



SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 11-050985-00000-0000

Fecha: 2011-04-26 16:44:30 Dep. 2020 DIR.NUEVASCR
Tra. 2 PATENTES Evs: 1 REGDEPOSITO
Act. 411 PRESENTACION Folios: 41

Industria y Comercio

SUPERINTENDENCIA

11-50985

DELEGATURA DE PROPIEDAD INDUSTRIAL

DIRECCIÓN DE NUEVAS CREACIONES

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
INVENTARIO

Je

SOLICITUD DE PATENTE DE
INVENCION

TITULO: MECANISMO PARA ASEGURAMIENTO DE TRANSACCIONES
ELECTRONICAS

SOLICITANTE: AZUAN TECHNOLOGIES S.A.

DIRECCION: Carrera 64 No. 96-17 Bogotá, D.C. Colombia

APODERADO: CARLOS R. OLARTE

BOGOTÁ 26 de abril de 2011

609 F110

P2010/000168

FORMULARIO ÚNICO DE SOLICITUD DE PATENTE

P2010/000168

SOLICITUD DE:

1

☒

Patente de Invención.

☐

Patente de Modelo de Utilidad.

2

SOLICITANTE
(71)

Nombre: AZUAN TECHNOLOGIES S.A.

Dirección: Carrera 64 No. 96-17, Bogotá, Colombia

Nacionalidad o Domicilio: COLOMBIANA

Lugar de Constitución: COLOMBIA

Teléfono:

Fax:

E-mail:

IDENTIFICACIÓN

C.C. ☐ NIT ☒

C.E. ☐ Otro ☐

Cual

Número 900088775-2

3

REPRESENTANTE
O APODERADO

Nombre: CARLOS R. OLARTE

Dirección: Diagonal 34 No. 5-28

Teléfono: 601-7700 **Fax:** 601-7799

E-mail: office@olartemoure.com

IDENTIFICACIÓN

C.C. ☒ NIT ☐

C.E. ☐ Otro ☐

Cual

Número 79.782.747 Btá
TP 74.295

4

INVENTOR (ES)
(72)

Nombre: Jaime Enrique Gómez Hernández, Carlos A. Perry Peinado, Wilmer Linares Montañez, Iván Darío Tovar Rueda.

Dirección: Carrera 64 No. 96-17, Bogotá, Colombia

Nacionalidad o Domicilio: Colombiana

5

Título (54) MECANISMO PARA ASEGURAMIENTO DE TRANSACCIONES ELECTRONICAS

6

Clasificación Internacional (51)

G 09 F 1/00

7

Prioridad

SI

☐

NO

☒

(33) País de Origen

(32) Fecha

(31) Número de Solicitud

8

Para publicar a partir de la fecha de la presente solicitud a los:

6 meses

☐

12 meses

☒

18 meses

☐

otro

☐

cual

9

Comprobante de pago No.

