sucesivos para el mismo ítem de seguridad de información. Además, algunas hileras del SAM representan niveles de madurez de capacidad

20 sucesivos asociados con un solo ítem de seguridad de información, como se describe en un párrafo de la norma BS7799/ISO17799. Otras hileras de la SAM pueden representar niveles de madurez de capacidad sucesivos de ítems de seguridad de información que la norma BS7799/ISO17799

25 describe en secciones o párrafos separados.

[0023] En una o más modalidades de la invención, una definición de ítem por cada ítem de seguridad de información se incluye en la SAM. La definición de ítem actúa como una leyenda para las definiciones de nivel para un ítem de seguridad de información particular. Además, en una o más modalidades de la invención, la SAM incluye definiciones de nivel como sigue: nivel 1-inicial, nivel 2-no escrito, pero comunicado por asesoría o entrenamiento; nivel 3-escrito; nivel 4-se define responsabilidad; nivel 5-existe proceso para atrapar desviaciones y mejorar la seguridad de información para evitarlas. Además, en una o más modalidades de la invención, la SAM incluye requerimientos de alcance. Los requerimientos de alcance indican a que diversos aspectos de las operaciones de la organización deben aplicarse los criterios establecidos en una hilera particular de la SAM.

[0024] La combinación de una cierta definición de nivel (por ejemplo nivel 1) con un ítem de seguridad de información (es decir una hilera específica de la SAM) produce un criterio específico que una persona con destreza en la especialidad podrá aplicar para establecer si la organización que se estima satisface, falla o excede este nivel de madurez para este ítem de seguridad de información. Además, aquellos con destreza en la especialidad pueden aplicar la definición general del nivel de

madurez (nivel 1 a 5) a un ítem de seguridad de información específico, de manera tal que puedan determinar fácilmente si la organización que se estima satisface, falla o excede este nivel de madurez para este ítem de seguridad, incluso si el criterio específico establecido en la intersección de estas hilera y columna de la SAM, es por alguna razón, no directamente aplicable en el caso de esta organización.

[0025] La Tabla 1 ilustra la SAM de acuerdo con una o más modalidades de la invención:

Tabla 1. Matriz de Evaluación de Seguridad

Categorías ISO 17799			Nivel 1 (Inicial)	Nivel 2 (Repetible)	Nivel 3 (Definido)	Nivel 4 (Administrado)	Nivel 5 (Optimización)	Requerimientos de alcance
Definiciones de Nivel ==> Definiciones de ítems \/				No escrito, pero comunicado por entrenamiento o asesoría	Escrito	Se define responsabilidad	Existe proceso para atrapar desviaciones y hacer mejoras constantes	
III	Política	Cobertura de Política de Seguridad	No hay política de seguridad	Existe política de Seguridad,	Existe política específica	Política de seguridad cubre todas	Claras responsabilidades y mecanismos vi-	Meta y principio de toda

b7

de Segu- ri- dad de In- for- ma- ción	Revisión de implementa- ción efecti- va de polí- tica de se- guridad de información Revisión de Política de Seguridad de Información	vigente	pero como una decla- ración ge- neral. In- ferir lo que es es- pecífica- mente obli- gado o prohibido requiere consultar personal especiali- zado. No hay revi-	ca, esta- blece claramen- te en de- talle lo que es obligado o prohi- bido. Una persona "normal" puede compre- nderlo fá- cilmente. Revisio-	las áreas de negocios. Política de seguridad es propiedad de funciones apropiadas incluyendo IT, pero también Fi- nanzas, HR, Legal, etc. Políticas de organización definen los papeles y	gentes para actualizar la política si se requiere des- pués de cada infracción de la política, también si ocurren cam- bios de nego- cios (adquisi- ción, venta de activos o de- sinversión, o cambios prin- cipales en	seguridad de infor- mación Ad- ministra- ción y responsa- bilidades para com- partir in- formación
---	--	---------	--	---	--	--	---

				siones re- gulares.	nes lle- vadas a cabo a interva- los pero no hay responsa- bilidad de admi- nistra- ción cla- ra para activar revisio- nes o ex- plotar	responsabi- lidades para seguir pro- cedimientos. Revisiones llevadas a cabo inter- valos y res- ponsabilidad de las revi- siones se definen ex- plícitamente en la polí- tica.	proceso tales como subcon- tratación).	
--	--	--	--	------------------------	--	---	--	--

					resulta- dos			
		Disponibili- dad de Polí- tica de Se- guridad para Educación de Seguridad y Entrenamien- to Técnico de los Em- pleados	No hay co- municación de política de seguri- dad a los empleados (no exis- tente, o limitado a personal IT).	La política de seguri- dad se dis- cute con los emplea- dos y per- sonal bajo contrato o temporal, al contra- tar.	No hay manual de Política de Segu- ridad, menciona- do en el tablero de avisos públicos y/o en la página de la red.	Comunicación de política de seguridad es parte de IT escrito y procedimien- tos de per- sonal. En- trenamiento y/o comuni- cación en política de seguridad	Cada incidente de seguridad está sujeto a un procedi- miento post mortem que in- cluye una re- visión de si se comunicaron correctamente las políticas aplicables. Se enseña a los	Conciencia y educa- ción del personal Responsa- bilidades y disposi- tivos de emergencia entrena- miento de políticas de seguri-

						ocurren al menos una vez al año.	usuarios los procedimientos de reporte de incidentes.	dad bien definido integrado en el pro- grama de desarrollo de perso- nal res- ponsabili- dad de ad- ministra- ción en proporcio- nar entre- namiento de seguri-
--	--	--	--	--	--	--	--	--

								dad, in- cluyendo la especi- ficación de un es- critorio limpio y claras po- líticas de clasifica- ción para todos los empleados.
--	--	--	--	--	--	--	--	---

		Revisión del Pro- ceso de Seguridad	Expe- dido una vez, nunca revi- sado	Ocasional- mente revi- sado si la administra- ción de al- to nivel (senior) si los audito- res, etc. lo piden	Revisión a intervalos, pero no hay clara res- ponsabilidad de adminis- tración para activar re- visiones de resultados de explota- ción	Una entidad o persona clara- mente designa- dos tienen responsabili- dad para el proceso, y lo revisa regu- larmente.	Hay un mecanismo definido para revi- sar y actualizar la política después de cada incidente de seguridad (¿hay al- go que falte de la política que pudie- ra haber evitado el problema?)	Responsa- bilidad de admi- nistra- ción ge- neral

5

IV.	In- 1 frae stru ctu- ra de Segu- ri- dad de In- for- ma- ción	Responsa- bilidad de la protec- ción de valores indivi- duales	No hay asig- nada res- ponsa- bili- dad.	Individuos específicos están cons- cientes de su respon- sabilidad por prote- ger algunos valores. La lista de responsabi- lidades asignadas no está do- cumentada.	Una matriz para respon- sabilidad de protección de valores existe y es- tá publica- da.	Una parte es- pecífica es responsable por definir y mantener la matriz de res- ponsabilidad de la protec- ción de valo- res individua- les. La acción sucesiva de la matriz se lo- gra para ayu- dar en inves- tigaciones fu-	Responsabilidad de seguridad es un campo requerido del proceso de adminis- tración de valores, de manera tal que se crean hileras en la matriz cuando se obtienen nuevos va- lores. A valores sin una parte res- ponsable se les po- ne bandera inmedia- tamente para acción correctiva.	Valores indivi- duales se refieren a los va- lores es- pecíficos de la or- ganiza- ción (por ej. com- putado- ras, im- presoras, etc.)
-----	---	---	--	---	--	--	--	--

						turas.		
		Seguridad en definición de trabajo y recursos	No hay proceso formalmente definido.	Individuos específicos están conscientes de su responsabilidad.	Responsabilidad para toma de decisiones de seguridad se ha asignado y documentado.	Una parte específica es responsable por desarrollar las responsabilidades de trabajo, supervisión de personal y convenios de confidencialidad.	Descripciones de trabajo y arreglos de supervisión de personal se revisan periódicamente para adaptarse a las necesidades cambiantes de seguridad del negocio. También se refiere personal para firmar y acordar los convenios de confi-	La interpretación se basa en la posición del tipo SSO/IRT.

							dencialidad.	
		Educación y entrenamiento de seguridad de información	No hay plan de entrenamiento formalmente definido.	Miembros clave del personal se entrena o en una base ad-hoc.	Entrenamiento para personal se define y realiza periódicamente.	Una parte específica es responsable por definir el plan de entrenamiento que desarrolla programas de entrenamiento para todo el personal.	Curriculum de seguridad se revisa periódicamente para adaptarse a las necesidades cambiantes del negocio. Registros de entrenamiento se revisan contra política y las excepciones llevan a actualizaciones del programa de entrenamiento.	

		Proceso de aprobación para adquisición e instalación de instalaciones IT.	No existe proceso de aprobación.	Conocimiento informal, no documentado de las etapas a seguir cuando se adquieren o realizan instalaciones IT.	Se define un proceso de aprobación claro para la adquisición e instalación de facilidades IT y publica en toda la empresa.	Una parte específica es responsable por definir y mantener el proceso de aprobación para adquisición de instalación y colocación IT.	El proceso de aprobación se realiza periódicamente para adaptarse a las necesidades cambiantes del negocio. El proceso de aprobación para cada adquisición y colocación de instalaciones IT se revisa por precisión y se lleva a cabo acción correctiva cuando sea apropiado.	
--	--	---	----------------------------------	---	--	--	---	--

IV.	Segu- 2 ri- dad de ac- ceso a Ter- ce- ras Par- tes	Control de Segu- ridad de Acceso a Terceras Partes para Ins- talación de Proce- dimiento de Infor- mación	No hay mecca- nismo de con- trol	Control de acceso fí- sico permi- te decisio- nes ad.hoc por el per- sonal IT, a quienes se les ha di- cho infor- malmente que hacer.	Las reglas de control de acceso están docu- mentadas. Hay contrato formal con cada parte que requiera acceso.	Acceso de ter- ceras partes está vinculado con el resto del sistema de seguridad de la organiza- ción a través de la expedi- ción de seña- les de acceso y se registran los accesos.	Los registros de acceso y la lista de terceras partes autorizadas se au- ditan regularmente y cambios a proce- dimiento se reali- zan cuando surge la necesidad.	
IV.	Sub- 3 con- tra-	Controles de segu- ridad pa-	Ningu- no; los	IT, Seguri- dad, Legal, o Compras	Los procedi- mientos para seguridad de	Hay un regis- tro de contra- tista. Firman	Se realizan proce- dimientos en al me- nos una base anual	Aplica- ciones críticas

60

	ta- ción	ra con- tratistas externos.	contra- tistas se ma- nejan por el pro- pieta- rio de tarea sin polí- ticas o pro- cedi- mien-	aplican a algunos pa- sos regula- res cuando se expiden contratos. Estos pasos no están documenta- dos especí- ficamente.	contratista se documen- tan por es- crito y per- sonal y ad- ministrado- res tienen acceso a ellos y es- tán cons- cientes de sus conteni- dos.	la política de seguridad, convenios IP y NODE. Audito- rías se llevan a cabo cuando menos trimes- tralmente para asegurarse que la lista de contratistas está al co- rriente. El propietario del proceso es definido.	para mejoras posi- bles.	quedan en casa Aproba- ción del propieta- rio del negocio. Implica- ciones para pla- nes de continui- dad en el negocio. Normas de y acata-
--	-------------	-----------------------------------	--	---	---	--	-----------------------------	--

			tos espe- cifi- cos.					miento seguridad Procedi- mientos de inci- dentes de seguri- dad.
V.1	Res- pon- sabi- li- dad	Cobertura de Mante- nimiento de Inven- tario de Valores	No hay inven- tario	Inventario manual, ocasional, ante deman- da.	Inventario realizado de acuerdo con procedimien- tos escri- tos, pero no	Programa, ac- tivadores, pa- peles y res- ponsabilidad están defini- dos. La pro-	Hay un proceso para revisar lo que su- cede después de cada inventario. Los inventarios son incrementales. No	Inventa- rio de Valores de Infor- mación

	de valo- res				están bien definidos programa y eventos de activación. Típicamente no está au- tomatizado	riedad es cla- ra y se conoce a través de la organización IT y adminis- tración.	incrementales no desde "cero" o lí- nea de partida cada vez. Los inventa- rios de valores son automatizados.	Inventa- rio de valores de Sopor- te Lógico Inventa- rio de Valores Físicos
		Facilidad de Alte- ración de Valores de Infor- mación	Los valo- res de Infor- mación pueden ser	Hay conoci- miento in- formal de que docu- mentos cla- sificados no pueden	Hay un pro- cedimiento de cambio documentado que aplica a todos los valores de	Hay mecanismo de control (por ej. con- troles de ac- ceso) para evitar altera- ción sin ade-	Hay un mecanismo en sitio para revisar la efectividad del proceso de control de cambio y detec- tar la necesidad por mejoras.	Reportes impresos Exhibi- ciones en Pantalla Medio Magnético

			alterados sin control	ser alterados a voluntad pero no hay procedimientos sistemáticos.	información clasificadas. No hay mecanismos de control sistemático en vigor.	cuada autorización.		Mensajes Electrónicos Transferecia de Archivos
		Cobertura de procedimientos de manejo de info.	No hay procedimientos en vigor para manejo de información.	Cubre algo de valores de información. Hay poca formación, no hay revisiones regulares.	Hay manual para manejo de información, mencionado en la página pública de la red y cubre esen-	Procedimientos para manejo de información son propiedad por funciones apropiadas incluyendo IT, Finanzas, HR,	El entrenamiento de manejo de info. es parte de procedimientos de IT y personal escrito. Procesos en vigor para reportar y aprender de casos cuando la informa-	Inventario de Valores de Información Inventario de Valores de Sopor-

			fo.	Aplicado por unas cuantas unidades de negocios.	cialmente todos los tipos de va- lores y to- das las uni- dades de ne- gocios.	Legal, etc. Políticas de organización definen los papeles y res- ponsabilidades a seguir los procedimien- tos.	ción se ha manejada incorrectamente.	te Lógico Inventa- rio de Valores Físicos Inventa- rio de Servicios Reportes Impresos Exhibido- res de Pantalla Medios Magnéti- cos Me-
--	--	--	-----	---	--	--	---	--

								dios Electró- nicos Transfe- rencias de Archi- vos ("Ma- nejo"= copiado, almacena- miento, transmi- sión electró- nica, transmi-
--	--	--	--	--	--	--	--	---

GC

								si3n ha- blada, transmi- si3n, destruc- ci3n)
V.2	Cla- sifi- ca- ci3n de In- for- ma- ci3n	Clasifi- caci3n de Valores de Infor- maci3n Etiqueta- do de Va- lores de Informa- ci3n	Sin clasi- fica- ci3n	Clasifica- ci3n ad hoc, a la iniciativa del propie- tario del documento. La mayorfa de los doc- tos. no es-	La clasifi- caci3n de valores de informaci3n est3 publi- cada y "im- pulsada" a todos los propietarios de documen-	Propiedad de la clasifica- ci3n se define claramente co- mo parte de los procedi- mientos de la compa3fa y es conocimiento de la adminis-	Clasificaci3n de seguridad se reali- za peri3dicamente. Lista de documentos con m3s alta clasi- ficaci3n se realiza peri3dicamente. Existen procedi- mientos de descla- sificaci3n.	Reportes Impresos Archivos de Inge- nierfa (fotos, microfi- chas, etc.) Exhibido-

				tán marca- dos. De es- tar marca- dos, las etiquetas son incon- sistentes. No hay cam- paña de conciencia sistemáti- ca.	tos poten- ciales. Cu- bre seguri- dad. Infor- mación cla- sificada es- tá etiqueta- da, consis- tentemente.	tración		res en Pantalla, Medios Magnéti- cos Men- sajes electró- nicos Transfe- rencia de Archivos
--	--	--	--	---	--	---------	--	--

VI.1	Segu- ridad en De- fini- ción de Traba- jo y Recur- sos	Supervi- sión del nuevo so- licitan- te. Veri- ficación completa del CV de los nue- vos soli- citantes. Supervi- sión de	Incompleto o falta de supervi- sión del solicitan- te. Con- tratación de contra- tista no es vetada por HR.	Supervisión del solici- tante se realiza de manera in- formal, no está docu- mentada y no se rea- liza con- sistente- mente.	Procedimientos documentados y publicados pa- ra supervisión del solicitan- te existen y se utilizan por la organi- zación.	Una parte es- pecífica es responsable por recibir y mantener el procedimiento de supervi- sión. Resul- tados de su- pervisión se capturan en el archivo HR del solici-	Se revisan procedimien- tos regular- mente para mejoras y cumplimien- tos. Los as- pectos de se- guridad que se encuentran relacionados a fallas en el procedi-	Solici- tante se refiere a todos los empleados (contra- tista, permanen- te o tiempo parcial)

		contra- tista y personal temporal.				tante.	miento de su- pervisión obligan a re- visión inme- diata y ac- tualización del procedi- miento.	
VI.2	Entre- na- miento del Usua- rio	Conciencia de seguridad del per- sonal	Poca conciencia de seguridad corporati- va.	Discutido con emplea- dos y per- sonal bajo contrato o temporal al contratar.	Documentado por escrito y disponible a todo el perso- nal. Empleados reciben una copia de polí- tica de segu-	Papeles y responsabili- dades para mantener y comunicar la política de seguridad son definidos. A	Auditorías de reconocimien- tos de segu- ridad se rea- lizan. Ocurre periódicamen- te un sistema de confirma-	

04

					ridad al con- tratar y se requiere que acusen recibo.	confirmación de la políti- ca se da se- guimiento y almacena como parte de la política HR del empleado.	ción de reco- nocimiento periódicamen- te y ante cambios de la política de seguridad. Se analizan in- cidentes para mejorar el desempeño pa- ra los proce- dimientos de conciencia de seguridad.	
--	--	--	--	--	--	--	--	--

		Educación de seguridad y entrenamiento técnico	No se proporciona educación o entrenamiento.	Educación de seguridad y entrenamiento técnico no se proporcionan consistentemente y la responsabilidad es a la discreción de la administración.	Educación de seguridad está documentada e incluida como parte del proceso de contratación. Mapas de entrenamiento técnico existen por cada empleado.	Una parte específica es responsable por definir y mantener el programa de educación de seguridad y entrenamiento técnico. Registros de entrenamiento se capturan en el archivo de los empleados. Re-	Planes de entrenamiento se revisan periódicamente para cumplir con las cambiantes necesidades del negocio. Registros de entrenamiento se revisan contra la política y las excepciones llevan a ac-	
--	--	--	--	--	--	--	--	--

						visión y planificación para entrenamiento futuro es parte del proceso de evaluación.	ciones correctivas.	
VI.3	Respon diendo a In- ciden- tes de Segu- ridad y Fa-	Proceso Discipli- nario pa- ra Viola- ciones de Seguridad de la Compañía	Ninguno documenta- do. Reac- ción es ad hoc.	Los admi- nistradores tienen con- ciencia in- tuitiva de la necesi- dad, pueden citar múl- tiples ni-	La definición de violacio- nes, procedi- mientos de in- vestigación, y lista de pena- lizaciones aplicables es- tá documenta-	El proceso documentado incluye pape- les y respon- sabilidades por cada eta- pa y un flujo de trabajo claro.	Después de cada inciden- te que provo- que que se invoque el procedimien- to, el proce- so se revisa y cuando	

	lla			veles de penaliza- ción, in- cluyendo pero no li- mitados a despido. Los admi- nistradores y HR inde- pendiente- mente con- vienen en cómo ini- ciar y con- ducir ac-	do, distribui- do y firmado por las partes apropiadas y el personal sea educado en cuanto al con- tenido.		aplica, el proceso es revisado (in- cluyendo en- trenamiento o las cláusulas de penaliza- ción).	
--	-----	--	--	---	--	--	---	--

ht

				ciones dis- ciplina- rias.				
VII. 1	Áreas Seguras	Protec- ción de acceso no auto- rizado. Control de en- trada física a oficina.	El equipo IT está sin ascen- der sin controles más allá de acceso físico al edificio o la cons-	Control de acceso se proporciona en una base ad hoc, tí- picamente por el ad- ministrador IT. No hay lista defi-	Lista de perfí- metros seguros y derechos de acceso a aque- llas áreas son documentadas y publicadas.	Todo acceso a áreas IT se- guras se rea- liza por un mecanismo (por ejemplo sistemas de control de acceso por credencial o	Auditoría de registro de sistema de control de acceso se realiza pe- riódicamente. Cambios en instalaciones y administra-	

		Seguri- dad fí- sica pa- ra ins- talacio- nes IT.	trucción.	nida de de- rechos de acceso pu- blicada o administra- da.		gafete) que permiten identifica- ción del per- sonal y audi- toría. Con- trol de acce- so se admi- nistra cen- tralmente pa- ra otorgar y revocar dere- chos y está vinculado con políticas de contratación	ción activan una revisión y repaso de los procedi- mientos de acceso.	
--	--	--	-----------	---	--	--	--	--

34

						y termina- ción.		
VII. 2	Seguri- dad de Equipo	Sistema de alar- ma con tra in- cendio no está presen- te.	El sistema de alarma contra in- cendio existe y a la gente se le ha hecho con- ciente in- formalmen- te del sistema.	Procedi- mientos pa- ra el sis- tema de alarma con- tra incen- dio son vi- sibles y están pre- sentados al corriente, incluyendo	Se prueba el sistema de alarma contra incendio. Existen proce- dimientos para evaluación del sistema de alarma contra incendio in- cluyendo eva-	Reacción a alarma actual se revisa y se implemen- tan mejoras en el sistema actual y sis- temas alter- nos se revi- san cuando sea necesá- rio.		

				ruta de evacuación, acciones de comportamiento, advertencias Halon, etc.	ños y recuperación, conteo de evacuación, etc.			
		Política de estación de trabajo personal	No existen políticas para estaciones de trabajo personal.	Existen políticas para la estación de trabajo personal pero no están publicadas o	Hay una política documentada para estación de trabajo personal y se toman pasos para dispersar o difundir su con-	Una parte específica es responsable por definir y mantener la política de estación de trabajo personal. Infor-	La política de estación de trabajo personal se revisa regularmente para asegurar que cumple con las ne-	

				adaptadas completa- mente por toda la or- ganización.	ciencia entre los empleados.	mación sensi- ble es prote- gida mediante cifrado.	cesidades cambiantes del negocio. Se revisan las necesi- dades de es- tación de trabajo per- sonal y se realizan cambios cuando es necesario. Las audito- rías se lle- van a cabo	
--	--	--	--	---	---------------------------------	---	--	--

							para asegu- rar que la organización mantenga una política de estación de trabajo re- conocida pa- ra asegurar administra- ción efi- ciente.	
		Protec- ción contra amenazas	No hay procedi- miento en vigor para	Hay en vi- gor una po- lítica de protección	Hay una polí- tica documen- tada formal en vigor. Deta-	Una parte es- pecífica es responsable por definir y	La política de amenaza a la seguridad se revisa	

08

	y ries- gos am- bienta- les. Protec- ción contra descuido humano (comer, fumar, beber). Protec- ción contra cable de	proteger contra riesgos o amenazas de seguri- dad.	de amenaza de seguri- dad infor- mal. No es- tá puesta en vigor a través de la organi- zación y los deta- lles de la política no están docu- mentados.	lla todas las etapas que re- quieren ser seguidas para proteger con- tra riesgos potenciales.	mantener las guías de con- trol de ame- naza a la se- guridad.	regularmente para asegu- rar que cum- ple con las necesidades cambiantes del negocio. La política se revisa regularmente y se reali- zan cambios cuando es necesario para asegu- rar un cum-	
--	---	---	---	---	--	---	--

		energfa y comu- nicacio- nes por inter- cepción o daño					plimiento continuo.	
VII. 3	Contro- les Ge- nerales	Inspec- ción por riesgos por en- trada de artícu- los	No se ins- pecciona entrada de artículos.	No hay pro- ceso formal para ins- peccionar entrada de artículos. Se lleva a cabo en una forma ad-	Hay un proceso documentado con el que to- da entrada de artículos se inspecciona de acuerdo con un plan definido.	Una parte responsable se identifica para adminis- trar los pro- cesos y pro- cedimientos para inspec- cionar entra-	Los procesos de clasifi- cación de artículos clave se re- visan regu- larmente y asegura que cumplen con	

				hoc.		da de artícu- los para cum- plimiento con seguridad.	las necesi- dades cam- biantes del negocio. Unas buenas necesidades de clasifi- cación se realizan y se realizan cambios cuando sean necesarios. La organiza- ción mantie- ne archivos	
--	--	--	--	------	--	---	---	--

							históricos de entrada de artículos; estos se revisan regularmente para asegurar que no haya discrepancias.	
		Proceso de remoción de la propiedad de la	No hay procedimiento estandarizado para remoción	Existe un proceso informal para la remoción de la propiedad.	Un proceso informal es documentado y publicado en la organización para re-	Un inventario de propiedad organizacional se mantiene y actualiza regu-	Auditorías de la propiedad de la organización se llevan a cabo periódicamente.	