Fecha 26 de abril de 2011

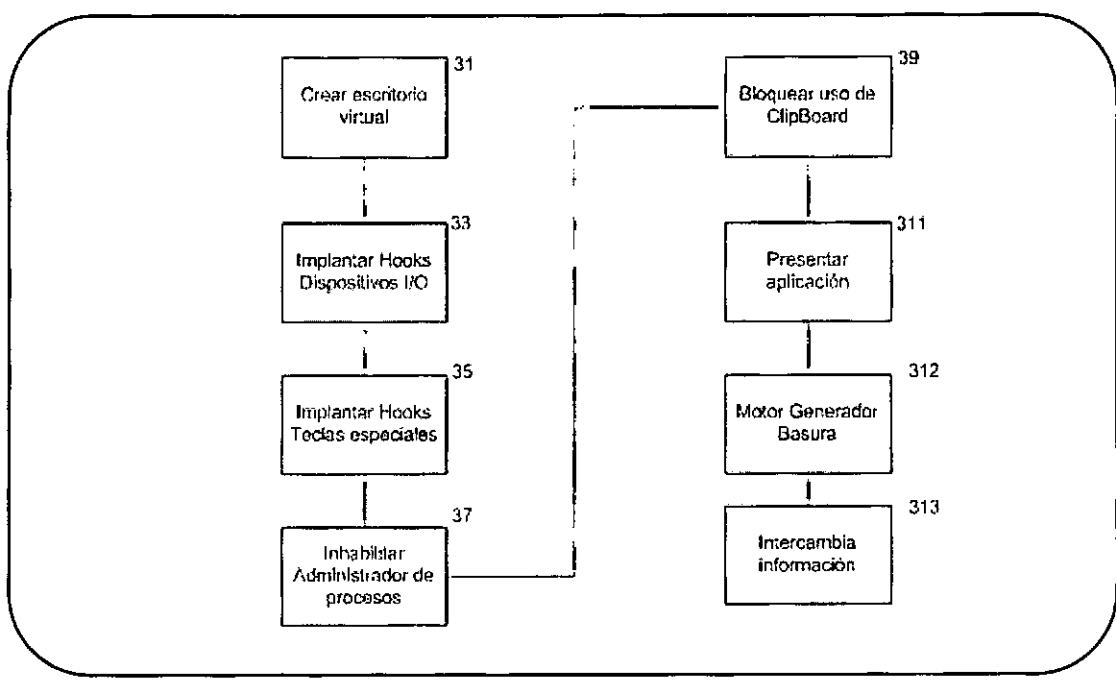
10

ANEXOS

- ☒ Comprobante de pago de la tasa de presentación de la solicitud.
- ☐ Comprobante de pago de la tasa por concepto de excedente de palabras en la publicación.
- ☐ Comprobante de pago por reivindicación de prioridad.
- ☒ Documento que acredita la existencia y representación legal cuando el solicitante sea persona jurídica.
- ☒ Poderes, si fuere el caso.
- ☐ Certificado de la fecha de presentación de la solicitud prioridad expedida por la autoridad correspondiente y una copia certificada de la primera solicitud, si se reivindica prioridad.
- ☐ Traducción simple de la primera solicitud, si se reivindica prioridad.
- ☐ Documento de cesión del inventor al solicitante o a su causante.
- ☐ Resumen.
- ☒ Descripción de la invención.
- ☒ Una o más reivindicaciones.
- ☒ Dibujos y/o planos necesarios.
- ☐ 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.
- ☐ De ser el caso, certificado de depósito del material biológico.
- ☒ Arte final 12 x 12.
- ☐ De ser el caso, información sobre otras solicitudes de patente o títulos obtenidos en el extranjero por el mismo titular o su causante, relacionadas parcial o totalmente con la invención de esta solicitud.

11

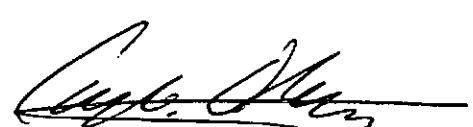
FIGURA CARACTERÍSTICA:



12

Solicito la concesión de la patente,

NOMBRE: CARLOS R. OLARTE

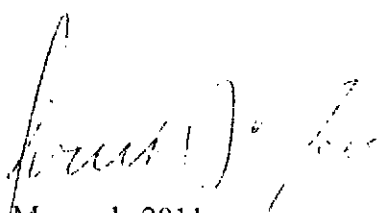
FIRMA: 
C.C. 79.782.747 Btá T.P. 74.295

Power of Attorney

The undersigned, Iván Darío Tovar Rueda

domiciled in Bogotá, D.C., Colombia

by means of these presents hereby grants to **Carlos R. Olarte and/or Juan Guillermo Moure** full and sufficient Power of Attorney to file, prosecute, obtain, defend and enforce any and all of the company's Patents for Inventions, Utility Models, Layout-Designs (topographies) of Integrated Circuits, Industrial Designs, Trademarks, Advertising Slogans, Trade Names, Commercial Emblems, Geographical Indications, Protection of Trade Secrets, Obtainer's Certificates, Copyrights, Registration of Domain Names, Health Registrations, or any other intellectual property right, also to file Unfair competition actions and request injunctions in the Republic of Colombia, to which end it empowers them to take all steps necessary before any administrative or judicial authority of any class for the objects stated, to file petitions, recourses, replies and oppositions, pay taxes and annuities, request testimonies, receive documents and securities, abandon applications, collect refunds, desist, settle, conciliate or negotiate. Sufficient power is hereby granted to receive notifications on behalf of the Company, to confer powers on those who are to represent the company judicially and extra judicially, to answer in court in the matter of all claims and demands that may be presented in connection with the objects stated, giving them likewise power to substitute these presents and revoke such substitutions.