		organi- zación	de propie- dad.		moción de la propiedad.	larmente. Se identifica un grupo o indi- viduo que ve- rifique que se siga el proceso.	dicamente y cuando es necesario se realizan cambios al proceso de remoción.	
		Mantenimiento de equi- po	No hay po- líticas de manteni- miento de equipo y el mante- nimiento de equipo se realiza	El manteni- miento de equipo se lleva a ca- bo en una base ad hoc, con base en los intervalos	El equipo está cubierto por seguro y el mantenimiento de equipo con- trola la de- terminación de riesgo.	Una parte responsable se identifica para supervi- sar que se sigan las po- líticas de mantenimiento de equipo.	Se examina el registro de manteni- miento de equipo para determinar patrones de falla o abu- sos. Se in-	

			solo al fallar.	de servicio recomen- dos por el fabricante.			corporan cambios apropiados en las polí- ticas de mantenimien- to.	
		Procedi- miento para de- sechar datos sensibles	No está definido un proce- dimiento para dese- cho de da- tos.	El procedi- miento de desecho de datos se define in- formalmen- te.	El procedi- miento de de- secho de datos está definido formalmente y publicado en la organiza- ción.	Una parte responsable se identifica que supervisa que se siga el procedi- miento de de- secho.	El procedi- miento de desecho se audita regu- larmente e incorporan etapas apro- piadas en el procedimien-	

							to.	
VIII	Proce- .1 dimien- tos Opera- ciona- les y Respon- sabili- dades	Procedi- mientos y Res- ponsabi- lidades de Admi- nistra- ción In- cidentes a los Procedi- mientos	Ninguno - cada inci- dente se maneja ad hoc en una base de mejor es- fuerzo.	Conciencia común de procedi- mientos. Esfuerzo para repe- titividad incluye juntas de personal, sesiones de entrena-	Documentado por escrito y disponible a todo el perso- nal IT (y otros del equipo del de- partamento con funciones IT)	Funciones y responsabili- dades se de- finen. Exis- ten cadenas de escala- miento y re- porte. Aspec- tos y solici- tudes se re- gistran como boletos de	Procedimien- tos incluyen un mecanismo para evolu- cionarlos. Los inciden- tes se ana- lizan para sugerir me- joras. Hay un proceso de mejora de	Procedi- mientos de repor- te cu- bren: to- dos los tipos de planes de contin- gencia por inci- dentes de

		de Re- porte		miento y asesoría		problema.	calidad, do- cumentado y aplicado.	seguridad auditoría de cam- bios y acciones de recu- peración similares y autori- dad
--	--	-----------------	--	----------------------	--	-----------	--	--

VIII	Planeación y Aceptación del Sistema	Prueba de nuevos requerimientos de sistemas de información y actualizaciones antes de despliegue	Ninguno; nuevos sistemas se ponen en operación sin ningún procedimiento de prueba formal.	La prueba es informal y se realiza con base en el conocimiento de los individuos, no en un proceso formal.	Un documento formal que define las pruebas y despliegue de sistemas nuevos y actualizados, es definido.	La responsabilidad en definir, revisar y asegurar cumplimiento con las políticas de pruebas se define. Hay herramientas a nivel de sistema que evitan cambios no au-	La política se revisa periódicamente y repasa ante cualquier cambio en los sistemas de producción o en la estructura organizacional. La metodología de prueba y he-	Incluye aspectos de planeación de capacidad y de aceptación del sistema. Aspectos a considerar incluyen: Desempeño y Requerimientos de Capacidad
------	-------------------------------------	--	---	--	---	--	---	--

						torizados a sistemas de producción. Existen do- cumentos que detallan interfases en el proce- so de admi- nistración de cambio.	rramientas se examinan continuamen- te para de- terminar la aplicabili- dad a la or- ganización y luego intro- ducen.	de Computa- dora Proce- dimientos de Recupe- ración de Error y Reinicio Controles/ Aspectos de Seguridad Procesos de Manual Arreglos de Continuidad de Negocios Carga Adi-
--	--	--	--	--	--	---	--	---

								cional en Máquinas Existentes, Entrena- miento en la opera- ción del nuevo equi- po
--	--	--	--	--	--	--	--	---

VIII	Protec- .3 ción Contra Soporte Lógico Mali- cioso	Detección y protec- ción con- tra sopor- te lógico malicioso. Conciencia del usua- rio de procedi- mientos para tra- tar con soporte lógico ma-	No hay pro- cedimientos de detec- ción, medi- das de pro- tección, reporte o recupera- ción, y el tratar con soporte lógico mali- cioso y ataques de virus es	El personal IT ha defi- nido infor- malmente procedimien- tos para de- tectar y ma- nejar sopor- te lógico malicioso y ataques de virus. No hay herra- mientas co- munes, docu-	Existe un procedi- miento formal, documenta- do para detectar y manejar soporte lógico ma- licioso y ataques de virus y se comunica a todos los	Una parte específica es responsa- ble por de- finir y man- tener los procedimien- tos de de- tección y protección, informar y entrenar a los usua- rios, admi- nistrar la	El procedi- miento inclu- ye un meca- nismo para evolución. Los inciden- tes se anali- zan para su- gerir mejoras . El juego de herramien- tas se exami- na continua- mente y ac- tualiza para	Los proce- dimientos cubren: Todo tipo de virus y soporte lógico ma- licioso incidente Planes de contingen- cia Regis- tros de auditoría y acciones
------	--	---	---	---	---	---	--	---

		licioso. Procedi- mientos para re- portar y recuperar ataques de virus	totalmente reactivo y manejado en una forma ad hoc.	mentación formal o programas de entrenamien- to para to- dos los em- pleados.	empleados como parte de la po- lítica de seguridad corporati- va. Un juego es- tándar de herramien- tas de protección se define y desplie- ga. El en- trenamien-	detección y los esfuer- zos de recu- peración, y seleccionar y mantener las herra- mientas pro- tectoras.	proporcionar protección máxima contra amenazas cam- biantes.	y autori- dad de re- cuperación similares.
--	--	---	---	---	---	---	--	---

					to se da a todos los empleados.			
		Política referente a soporte lógico con licencia y prohibición de soporte lógico no autorizado.	No hay política o supervisión respecto a instalación de soporte lógico.	Políticas de supervisión de soporte lógico son informales y se realizan en una base ad hoc. La organización IT, cuando está involucrada en procurar el	Una política de licencias de soporte lógico es documentada y publicada a todos los empleados.	Una parte específica es responsable por supervisar y mantener licencias de soporte lógico autorizadas para la empresa. Una herramienta para	Lista de soportes lógicos autorizados se revisa periódicamente para cumplir con las necesidades cambiantes del negocio. Se revisan auditorías de soporte lógico	

				soporte lógico, aplica controles informalmen- te.		licencia de inventario de soporte lógico se utiliza para supervisar y asegurar cumplimiento.	co y las excepciones llevan a acciones correctivas.	
VIII	Mantenimiento	Supervisión de energía y almacenamiento de procesamiento pa-	No existe supervisión. Ajustes de capacidad se realizan en reacción a	Supervisión informal como parte de procedimientos de administración de sistema	El proceso de administración de capacidad y el plan de capacidad	Se define propiedad del plan de capacidad y el proceso de administración de	Nueva tecnología, convenios contractuales y selección de proveedor se investigan e	

		ra asegu- rar dispo- nibilidad.	los proble- mas.	se realiza en una base según se re- quiera. No hay plan de capacidad de administra- ción o mode- lo que se defina espe- cíficamente.	cubren energía de procesa- miento, memoria, espacio de disco, ca- pacidad LAN/WAN, capacidad de respal- do, número de esta- ción de trabajo de usuario,	capacidad. Mecanismo formal para administra- dores de ne- gocios para colocar re- querimientos en el plan y enlazar en- tre el pro- ceso de pla- neación de capacidad y el proceso del presu-	introducen continuamente en el ambien- te a fin de proporcionar los recursos necesarios mientras que se optimizan los costos.	
--	--	---------------------------------------	---------------------	--	--	--	--	--

					espacio físico y potencia.	puesto.		
VIII	Admi- .5 nistra- ción de Red	Cubierto por otros asuntos en esta sección						
VIII	Manejo .6 y segu- ridad de me- dios	Procedi- mientos y controles para pro- teger me- dios de computado- ra	No hay co- locados procedi- mientos o controles para prote- ger medios de computa-	Personal IT ha definido informalmen- te procedi- mientos y controles para prote- ger medios	Existen procedi- mientos documenta- dos, for- males para proteger medios de	Una parte específica es responsa- ble por de- finir y man- tener proce- dimientos para siste-	Procedimien- tos se revi- san periódica- mente para atender cam- bios del tipo o volumen de medios de	Medios in- cluyen: medio de sala de computado- ra IT (es decir cin- tas de

			dora.	de computa- dora. No hay documenta- ción formal, registros de acceso o programas de entrenamien- to para to- dos los em- pleados.	computado- ra y se comunican a todos los em- pleados como parte de la po- lítica de seguridad de la cor- poración. Los con- troles es- tán en si- tio para	mas de con- trol de ac- ceso y audi- tar el acce- so a los me- dios de com- putadora.	computadora a manejar. Se revisan los registros de auditoría y las excepcio- nes llevan acción co- rrectiva.	respaldo, unidades de disco duro remo- vibles, CD ROMs, etc.) Me- dios de usuario (por ej. CD ROMs, discos flexibles, etc.)
--	--	--	-------	---	---	---	--	--

					limitar y dar seguimiento a accesos a los medios. Se da entrenamiento a todos los empleados.			
VIII .7	Inter-cambios de Información y Soporte	Seguridad de intercambio de datos y soporte lógico con	No hay procedimientos definidos para asegurar el intercambio	No hay norma corporativa o política que exista para atender el asegurar	Una norma corporativa para el intercambio de seguridad de	Una parte específica es responsable por definir y mantener las	Las normas se revisan periódicamente para atender cambios a los datos inter-	Normas para asegurar intercambio de datos y soporte

	Lógico	otras or- ganizacio- nes.	de datos o soporte ló- gico.	el intercam- bio de datos y soporte lógico con otras orga- nizaciones.	datos y soporte lógico con otras or- ganizacio- nes se do- cumenta y publica para todos los em- pleados.	normas para el intercam- bio seguro de datos y soporte ló- gico. Una política de clasifica- ción e in- formación determina que puede ser y como se transmi- te.	cambiados o los medios de intercambio. La política de clasifica- ción e infor- mación evolu- ciona conti- nuamente.	lógico con terceras partes y distribui- dores ex- ternos. Política de clasi- ficación de infor- mación

100

IX.1	Requeri- mientos de Nego- cios pa- ra Con- trol de Acceso	Documenta- ción de re- querimien- tos de ne- gocios para control de acceso. De- claración de política de acceso que define el derecho de acceso de cada	No hay conciencia o práctica de con- trol de acceso.	Una práctica de control de acceso no documentada, se informal se aplica en una base ad hoc.	Existe una declaración de política de acceso define dere- chos de ac- ceso de cada usuario o grupo de usuarios y es publica- da.	Una parte específica es respon- sable por definir y mantener la declaración de política de acceso y asegurar que está en línea con los reque- rimientos	La declara- ción de po- lítica de acceso se realiza pe- riódicamente para cumplir con las ne- cesidades cambiantes del negocio. Incidentes de seguridad se revisan y	Los dere- chos de acceso abarcen cuentas para acce- so a red, sistema operativo y aplica- ción. ACLs, cuentas de

		usuario o grupo de usuarios. Protección de servicios conectados contra uso no autorizado. Revisión de derecho de acceso de usuario y capacidades Política referente				de nego- cios.	las modifi- caciones a la declara- ción de po- lítica de acceso se hacen cuando sea apropia- do.	usuario y sistema, etc. Iden- tificación automática de termi- nales y dispositi- vos portá- tiles. In- terrupcio- nes de sistemas remotos se queda sin atender
--	--	---	--	--	--	----------------	--	--

		al uso de red y servicios de red. Controles de red en vigor.						por periodos prolongados de tiempo.
IX.2	Administración de Acceso de Usuario	Sistema de registro/desregistro formal para acceso a servicio IT. Promoción de	No hay control sobre acceso a servicios IT.	Una práctica de cuenta de usuario no documentada informal se aplica en una base ad hoc.	Una política de cuenta de usuario de fine derechos de acceso, a nivel de privilegio y reglas de	Una parte específica es responsable por definir y mantener la política de cuenta de usuario.	La política de cuenta de usuario se revisa periódicamente para cumplir con las necesidades cambiantes	Eliminación contra desactivación de cuenta. Id única para todos los usuarios.

		cuenta in- mediata pa- ra usuarios que cambian cargos o dejan la compañía. Privilegios de usuarios para supe- rar la res- tricción de aplica- ción/siste- ma. Regis- tro se			creación/ eliminación existen y están publi- cadas.	Registros de crea- ción/ eli- minación de cuenta de usuario se archivan.	del negocio. Los requeri- mientos de auditoría se revisan y modificacio- nes a la po- lítica de cuenta de usuario se realizan cuando sea apropiado. Se crean o eliminan múltiples	
--	--	--	--	--	---	--	--	--

		mantiene de todos los privilegios asignados. Rutina de sistema para otorgar privilegio a usuario. Control de acceso a biblioteca fuente de programa					cuentas por individuo a través de un solo punto de control.	
--	--	---	--	--	--	--	---	--

IX.3	Responsa- bilidades de Usuario	Seguridad de clave de usua- rio. Nivel de confi- denciali- dad de clave de usuario.	No se emplean claves.	Se aplica una prác- tica de clave no documenta- da, infor- mal en una base ad hoc.	Una polí- tica de clave pu- blicada define la fuerza de la clave, (por ej. longitud, inclusión de carac- teres es- peciales), edad y uso.	Una parte específica es respon- sable por definir y mantener la política de claves. El registro de historia de claves se archiva.	La política de claves se revisa pe- riódicamente para cumplir con las ne- cesidades cambiantes del negocio. Auditorías periódica (descifrado de códigos) de claves se realizan pa-	Límite de número de intentos de clave antes de que el sistema blo- quee al usuario. Registra ya sea al usua- rio concien- te de inten- tos de re- gistros sin éxito. Pues-
------	--------------------------------------	---	-----------------------------	--	---	--	--	--

							ra asegurar cumplimiento y excepciones se anotan, documentan y se toma acción correctiva.	ta en vigor de reglas de clave
		Guías de buena práctica a los usuarios para asegurar buena seguridad.	No existen guías.	Se proporcionan guías no documentadas informales a los usuarios en	Declaración de guía de buena práctica se define e incorpora en los	Una parte específica es responsable por definir y mantener las guías de buena	Existe un proceso para solicitar sugerencias para guías de mejor práctica para fuentes	No hay exhibición de identificadores de sistema hasta que ha sido exitoso el registro

				una base ad hoc.	programas de entre- namiento de usua- rio.	práctica	internas y externas e incorporar- las en las guías de se- guridad del usuario en la organiza- ción.	siguiente. Una adver- tencia gene- ral que el sistema solo deberá ser empleado por usuarios au- torizados Si ocurre error al registrar no indica cual fue el error
--	--	--	--	---------------------	--	----------	---	---

		Controles Criptográ- ficos	No exis- ten guías.	Guías no documenta- das infor- males se proporcio- nan a los usuarios en una ba- se ad hoc.	Una decla- ración de guía de buena práctica se define e incorpo- ra en los programas de entre- namiento de usua- rio. Las guías cu- bren: ci- frados,	Una parte específica es respon- sable por definir y mantener las guías de buena práctica.	Existe un proceso para solicitar sugerencias para guías de mejor práctica por fuentes in- ternas y ex- ternas e in- corporarlas en las guías de seguridad de usuario de la orga- nización	
--	--	----------------------------------	---------------------------	---	--	---	--	--

					firmas di- gitales, adminis- tración de claves, servicios con reco- nocimiento de autoría			
IX.4	Control de acceso a red	Cubierto en otras áreas en esta sec- ción						
IX.5	Control de acceso a sistema operativo	Cubierto en otras áreas en esta sec- ción						

IX.6	Control de acceso a aplicación	Cubierto en otras áreas en esta sección						
IX.7	Acceso y uso de sistemas de transmisión	Cubierto en otras áreas en esta sección						
IX.8	Computación móvil y trabajo a distancia	Computación móvil y trabajo a distancia	No existen guías	Se proporcionan guías no documentadas informales a los usuarios en	Se define una declaración de guías de buena práctica e incorpora en los	Una parte específica responsable por definir y mantener las guías de buena práctica.	Existe un proceso para solicitar sugerencias para guías de mejor práctica de fuentes in-	Seguridad de Laptop, Mobile y Paltop para asegurar que información de la compañía no esté

				una base ad-hoc.	programas de entre- namiento de usua- rio.		ternas y ex- ternas e in- corporarlas en las guías de seguridad de usuario de la orga- nización.	comprometi- da.
X.1	Requeri- mientos de seguridad en los sistemas	Evaluación de riesgo y adminis- tración de riesgo em-	No hay marco para evalua- ción de	Una prác- tica de adminis- tración de riesgos y	Existe un procedi- miento de adminis- tración de	Una parte específica es respon- sable por definir y	Las políti- cas de admi- nistración de riesgos y evaluación	

		pleadas para analizar requerimientos de seguridad.	riesgos.	evaluación de riesgos no documentada e informal se aplica en una base ad-hoc.	riesgos y evaluación de riesgos publicado.	mantener las guías de administración de riesgos y evaluación de riesgos. Se mantiene un archivo de los riesgos identificados y la acción que se toma para adminis-	de riesgos se realizan periódicamente para cumplir con las necesidades cambiantes del negocio. Se realizan cambios a la política cuando se requieren.	
--	--	--	----------	---	--	--	---	--

						trar el riesgo.		
		Verifica- ción de seguridad mientras que se procuran nuevos programas y soporte lógico	No se llevan a cabo ve- rifica- ciones de segu- ridad cuando se pro- cura nuevo soporte lógico.	Existe un procedi- miento in- formal con el que se estiman nuevos programas y soporte lógico an- tes de po- nerse en el ambien-	Hay un procedi- miento do- cumentado que es se- guido an- tes que se adquiera cualquier soporte lógico. Esto ase- gura que	Una parte específica es respon- sable por definir y mantener las guías de verifi- cación de seguridad de soporte lógico. Mo- dificacio-	Las verifi- caciones de seguridad se revisan re- gularmente para asegu- rar que cum- plan con las necesidades cambiantes del negocio. Hay un aná- lisis de	

				te opera- cional.	todo el soporte lógico ad- quirido cumpla con las guías de seguri- dad de la compañía.	nes a los paquetes suministra- dos por distribui- dor se rea- lizan para cumplir con los reque- rimientos del sistema y consenti- miento del distribui- dor se ob- tiene antes	riesgo regu- lar realiza- do para afirmar la seguridad de sistemas existentes y compromiso a su seguridad se controla. Se da enfa- sis en cer- tificación de calidad de nuevos productos	
--	--	--	--	----------------------	--	---	---	--

						de hacerlo		
X.2	Seguridad en sistemas de aplicación	Control de validación mientras que se alimentan datos al sistema de aplicación Validación de datos de información almacenada Validación	No hay validación de información en sistemas de aplicación.	Existe un proceso informal en donde los datos tanto se verifican antes de alimentar-se en aplicaciones como se verifican datos	Hay una norma publicada que describe las pruebas de validación que se realizan. Se sigue un proceso documentado.	Una parte específica es responsable por definir y mantener las guías de control de validación.	El procedimiento de control de validación se revisa regularmente para asegurar que cumple con las necesidades cambiantes de los negocios. Se realizan au-	

		de datos de salida		existentes. Pruebas básicas como datos incompletos o faltantes, caracteres inválidos y campos, se realizan en una base ad-hoc.			ditorias periódicas de datos en sistemas de aplicación para asegurar cumplimiento. Se anotan excepciones, documentan y se toma acción correctiva.	
--	--	-----------------------	--	--	--	--	---	--

X.3	Controles criptográ- ficos	Controles criptográ- ficos	No hay contro- les cripto- gráficos o archi- tectura del sis- tema existen- te no soporta cripto- grafía.	Hay una práctica informal empleada con lo que algunos archivos se cifran. Esto se realiza a discreción del usua- rio en una base ad- hoc.	Hay un procedi- miento do- cumentado que define las etapas que esta- blecen que clasifica- ciones de documentos se requie- ren cifrar y el pro- ceso a se-	Una parte específica responsable por definir y mantener las guías de control de cripto- grafía. Procedi- mientos de administra- ción de claves se- parados se	Los controles criptográfi- cos se revi- san regular- mente para asegurar que cumplen con las necesida- des cambian- tes del nego- cio. Se lle- van a cabo auditorías regularmente para asegurar	
-----	----------------------------------	----------------------------------	--	---	--	---	---	--

					guir para lograrlo.	utilizan para firmas digitales y cifrado.	que la infor- mación que debería ser cifrada se mantenga ci- frada y que el método de cifrado em- pleado sea adeuado.	
		Vulnerabi- lidad de claves criptográ- ficas. El sistema de	No hay procedi- mientos de admi- nistra- ción de	Hay un proceso en vigor con lo que existe ad- ministra-	Hay un sistema de adminis- tración de claves do- cumentado	Una parte específica responsable por definir y mantener el sistema	El sistema de administra- ción de cla- ves se revisa regularmente para asegurar	

		adminis- tración de claves. Documenta- ción del sistema de adminis- tración de claves (fecha de activación y desacti- vación, informa- ción de certifica-	claves.	ción de claves convenien- te o ade- cuada, con base en un juego in- formal de normas, procedi- mientos y métodos seguros.	que define las etapas a seguir. Esto ase- gura que el tipo de algoritmo y longitud de claves se consi- deren para identifi- car nivel de protec- ción crip- tográfica.	de adminis- tración de claves. Se utilizan procedi- mientos de administra- ción de claves se- parados pa- ra firmas digitales y cifrado. Claves criptográ- ficas tienen	que cumple con las nece- sidades cam- biantes del negocio. Ne- cesidades de administra- ción de cla- ves se revi- san y se rea- lizan cambios cuando sean necesarios. Se llevan a cabo audito- rias para	
--	--	--	---------	---	---	--	---	--

		do)				fechas de activación y desactivación de finidas. Las claves están protegidas contra modificación y destrucción en caso de compromiso de claves privadas.	asegurar que la organización mantiene una autoridad de certificación reconocida para asegurar protección de claves y administración de claves eficiente.	
--	--	-----	--	--	--	--	--	--