Signature/Firma: 

Date/Fecha: 13 de Marzo de 2011

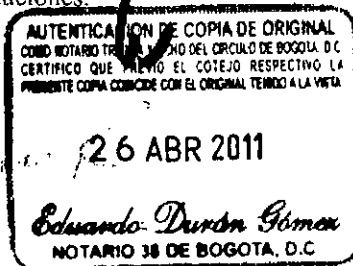
City/Country/Ciudad,País: Bogotá, D.C., Colombia

Poder

El suscrito, Iván Darío Tovar Rueda

domiciliado en Bogotá, D.C., Colombia

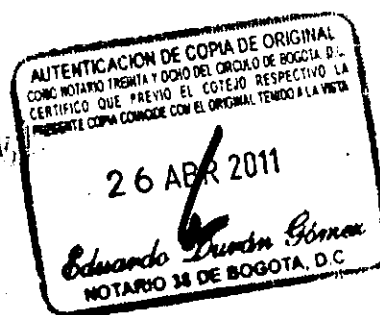
por medio del presente otorga a **Carlos R. Olarte y/o Juan Guillermo Moure** poder amplio y suficiente para presentar, tramitar, obtener, defender y hacer respetar todas y cualquiera de las Patentes de Invención, Modelos de Utilidad, Esquemas de Trazados de Circuitos Integrados, Diseños Industriales, Marcas, Lemas Comerciales, Nombres Comerciales, Enseñas Comerciales, Denominaciones de Origen, Protección de Secretos Empresariales, Certificados de Obtentor, Derechos de Autor, Registro de Nombres de Dominio, Registros Sanitarios, o cualquier otro bien de propiedad intelectual y también para presentar acciones de competencia desleal y pedir medidas cautelares a nombre de la Universidad en la República de Colombia, a cuyo efecto los faculta para dar todos los pasos necesarios ante cualquier autoridad administrativa o judicial de cualquier jerarquía para cumplir con lo encomendado, elevar solicitudes, recursos, respuestas y oposiciones, pagar impuestos y anualidades, solicitar testimonios, recibir documentos y valores, desistir, transigir, y percibir. Se concede poder bastante para recibir notificaciones a nombre de la compañía, otorgar poderes a quienes vayan a representar a la compañía judicial y extrajudicialmente, responder en juicio a todas las reclamaciones o demandas que por motivo de lo encomendado se presentaren, dándoles asimismo facultad para sustituir el presente y revocar dichas sustituciones.

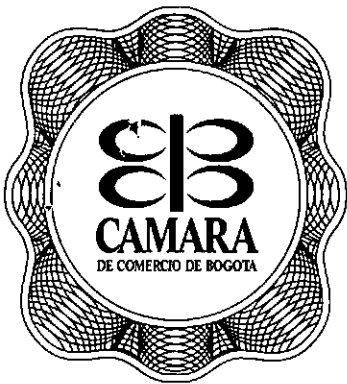


Ben Domo Goya
Ronda

79731405

[Handwritten signature]
[Large handwritten 'M']





01



* 1 0 3 4 3 9 8 4 4 *

9

CAMARA DE COMERCIO DE BOGOTA

SEDE CHAPINERO

26 DE ABRIL DE 2011 HORA 11:41:32

R031285419

PAGINA: 1 de 2

* * * * *

CERTIFICADO DE EXISTENCIA Y REPRESENTACION LEGAL O INSCRIPCION DE DOCUMENTOS

LA CAMARA DE COMERCIO DE BOGOTA, CON FUNDAMENTO EN LAS MATRICULAS E INSCRIPCIONES DEL REGISTRO MERCANTIL

CERTIFICA:

NOMBRE : AZUAN TECHNOLOGIES S A

N.I.T. : 900088775-2 ADMINISTRACION : DIRECCION SECCIONAL DE IMPUESTOS DE BOGOTA, REGIMEN COMUN

DOMICILIO : BOGOTA D.C.