X.4	Seguridad de archivos de sistema	Protección en control de datos de prueba de sistema. Procedimiento control de cambios. Control de soporte lógico operacional.	No hay procedimiento de control de cambio en vigor y no hay disposiciones para la protección de datos de prueba de sis-	Existe un procedimiento informal para control de cambios. Esta tarea se realiza en una base ad-hoc.	Hay una norma documentada disponible para empleos que describen los procedimientos a seguir para asegurar que los procedimientos de control de cambio	Una parte específica responsable por definir y mantener las guías de control de cambio. Control de versión para actualización de soporte lógico se mantiene y se mantie-	La política de control de cambios se revisa regularmente para asegurar que cumple con las necesidades del negocio. Registros de control de versión se auditan y se documentan	
-----	----------------------------------	---	---	---	---	--	---	--

			tema.		de cambios se sigan correcta- mente	nen archi- vos de to- das las versiones.	cualquier ex- cepciones, anotan y se toma de ser necesario ac- ción correc- tiva.	
X.5	Seguridad en desa- rrollo y procesos de sopor- te.	Conscien- cia de ac- tualiza- ción de soporte lógico pa- ra mejorar el nivel de seguri-	No hay proceso en vigor para su- pervisar el ries- go de seguri- dad pre-	Un proce- dimiento informal existe pa- ra super- visar los sitios de red de distribui-	Hay una norma do- cumentada disponible a los em- pleados que des- cribe los procedi-	Una parte específica responsable por definir y mantener guías de actualiza- ción de so- porte lógi-	La política de la actua- lización de soporte lógi- co se realiza regularmente para asegurar que cumple con las nece-	El nuevo so- porte lógico se pone en un ambiente de prueba para verifi- car anoma- lías con po- líticas de

		dad.	sentado por so- porte lógico instala- do en las má- quinas. Actuali- zación de so- porte lógico no toma en cuen- ta la	dor para obtener actualiza- ciones de soporte lógico. Estas ta- reas se realizan en una ba- se ad-hoc. Aspectos de seguri- dad defi- nidos por los dis-	mientos a seguir pa- ra asegu- rar que todo so- porte ló- gico ins- talado en sus máqui- nas sea la última versión. Todos los aspectos de seguri- dad con la	co. Un ar- chivo se mantiene de todas las actualiza- ciones de soporte ló- gico. Pro- cedimientos de control de cambio y convenios contractua- les existen para esca- lar los as-	sidades cam- biantes del negocio. Au- ditorías pe- riódicas se realizan de actualizacio- nes de sopor- te lógico pa- ra asegurar cumplimiento. Se anotan ex- cepciones, documentan y se lleva a cabo acción	seguridad antes de im- plementa- ción.
--	--	------	---	--	---	--	--	---

			seguri- dad de las nue- vas ver- siones.	tribuido- res solo son consi- derados.	nueva ver- sión espe- cífica a una plata- forma de sistema organiza- cional se identifi- can y con- firman con el distri- buidor	pectos de seguridad a niveles apropiados y remediar- los.	correctiva.	

XI.1	Aspectos de administración de continuidad de negocio.	Contenidos de proceso de continuidad de negocios, procedimientos y programas incluidos en el proceso.	Sin plan.	Hay algún conocimiento de qué hacer en caso de desastre (por ejemplo con base en entrenamiento o de experiencia previa) pero no en proceso	Hay un plan escrito y adecuada-mente distribuido. El proceso incluye: - Procedimientos de retroceso -Procedimientos de reanudación	Los empleados se entrenan y el entrenamiento se renueva periódicamente. El plan incluye métodos de comunicación alternos si la comunicación se afecta se-	Incluye el proceso para mejora después de invocación	Análisis de riesgo de procesos de negocios críticos. Identifica eventos que pueden provocar interrupciones a procesos de negocios e incluye evaluación de impacto de esas interrupciones.
------	---	---	-----------	--	--	---	--	---

				documenta- do.	- Progra- mas de manteni- miento	veramente. El proceso incluye: - Asigna- ción de responsabi- lidades - Condi- ciones para activación		
		Desarrollo de proceso de conti- nuidad de negocios prueba de	El plan no exis- te. Al- guna cons- ciencia	Un conjun- to de me- didas pue- de apli- carse en caso de	Hay un proceso de continui- dad de ne- gocios es- crito que	El respon- sable en la cadena de administra- ción para ejecutar el	El proceso se revisa en caso de cambio de sistema, personal,	Proceso de continuidad de negocios cubre eventos que son espe- cíficos al

		procesos de continuidad de negocios revisión y actualización de procesos de continuidad razones para provocar revisión del plan	de medidas que pueden tomarse en caso de interrupción de negocio. Acciones ocurrirán en una forma ad-hoc.	interrupción de negocios. No constituyen un plan formal, definido, publicado o administrado.	incluye riesgos, eventos, papeles y responsabilidades, medidas técnicas, reportes y comunicaciones. El plan se ha probado al menos una vez.	proceso de continuidad de negocios es definido, y todos los administradores y personal saben cual es la cadena. Ocurre prueba al menos anualmente y mantiene la conti-	contratista y recuperación de desastre o contrato, negocios, aplicación, ubicaciones o legislación. Revisiones post-mortem después de ejecución con acciones de me-	ambiente local (es decir inundación, falta de energía, inestabilidad política, incendio, huracán, terremotos, etcétera) y necesidades de negocios (es decir centro de tarjeta de crédito no
--	--	---	---	--	---	--	---	---

						nuidad del negocio	jora docu- mentada.	puede estar inoperativo más de unos cuantos minu- tos).
XII.	Cumpli- 1 miento con los reque- rimientos legales.	Restric- ciones en vigor en el uso de materiales a los cua- les puede haber de- rechos de	No hay restric- ciones en vi- gor.	Restric- ción ad- hoc en al- gunos do- cumentos solamente.	Restric- ciones sistemáti- cas, docu- mentadas, con base en clasi- ficación de infor-	Clara res- ponsabili- dad por po- ner en vi- gor las restriccio- nes. Se proporciona entrena-	Revisión periódica de la polí- tica para continuar la mejora. Revisión periódica de las res-	Política de procedimien- tos de adqui- sición infor- mación de conciencia de Derechos de Autor Mante- nimiento de

		propiedad intelec- tual.			mación.	miento. Los empleados están con- cientes.	tricciones para asegu- rar que son apropiadas.	licencias ve- rificación de soporte lógi- co conteni- do/empleado política en desecho de soporte lógi- co, cumpli- miento con licencias.
		Protección contra pérdida, destruc- ción o	No hay protec- ción em- pleada. No hay	Algunos datos de organiza- ción res- paldados y	Claras responsa- bilidades para ase- gurar que	Proteccio- nes en vi- gor que cu- bren todos los regis-	Revisión periódica de sistemas en vigor y sistemas de	Información de personal, información de derechos de autor in-

		falsifica- ción de registros organiza- cionales.	jerar- quía de- finida en cuan- to a quién tiene acceso a qué in- forma- ción.	asegura- dos. Res- paldos pueden mantenerse en vigor. No se man- tienen re- gistros de actividad de usua- rio.	los regis- tros de la organiza- ción no están com- prometi- dos. Algo de activi- dad del usuario se registra. Rasgos de organiza- ción se mantienen en forma	tros orga- nizaciona- les. Entre- namiento proporcio- nado para educar a los usua- rios. Admi- nistración responsable para asegu- rar que se mantengan registros precisos y	seguridad que tratan con regis- tros de or- ganiza- ción. Cada incidente está sujeto a un proce- dimiento post-mortem que incluye una revi- sión de si las políti- cas aplica-	formación confidencial de la compa- ñía, sitios de red públi- cos.
--	--	--	--	---	---	--	---	---

					segura. Están públicamente disponibles los documentos que describen política y procedimientos que los empleados deberán seguir para mante-	seguros. Derechos y privilegios de acceso en vigor para restringir acceso a ciertos registros organizacionales. Si- tios de red protegidos contra de- formación.	bles fueron correctamente comunicadas. Se enseña a los usuarios los procedimientos de reportes de incidentes Se mantienen registros completos de auditoría	
--	--	--	--	--	---	---	---	--

					ner la in- tegridad y seguridad de regis- tro de in- formación.	Archivos críticos identifica- dos y pro- tegidos contra fal- sificación por verifi- caciones CRC, etcé- tera.	con tiempos de ini- cio/fin del sistema, errores del sistema y acción co- rrectiva y nombre de la persona que hace alteracio- nes a la informa- ción.	
--	--	--	--	--	--	---	---	--

		Cumpli- miento con legisla- ción de protección de datos.	Conoci- miento de le- gisla- ción es- tá limi- tado a personas o depar- tamentos especí- ficos (HR, le- gal, et- cétera) y no es-	Legisla- ción de protección de datos se discute con em- pleados y personal bajo con- trato o temporal al contra- tarse en departa- mentos es- pecíficos.	La legis- lación se aplica y la legis- lación de protección de datos se hace disponible a los em- pleados en un sitio centrali- zado. Im- pacto en legisla-	Procesos y procedi- mientos se ponen en práctica para super- visión a fin de ase- gurar que la compañía cumpla en forma con- tínua. La responsabi- lidad de hacerlo es-	Hay un pro- ceso regu- lar en vi- gor para revisar cambios en legislación o nuevas necesidades del nego- cio. Se proporciona entrena- miento a los usua- rios para	
--	--	---	--	---	--	--	---	--

			tá docu- mentado.		ción y da- tos invo- lucrados ha sido escrito y disponible a todos los em- pleados. Todos los procesos afectados incluyen etapas de protección adecuada.	tá clara- mente asig- nada.	asegurar el cumplimien- to continuo con la le- gislación. El proceso y la res- ponsabili- dad para recibir, investigar y corregir cualquier excepción reportada se definen.	
--	--	--	----------------------	--	---	-----------------------------------	--	--

		Cumpli- miento de sistemas de infor- mación con normas pu- blicadas o códigos de práctica.	No hay códigos de prác- tica pu- blicados y no hay conciencia.	Normas y códigos de práctica se entien- den en ge- neral pero se aplican inconsis- tentemente a través de la or- ganización	Normas de códigos de práctica se definen y publican interna- mente y se hacen dis- ponibles a los em- pleados en un sitio centrali- zado.	Una persona o entidad claramente designada tiene res- ponsabili- dad por re- visar, man- tener y en- trenar a los usua- rios en las normas pu- blicadas o códigos de práctica.	Hay un proce- so regular en vigor para revisar cam- bios en las normas publi- cadas o códi- gos de prác- tica. Hallaz- gos de incum- plimiento re- sultan en ac- ción correc- tiva.	Derechos de Propiedad Intelectual Acta de Pro- tección de Datos
--	--	--	--	--	--	---	--	--

XII.	Revisión	Documenta-	No exis-	Existe al-	Documentos	Se asignan	Los documen-	Leyes de
2	de políti-	ción de	te docu-	go de do-	se hacen	responsabi-	tos se crean	protección
	ca de se-	requeri-	menta-	cumenta-	pública-	lidades a	tan pronto	y/o correc-
	guridad y	mientos	ción.	ción aun-	mente dis-	individuos	como hay un	ción de in-
	cumpli-	regulato-		que no cu-	ponibles	para produ-	cambio en los	formación a
	miento	rios y		bre todos	en el si-	cir docu-	requerimien-	personal
	técnico.	contrac-		los deta-	tio de red	mentos tan	tos contrac-	(empleados
		tuales pa-		lles de	corporati-	pronto como	tuales o re-	y/o clien-
		ra cada		los reque-	vo o en un	un nuevo	gulatorios	tes, proove-
		sistema de		rimientos	tablero de	sistema es	del proyecto.	dores, etcé-
		informa-		regulato-	avisos al	fuelle.	La documenta-	tera).
		ción.		rios/con-	público.	Existen	ción está	Procedimien-
				tractuales	Completa	plantillas	disponible al	tos para
				por cada	documenta-	para la	personal con	descripción
				IS. No hay	ción exis-	creación de	acreditación	a autorida-
				plantilla	te para	documentos	correcta. In-	

				de docu- mento es- tándar empleado, los docu- mentos se crean como y cuando se requie- ran por empleados individua- les, no hay un al- macena- miento de	requeri- mientos contrac- tuales re- gulatorios para todos los siste- mas de in- formación en la or- ganiza- ción.	y hay un depósito central en donde se almacenan. Las planti- llas tienen propieta- rios desig- nados.	ventario pe- riódico de sistemas de información incluye veri- ficaciones que existen requerimien- tos para cum- plir. Excep- ciones acti- van un proce- so bien defi- nido para procedimien- tos de revi-	des adecua- das. Requerimien- tos ISO 9000 Agencias re- gulatorias (por ejemplo FDA o FCC en los E.U.A.)
--	--	--	--	---	---	--	--	--

				datos cen- tral para los docu- mentos (requerido para pre- guntar a la persona o personas que saben.			sión a fin de eliminar este riesgo.	
XII. 3	Considera- ciones de auditoría de siste- ma.	Control contra mal uso de computado- ras, pro- tección de	No hay contro- les o protec- ción en vigor.	Términos de uso de equipo de computado- ras se discuten	Términos de uso de equipos de computado- ra de las organiza-	La respon- sabilidad de los ad- ministrado- res está definida.	Revisiones periódicas de quién está autorizado a hacer qué. Información	

		herramientas de auditoría para evitar mal uso.		con empleados y personal bajo contrato o temporal al contratar.	ciones están disponibles de un sitio centralizado (sistema intranet, tablero de avisos de oficina, etcétera).	Herramientas empleadas para supervisar el uso de equipo de computadora. El personal tiene bien definidos papeles y derechos de acceso a sistemas de temas de archivos de	recolectada de herramientas de supervisión se utiliza para tomar decisiones para política futura. Hay un procedimiento de revisión de incidentes. Intentos de intrusión "de sombrero blanco" pe-	
--	--	--	--	---	---	--	--	--

						computado- ra. El per- sonal está consciente de sus ac- tividades relaciona- das a la computadora se supervi- san y en qué medida.	riódicos se realizan y son seguidos por acciones correctivas.	
		Revi- sión/audi- toría de sistemas	No hay proceso en vi- gor.	Se revisan o auditan ocasional- mente si	Revisión a interva- los, pero no hay	Una persona o entidad claramente designada	Hay un meca- nismo defini- do para revi- sar y actua-	

121

		de infor- mación pa- ra asegu- rar que cumplen con polí- ticas y normas de seguridad.		lo pide la adminis- tración en jefe, au- ditores, etcétera.	responsa- bilidad de adminis- tración clara para activar revisiones de resul- tados de explota- ción.	tiene res- ponsabili- dad por el proceso y lo revisa regularmen- te.	lizar la po- lítica des- pués de cada incidente de seguridad (¿falta algo en la políti- ca que pudie- ra haber evi- tado el pro- blema?).	
		Cobertura de regimen de sistema (registro de even-	No exis- te co- bertura.	Pocas pro- tecciones en vigor. Herramien- tas de au-	Claras responsa- bilidades para ase- gurar que	Herramien- tas de au- ditoría so- lo estan disponibles	Protecciones en vigor cu- bren todas las herra- mientas de	

		tos)		ditorfa no se admi- nistran seguramen- te y el acceso de usuario no se super- visa.	las herra- mientas de auditorfa no se usen mal. En- trenamien- to se pro- porciona para edu- car a los usuarios.	para uso por perso- nal clave. Derechos y privilegios de acceso se ponen en vigor para mantener la seguridad.	auditorfa. Revisi3n pe- ri3dica de sistemas en vigor y segu- ridad de sis- temas que au- ditan los sistemas. Los usuarios son educados respecto a la importancia de proteger sus herra- mientas de	
--	--	------	--	---	--	--	---	--

							auditoría.	
		Cumpli- miento de sistemas de infor- mación con normas pu- blicadas o códigos de práctica.	No hay códigos de prác- tica pu- blicados y no hay conciencia.	Normas y códigos de práctica en general se entien- den pero se aplican inconsis- tentemente a través de la or- ganiza- ción.	Normas y códigos de práctica se definen y publican interna- mente y se hacen dis- ponibles a los em- pleados en un sitio centrali-	Una persona o entidad claramente designada tiene res- ponsabili- dad para revisar, mantener y entrenar a los usua- rios en las normas pu-	Hay un proce- so regular en vigor para revisar cam- bios en nor- mas publica- das o códigos de práctica. Hallazgos de incumplmien- to resultan en acción co- rrectiva.	Derechos de Propiedad Intelectual, Derechos de Autor, Acta de Protec- ción de Da- tos.

					zado.	blicadas o códigos de práctica.		
--	--	--	--	--	-------	---------------------------------------	--	--

[0026] Con referencia a la Matriz de Evaluación de Seguridad mostrada en la Tabla 1, para realizar la evaluación para un ítem determinado, la entidad de evaluación solo requiere realizar las siguientes etapas:

- 5 (i) encontrar el ítem en cuestión, primero por categoría, luego por sub-categoría; (ii) leer las descripciones bajo cada nivel de madurez y determinar si se satisfacen los requerimientos de este nivel de madurez; y (iii) registrar el más alto nivel de madurez para este ítem que se
- 10 satisfaga por las políticas y prácticas de seguridad de información actual de la organización.

[0027] Una vez que se ha completado la calificación preliminar, puede exhibirse en una forma gráfica. En una modalidad de la invención, la calificación preliminar se exhibe utilizando una Herramienta para Reporte

15 de Evaluación de Madurez de Seguridad (SMART = Security Maturity Assessment Reporting Tool). SMART permite que la calificación preliminar sea mostrada a un nivel detallado, es decir todos los 61 elementos se ilustran, o a

20 un nivel de compendio, es decir solo 10 amplias categorías se muestran. Además, SMART permite a la organización comparar la calificación preliminar con una meta preliminar, un promedio de industria, o con una evaluación previa. Adicionalmente, la distribución del repor-

te SMART, permite a una organización fácilmente identificar áreas que requieren mejora.

[0028] La Figura 3 ilustra una porción de un reporte SMART de acuerdo con una o más modalidades de la invención. Una primer columna (10) cita las amplias categorías. Una segunda columna (12) cita los ítems dentro de cada una de las categorías. Una tercer columna (14) representa gráficamente la "Madurez de Capacidad Evaluada" (ACM = Assessed Capability Maturity) (16). La tercer columna se subdivide en 5 niveles (L1, L2, L3, L4, y L5) que corresponden a los niveles de madurez citados anteriormente. Por cada ítem, la ACM se representa al sondear la hilera correspondiente hasta el nivel apropiado. Si la ACM no está en una meta (18), es decir el nivel en el cual la organización desea estar para el ítem particular, entonces está presente un sombreado adicional que representa un espacio (20) entre la meta (18) y la ACM (16).

[0029] Por ejemplo, en la Figura 3, la categoría contiene cuatro ítems: ítem D (2), ítem E (4), ítem F (6), e ítem G (8). Específicamente, viendo al ítem (8), la ACM (16) está a un nivel 2 (22), mientras que la meta (18) está a un nivel 3 (24). De esta manera, está presente un espacio (20) entre el nivel 2 (22) y nivel 3 (24) en la hilera que contiene el ítem G (8). De esta

manera, la organización puede ver fácilmente que el ítem G (8) está por debajo de la meta (18). Por contraste, la organización también puede fácilmente ver que ese nivel de madurez de capacidad para el ítem F (6) está en la meta (26) establecida para este ítem, de manera tal que no hay espacio respecto al ítem F (6).

[0030] Regresando a la fase SMA, una vez que se ha completado la calificación preliminar, la entidad de evaluación realiza la calificación preliminar con la organización. Durante la revisión, puede revisarse la calificación preliminar de ser necesario. Una vez que se ha completado, se genera una calificación final.

[0031] Durante la fase del plan de acción correctivo (CAP), el CAP se genera utilizando la calificación final y la matriz de evaluación de seguridad. Las acciones propuestas son dirigidas o son destinadas a mejorar los ítems que tienen espacios y llevar los ítems hasta la meta. Adicionalmente, a los ítems en CAP también se les puede asignar prioridades de acuerdo con las necesidades y recursos de la organización. Durante la fase de ejecución del plan de acción correctivo, CAP se ejecuta. Por ejemplo, si la SAM establece que para un cierto ítem esté a un nivel 3, la política es escrita, y para estar a nivel 4, "hay un administrador asignado a

cargo de aplicar esta política", entonces se concluye que si una organización se estima a nivel 3 para este ítem, y su meta es estar a nivel 4, entonces CAP deberá incluir la siguiente acción: "poner un administrador a cargo de esta política".

[0032] La fase de supervisión de SMA incluye reportes periódicos SMART para asegurar que las metas se cumplan y mantengan. Además, durante esta fase, la entidad de evaluación puede necesitar cambio en el ambiente que pueda requerir adiciones o cambios en las prácticas y/o políticas de seguridad. Adicionalmente, durante la fase de supervisión, la entidad de evaluación puede proporcionar asistencia para indagar en la organización en el caso de un incidente de seguridad de información. En una o más modalidades de la invención, es opcional la fase de supervisión.

[0033] La Figura 4 ilustra un diagrama de flujo que detalla el método SMA de acuerdo con otra modalidad de la invención. Inicialmente, las metas de negocios de la organización se determinan (etapa 112), así como el riesgo asociado en términos de seguridad de información (etapa 114). Documentación escrita luego se captura respecto a las políticas y prácticas de seguridad de información existentes en la organización (etapa 116). Luego

se captura información adicional por entrevistas (etapa 118). Utilizando la información capturada en las etapas 112 a 118, la calificación SAM se genera (etapa 120). Si se obtiene información adicional (etapa 122), entonces
5 puede repetirse la etapa 120. Si no se obtiene información adicional (etapa 122), entonces se propone una lista de acciones correctivas (etapa 124). A las acciones correctivas subsecuentemente se les asignan prioridades (etapa 126) y ejecutan (etapa 128) para generar políticas
10 y procedimientos de seguridad de información modificada. Las políticas de procedimientos de seguridad de información modificadas luego se supervisan (etapa 130). Si hay un cambio en el ambiente de seguridad de información, por ejemplo una primera organización se fusiona con una se-
15 gunda organización resultando en que la red de la primer organización se integre en la red de la segunda organización, o si llega el tiempo para una revisión periódica (etapa 132) entonces el proceso pasa de regreso a la etapa 116.

20 [0034] La invención, en una o más modalidades, puede tener una o más de las siguientes ventajas: el método SMA es un enfoque sistemático que incluye un proceso, un método detallado para evaluación (es decir SAM) y una herramienta de reporte (es decir SMART). Además, el

método SMA cubre todos los aspectos de seguridad de información y define explícitamente lo que cada nivel significa para cada ítem. Además el método SMA está orientado por acción. Además, cada ítem se estima como una
5 madurez de capacidad en vez de aprueba o pasa/falla, permitiendo a una organización fácilmente medir donde está la organización respecto a un ítem de seguridad de información particular y medir el avance con el tiempo o con toda la meta, incluso si este avance es gradual. Adicionalmente, la matriz de evaluación de seguridad puede utilizarse como una lista de recomendaciones para detallar como la organización puede alcanzar sus metas de seguridad de información.
10

[0035] Además, el método SMA es fácil de aplicar, ya que cada ítem y juego correspondiente de criterios por cada nivel de madurez asociado con el ítem se definen claramente. Además, el método SMA es flexible, ya que puede utilizarse para múltiples propósitos, por ejemplo, el SMA puede utilizarse con el propósito de establecer a un cliente o autoridad regulatoria, que una
15 organización tiene la capacidad requerida para realizar una cierta tarea. SMA también puede utilizarse con el propósito de supervisar internamente, con el tiempo, las mejoras decididas por la administración de la organiza-
20

ción. SMA también puede utilizarse con el propósito de satisfacer una cierta norma de la industria o alcanzar una meta establecida a través de análisis de las capacidades de seguridad de la competencia.

5 [0036] Además, la invención produce una calificación objetiva de las prácticas y políticas de seguridad de información de una organización retirando el elemento subjetivo de un proceso de evaluación.

 [0037] Mientras que la invención se ha descrito con respecto a un número limitado de modalidades, aquellos con destreza en la especialidad, que tengan el beneficio de esta descripción, apreciarán que pueden diseñarse otras modalidades que no se apartan del alcance de la invención como aquí se describe. De acuerdo con
10 esto, el alcance de la invención habrá de limitarse solo
15 por las reivindicaciones anexas.

REIVINDICACIONES

1. Un sistema de computadora para estimar una política y práctica de seguridad de información de una organización, caracterizado porque comprende: un procesador; una memoria; un medio de alimentación; e instrucciones de programa o soporte lógico almacenadas en la memoria para permitir al sistema de computadora bajo el control del procesador, para: determinar un riesgo asociado con la política y práctica de seguridad de información; capturar información respecto a la política y práctica de seguridad de información utilizando los medios de alimentación; generar una calificación utilizando una matriz de evaluación de madurez de seguridad, la información capturada y el riesgo asociado con la política y práctica de seguridad de información y generar una lista de acciones correctivas utilizando la calificación.