CERTIFICA:

MATRICULA NO: 01605218 DEL 7 DE JUNIO DE 2006

CERTIFICA:

DIRECCION DE NOTIFICACION JUDICIAL : CRA 64 NO. 96-17

MUNICIPIO : BOGOTA D.C.

EMAIL DE NOTIFICACION JUDICIAL : azuan@azuan.com

DIRECCION COMERCIAL : CRA 64 NO. 96-17

MUNICIPIO : BOGOTA D.C.

EMAIL COMERCIAL : azuan@azuan.com

CERTIFICA:

CONSTITUCION: QUE POR ESCRITURA PUBLICA NO. 0000911 DE NOTARIA 45 DE BOGOTA D.C. DEL 18 DE FEBRERO DE 2006, INSCRITA EL 7 DE JUNIO DE 2006 BAJO EL NUMERO 01059890 DEL LIBRO IX, SE CONSTITUYO LA SOCIEDAD COMERCIAL DENOMINADA AZUAN TECHNOLOGIES S A.

CERTIFICA:

VIGENCIA: QUE LA SOCIEDAD NO SE HALLA DISUELTA. DURACION HASTA EL 18 DE FEBRERO DE 2026 .

CERTIFICA:

OBJETO SOCIAL : LA SOCIEDAD TENDRA COMO OBJETO PRINCIPAL LAS SIGUIENTES ACTIVIDADES: A) EL DISEÑO, FABRICACION, IMPLEMENTACION, ADQUISICION, ENAJENACION, REPARACION, TRANSFORMACION, COMERCIALIZACION, EXPORTACION, IMPORTACION, DISTRIBUCION, PROMOCION, FINANCIACION Y ADMINISTRACION DE: SISTEMAS OPERATIVOS, PROGRAMAS DE COMPUTACION Y PAQUETES COMPUTACIONALES DE USO GENERAL O ESPECIFICO, PARA LA PUBLICACION, ADQUISICION, TRANSMISION, ALMACENAMIENTO Y COMUNICACION DE TODO TIPO DE INFORMACION, DIRECTAMENTE O MEDIANTE CONTRATOS O SUBCONTRATOS RELACIONADOS CON TERCEROS POR CUENTA PROPIA O AJENA Y CON RECURSOS PROPIOS O FINANCIACIONES EXTERNAS. B) EL DISEÑO, FABRICACION, ADQUISICION, ENAJENACION, REPARACION, ENSAMBLAJE, REPOSICION, TRANSFORMACION, COMERCIALIZACION, EXPORTACION, IMPORTACION, DISTRIBUCION, PROMOCION Y FINANCIAMIENTO DE: REPUESTOS, PARTES, ACCESORIOS Y EQUIPOS DE COMPUTACION Y TRANSMISION DE DATOS, ALMACENAMIENTO Y GRABACION DE INFORMACION, TELECOMUNICACIONES, REDES, TELEMATICA, EQUIPOS DE OFICINA, ETC ., DIRECTAMENTE O MEDIANTE CONTRATOS O SUBCONTRATOS RELACIONADOS CON