2. El sistema de computadora de conformidad con la reivindicación 1, caracterizado porque además comprende instrucciones de soporte lógico almacenadas en la memoria para permitir al sistema de computadora, bajo el control del procesador, que: genere una nueva calificación utilizando la matriz de evaluación de capacidad de seguridad, cuando hay un cambio en un ambiente de seguridad de información de la organización.

3. El sistema de computadora de conformidad con la reivindicación 1, caracterizado porque además comprende instrucciones de soporte lógico almacenadas en la memoria para permitir al sistema de computadora, bajo el control del procesador que: genere una evaluación gráfica de la calificación.

4. El sistema de computadora de conformidad con la reivindicación 3, caracterizado porque la evaluación gráfica de la calificación se genera por una herramienta para reporte de evaluación de madurez de seguridad, que se ejecuta en el sistema de computadora.

5. El sistema de computadora de conformidad con la reivindicación 4, caracterizado porque la herramienta para reporte de evaluación de madurez de seguridad comprende funcionalidad para dar seguimiento a la calificación de la política y práctica de información de seguridad con el tiempo.

6. El sistema de computadora de conformidad con la reivindicación 4, caracterizado porque la herramienta para reporte de evaluación de madurez de seguridad comprende funcionalidad para comparar gráficamente la calificación con una meta de calificación.

7. El sistema de computadora de conformidad con la reivindicación 1, caracterizado porque la recolec-

ción de información comprende recolectar documentación que detalla la política y práctica de seguridad de información de la organización.

8. El sistema de computadora de conformidad
5 con la reivindicación 1, caracterizado porque la matriz de evaluación de seguridad comprende una matriz en donde cada una de una pluralidad de columnas denota un nivel de madurez y cada una de una pluralidad de hileras denota una característica de seguridad de información particular
10 de manera tal que la intersección de una de la pluralidad de columnas con una de la pluralidad de hileras es un nivel de madurez de capacidad.

9. El sistema de computadora de conformidad con la reivindicación 8, caracterizado porque cada una de
15 la pluralidad de hileras es un agrupamiento de los ítems de la Institución de Normas Británica 7799 (British Standard Institution 7799).

10. El sistema de computadora de conformidad con la reivindicación 8, caracterizado porque cada una de
20 la pluralidad de hileras es un agrupamiento de un conjunto de controles que establecen las prácticas de mejor modo en seguridad de información.

11. El sistema de computadora de conformidad con la reivindicación 8, caracterizado porque cada una de
25 la pluralidad de hileras es un agrupamiento de los ítems

de la Organización Internacional para Normalización 17799 (International Organization for Standardization 17799).

5 12. El sistema de computadora de conformidad con la reivindicación 8, caracterizado porque cada una de la pluralidad de columnas es un nivel de madurez definido de acuerdo con el Modelo de Madurez de Capacidad (Capability Maturity Model) del Instituto de Ingeniería de So-

10 13. El sistema de computadora de conformidad con la reivindicación 9, caracterizado porque el agrupamiento de los ítems de la Institución de Normas Británica 7799 (British Standard Institution 7799) comprende una categoría de la Institución de Normas Británica 7799 (British Standard Institution 7799).

15 14. El sistema de computadora de conformidad con la reivindicación 11, caracterizado porque el agrupamiento de los ítems de la Organización Internacional para Normalización 17799 (International Organization for Standardization 17799) comprende una categoría de la Organi-

20 zación Internacional para Normalización 17799 (International Organization for Standardization 17799).

25 15. El sistema de computadora de conformidad con la reivindicación 1, caracterizado porque generar la lista de acciones correctivas, comprende comparar una descripción de un nivel de madurez actual de una organi-

zación por cada uno de una pluralidad de ítems de seguridad de información en la matriz de evaluación de seguridad, con una descripción de un nivel de madurez deseado por cada uno de la pluralidad de ítems de seguridad de información.

16. El sistema de computadora de conformidad con la reivindicación 1, caracterizado porque las acciones en la lista de acciones correctivas se ejecutan para crear una nueva política y práctica de información de seguridad.

17. El sistema de computadora de conformidad con la reivindicación 1, caracterizado porque la nueva política y práctica de información de seguridad se supervisa.

18. Un medio legible por computadora que almacena instrucciones de soporte lógico que incluye la funcionalidad para: determinar un riesgo asociado con la política y práctica de seguridad de información; recolectar información respecto a la política y práctica de seguridad de información utilizando los medios de alimentación; generar una calificación utilizando una matriz de evaluación de madurez de seguridad, la información recolectada, y el riesgo asociado con la política y práctica de seguridad de información; y generar una lista de acciones correctivas utilizando la calificación.

19. El medio legible por computadora de conformidad con la reivindicación 18, caracterizado además porque comprende instrucciones de soporte lógico que incluyen funcionalidad para generar una nueva calificación
5 utilizando la matriz para evaluación de capacidad de seguridad cuando hay un cambio en un ambiente de seguridad de información en la organización.

20. El medio legible por computadora de conformidad con la reivindicación 18, caracterizado además
10 porque comprende instrucciones de soporte lógico que incluyen funcionalidad para generar una evaluación gráfica de la calificación.

21. El medio legible por computadora de conformidad con la reivindicación 20, caracterizado porque
15 la evaluación gráfica de la calificación se genera por una herramienta de reporte de evaluación de madurez de seguridad, en donde las instrucciones de soporte lógico comprenden funcionalidad de la herramienta de reporte de evaluación de seguridad se almacenan en el medio legible
20 por computadora.

22. El medio legible por computadora de conformidad con la reivindicación 21, caracterizado porque la herramienta de reporte de evaluación de madurez de seguridad comprende funcionalidad para dar seguimiento a la

calificación de la política y práctica de información de seguridad con el tiempo.

23. El medio legible por computadora de conformidad con la reivindicación 21, caracterizado porque
- 5 la herramienta de reporte de evaluación de madurez de seguridad comprende funcionalidad para comparar gráficamente la calificación con una meta de calificación.

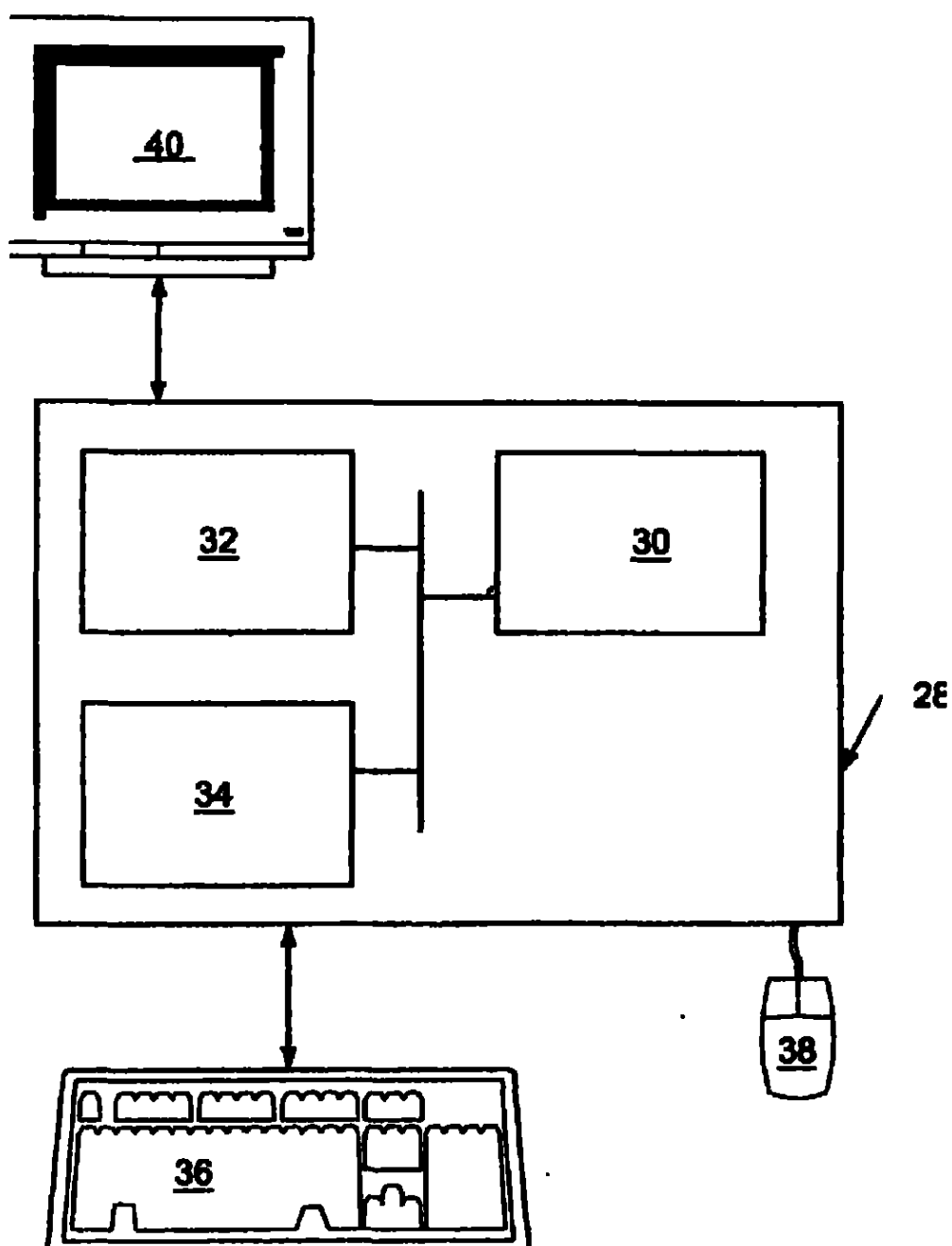


FIGURA 1
(TÉCNICA PREVIA)

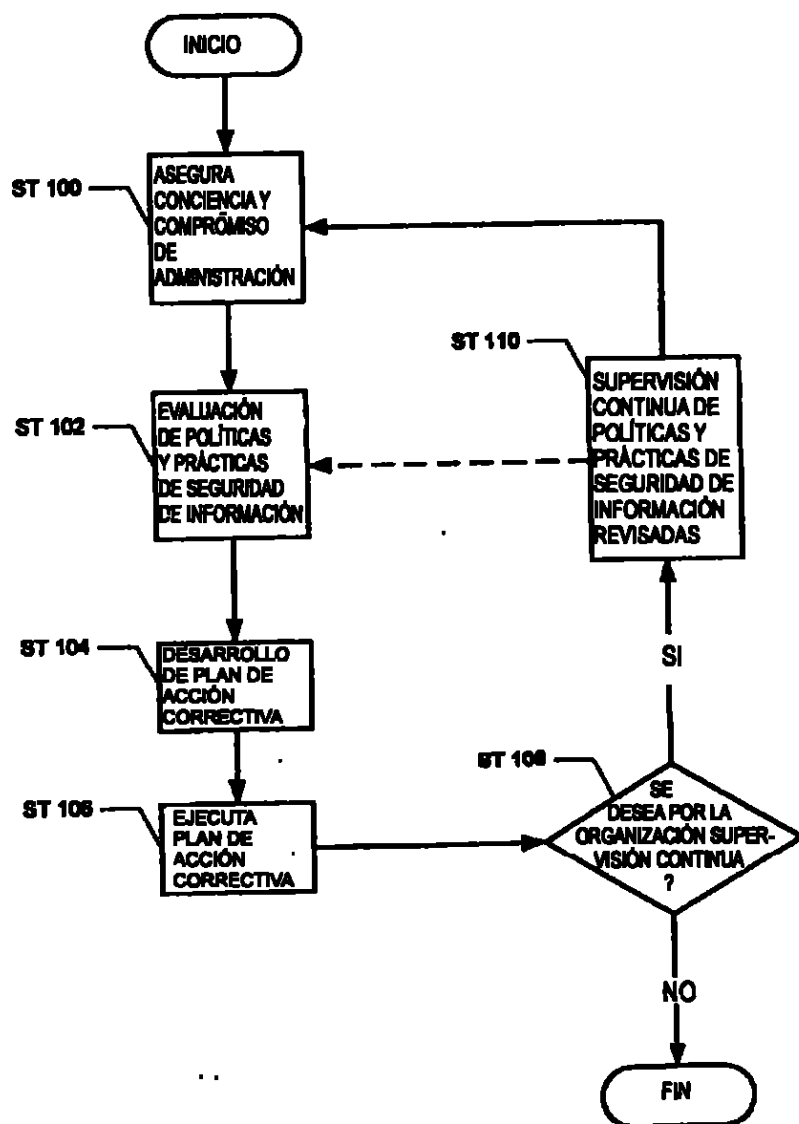


FIGURA 2

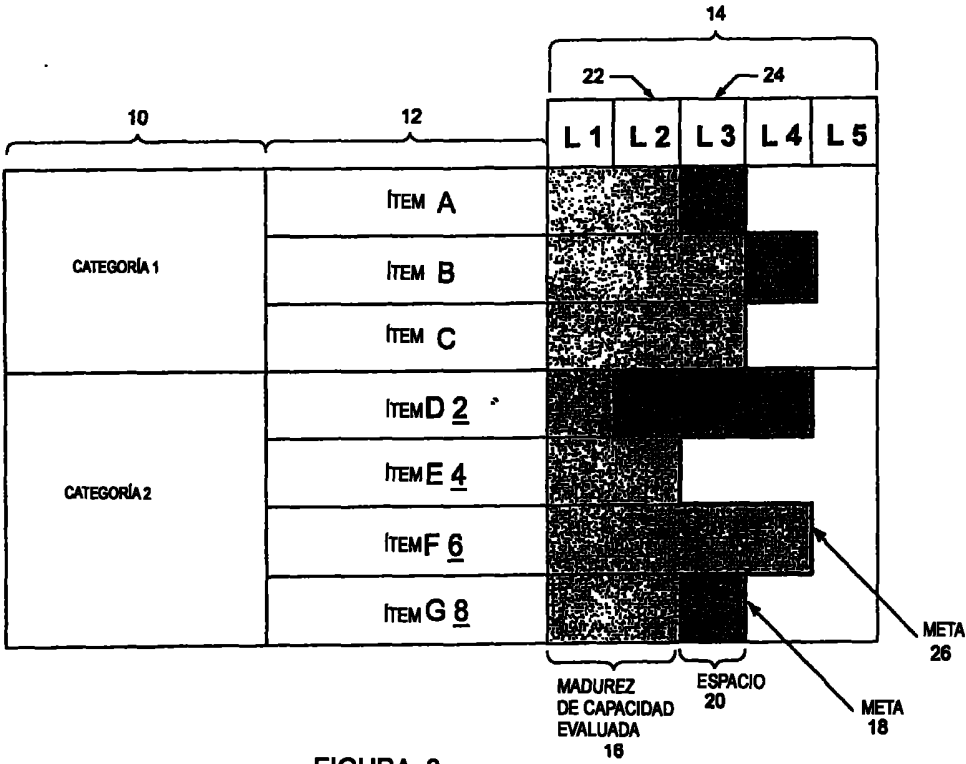


FIGURA 3

12

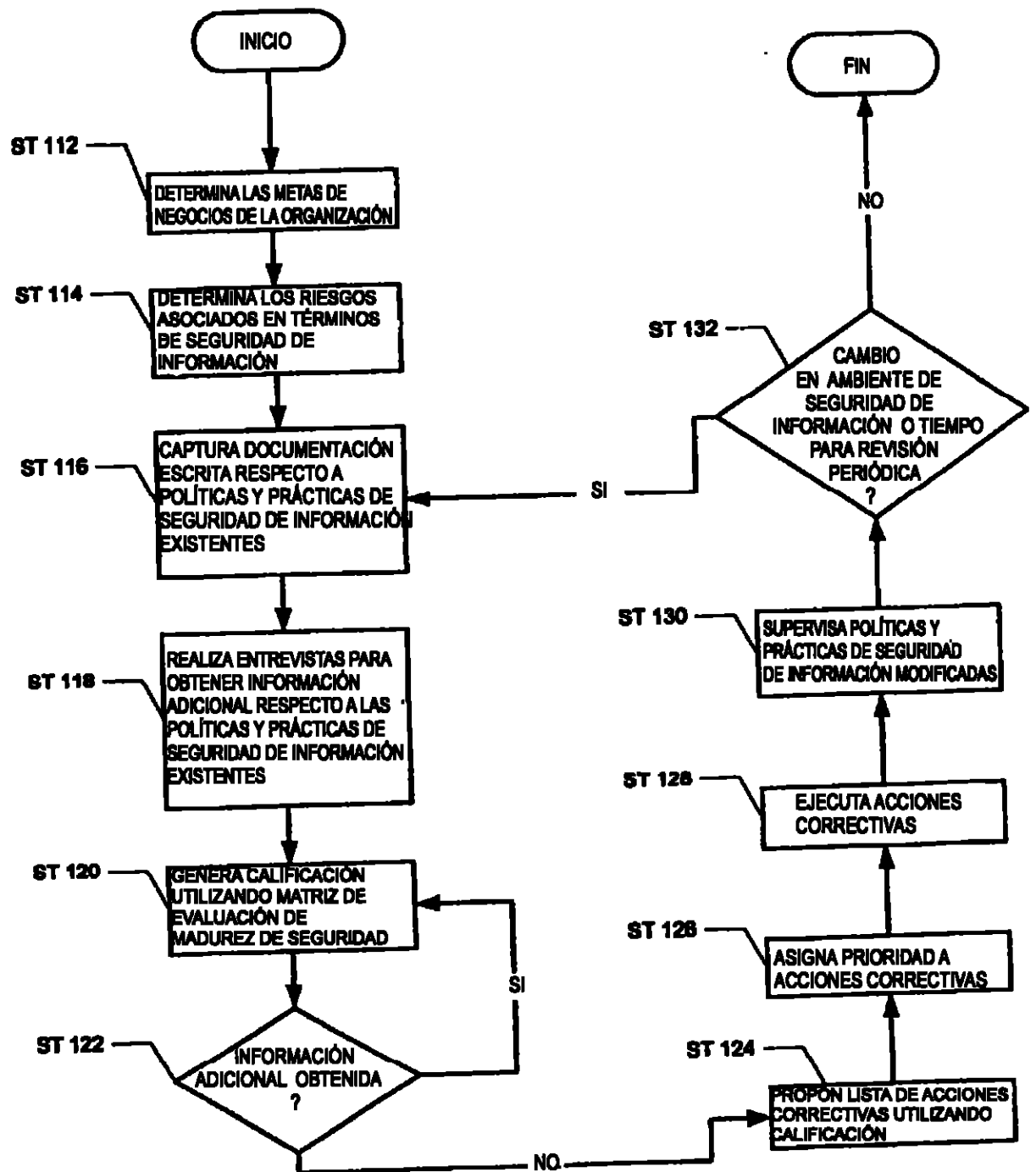


FIGURA 4

161

SUPERINDUSTRIA Y COMERCIO
Radicación : 34116633 88333333 Folios: 163
Fecha (ACD): 2004-11-25 16:18:01
Trámite : 011 PCT-PATENT 379 FASE INCI 411 PRESENTA
Dependencia: 2828 DIVISION DE NUEVAS CREACIONES



Industria y Comercio
SUPERINTENDENCIA

**REQUISITOS MINIMOS PARA ADMISION A TRAMITE
PCT**

PATENTE DE INVENCION [x]

MODELO DE UTILIDAD []

- ◆ Indicación de que se solicita la concesión de una patente [X] 1
- ◆ Datos de identificación del solicitante o de la persona que presenta la solicitud [X] 1
- ◆ Descripción de la invención [X] 1
- ◆ Dibujos de ser estos pertinentes [X]
- ◆ Comprobante de pago de las tasas establecidas [X] 2

COMPLETA [✓]

INCOMPLETA []

DISEÑO INDUSTRIAL []

- ◆ Indicación de que se solicita el registro de Diseño Industrial []
- ◆ Datos de identificación del solicitante o de la persona que presenta la solicitud []
- ◆ Representación gráfica y fotográfica del Diseño Industrial o muestra del material que incorpora el diseño []
- ◆ Comprobante de pago de las tasas establecidas []

COMPLETA []

INCOMPLETA []

ESQUEMA DE TRAZADO []

- ◆ Indicación de que se solicita el registro de un Esquema de Trazado []
- ◆ Datos de identificación del solicitante o de la persona que presenta la solicitud []
- ◆ Representación gráfica del esquema trazado []
- ◆ Comprobante de pago de las tasas establecidas []

COMPLETA []

INCOMPLETA []

Claudia M Neua
Firma Responsable

Fecha _____

Carrera 13 No. 27-00 Piso 5, 7 y 10
Conmutador: 3 82 08 40
Fax: 350 52 20
E-mail: info@slc.gov.co
www.slc.gov.co
Bogotá, D.C., Colombia



**EXTRACTO PARA PUBLICACIÓN
SOLICITUD DE PATENTE DE INVENCION**

No. SOLICITUD INTERNACIONAL : PCT/US2003/013298 (51) INT. CL.: G06F 1/00
(21) No. SOLICITUD:
(22) FECHA DE PRESENTACIÓN: 25-11-04 (71) SOLICITANTE: SCHLUMBERGER OMNES, INC.
(30) PRIORIDAD:
(31) No. DE SOLICITUD: 10/134,815 (72) INVENTOR/ES: BAUDOIN, Claude R. y ELLIOTT, Collin, R.
(32) FECHA DE PRESENTACIÓN: 29-04-02
(33) PAÍS: US (74) REPRESENTANTE ALICIA LLOREDA RICAURTE LEGAL:

(54) TÍTULO:
"MÉTODO PARA EVALUACIÓN DE MADUREZ DE SEGURIDAD"

(57) RESUMEN:

Reivindicación número 1.-

Un sistema de computadora para estimar una política y práctica de seguridad de información de una organización, caracterizado porque comprende: un procesador; una memoria; un medio de alimentación; e instrucciones de programa o soporte lógico almacenadas en la memoria para permitir al sistema de computadora bajo el control del procesador, para: determinar un riesgo asociado con la política y práctica de seguridad de información; capturar información respecto a la política y práctica de seguridad de información utilizando los medios de alimentación; generar una calificación utilizando una matriz de evaluación de madurez de seguridad, la información capturada y el riesgo asociado con la política y práctica de seguridad de información y generar una lista de acciones correctivas utilizando la calificación.

2020
Bogotá, D.C.,

Doctor(a):
ALICIA LLOREDA RICAURTE

Oficio N° 11484

ASUNTO:	Radicación N°	04-118803
	Solicitud internacional	PCT/US03/013298
	Fecha inicio fase nacional	29/11/2004
	Trámite	011
	Evento	379
	Actuación	416
	Folios	001

Como resultado del examen de forma, realizado con fundamento en el artículo 38 de la Decisión 486 de la Comisión de la Comunidad Andina, artículo 27 del Tratado de Cooperación en Materia de Patentes (PCT), regla 51 bis del Reglamento y Circular Única de la Superintendencia de Industria y Comercio, se le comunica que:

- Si fuere el caso, el solicitante debe adjuntar la traducción de los anexos del reporte de examen preliminar internacional (Art. 36.2.b) del tratado PCT).
- La solicitud no contiene la copia del documento en que consta la cesión del derecho a la patente del inventor al solicitante o a su causante. (Art. 26-k) Decisión 486).
- La solicitud no contiene el poder debidamente otorgado, con el lleno de los requisitos exigidos por los artículos 63 y subsiguientes del Código de Procedimiento Civil. Adicionalmente, deberá presentar el documento que acredita la existencia y representación legal de la sociedad solicitante, cuando ésta fuere persona jurídica.
- El solicitante debe aclarar si la solicitud corresponde al capítulo I o II del PCT por que la indicación en el petitorio no corresponde a los documentos del expediente, en caso necesario adjuntar los documentos que corresponden.

En cumplimiento de lo dispuesto por el artículo 39 de la Decisión 486, se le requiere para que dentro del término de dos meses siguientes a la fecha de notificación del presente oficio, complete los requisitos anteriormente enunciados. En caso de no dar cumplimiento al presente requerimiento, la solicitud se considerará abandonada y perderá su prelación.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 5.2, literal e), del capítulo quinto del título primero de la Circular Única N° 10 de 2001.

ALIX CARMENZA CESPEDES DE VERGEL
Jefe de la División de Nuevas Creaciones.

El anterior requerimiento fue notificado por fijación en lista de fecha, 17 dic. 2004.

202047