TERCEROS POR CUENTA PROPIA O AJENA Y CON RECURSOS PROPIOS O FINANCIACIONES EXTERNAS. C) EL DISEÑO, FABRICACION, ADQUISICION, ENAJENACION, TRANSFORMACION, COMERCIALIZACION, EXPORTACION, IMPORTACION, DISTRIBUCION, PROMOCION Y FINANCIAMIENTO DE MATERIALES DEDICADOS A ESTA CLASE DE OPERACIONES TALES COMO LIBROS, MANUALES, ARTICULOS MISCELANEOS, ETC. D) EL DISEÑO, FABRICACION, ADQUISICION, ENAJENACION, TRANSFORMACION, COMERCIALIZACION, EXPORTACION, IMPORTACION, DISTRIBUCION Y PROMOCION DE MARCAS, DIBUJOS, INSIGNIAS Y DEMAS MATERIAL GRAFICO O PUBLICITARIO. E) BRINDAR ASESORIAS EN LA IMPLEMENTACION DE SISTEMAS DE INFORMACION PARA EMPRESAS DE ORIGEN PUBLICO O PRIVADO F) ADQUISICION DE ACCIONES, PARTES O CUOTAS DE INTERES Y EN GENERAL PARTICIPAR EN CUALQUIER FORMA DE SOCIEDAD O CONTRATO QUE TENGA COMO OBJETO LA EXPLOTACION O DESARROLLO DE LA INFORMATICA, O LA PRODUCCION O NEGOCIACION DE ELEMENTOS DE LA INDUSTRIA INFORMATICA. G) LA CONSTITUCION DE LA EMPRESA O SOCIEDADES QUE PERSIGAN FINES ANALOGOS O COMPLEMENTARIOS A LOS DE ESTA SOCIEDAD. EN DESARROLLO DEL MISMO PODRA LA SOCIEDAD EJECUTAR TODOS LOS ACTOS O CONTRATOS QUE FUEREN CONVENIENTES O NECESARIOS PARA EL CABAL CUMPLIMIENTO DE SU OBJETO SOCIAL Y QUE TENGAN RELACION DIRECTA CON EL OBJETO MENCIONADO, TALES COMO: FORMAR PARTE DE OTROS SOCIEDADES ANONIMAS O DE RESPONSABILIDAD LIMITADA.

CERTIFICA:

CAPITAL:

** CAPITAL AUTORIZADO **

VALOR : \$50,000,000.00
NO. DE ACCIONES : 5,000.00
VALOR NOMINAL : \$10,000.00

** CAPITAL SUSCRITO **

VALOR : \$35,000,000.00
NO. DE ACCIONES : 3,500.00
VALOR NOMINAL : \$10,000.00

** CAPITAL PAGADO **

VALOR : \$35,000,000.00
NO. DE ACCIONES : 3,500.00
VALOR NOMINAL : \$10,000.00

CERTIFICA:

** JUNTA DIRECTIVA: PRINCIPAL (ES) **

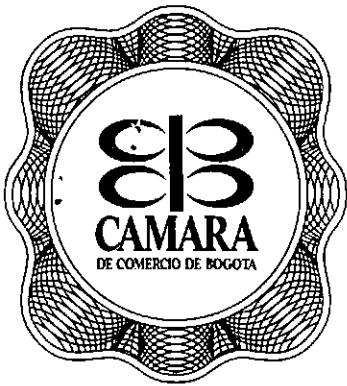
QUE POR ESCRITURA PUBLICA NO. 0000911 DE NOTARIA 45 DE BOGOTA D.C. DEL 18 DE FEBRERO DE 2006, INSCRITA EL 7 DE JUNIO DE 2006 BAJO EL NUMERO 01059890 DEL LIBRO IX, FUE (RON) NOMBRADO (S):

NOMBRE	IDENTIFICACION
PRIMER RENGLON	
GOMEZ HERNANDEZ JAIME ENRIQUE	C.C. 000000079436464
SEGUNDO RENGLON	
PERRY PEINADO CARLOS ALFONSO	C.C. 000000080844839
TERCER RENGLON	
TOVAR IVAN	C.C. 000000079781465

** JUNTA DIRECTIVA: SUPLENTE (S) **

QUE POR ESCRITURA PUBLICA NO. 0000911 DE NOTARIA 45 DE BOGOTA D.C. DEL 18 DE FEBRERO DE 2006, INSCRITA EL 7 DE JUNIO DE 2006 BAJO EL NUMERO 01059890 DEL LIBRO IX, FUE (RON) NOMBRADO (S):

NOMBRE	IDENTIFICACION
PRIMER RENGLON	



01



* 1 0 3 4 3 9 8 4 5 *

5

CAMARA DE COMERCIO DE BOGOTA

SEDE CHAPINERO

26 DE ABRIL DE 2011

HORA 11:41:32

R031285419

PAGINA: 2 de 2

* * * * *

DUARTE RESTREPO GERMAN ALBERTO
SEGUNDO RENGLON

C.C. 000000079492065

LINARES MONTAÑEZ WILMER

C.C. 000000079753799

TERCER RENGLON

MADIEDO MONTOYA DIEGO FERNANDO

C.C. 000000079795157

CERTIFICA:

REPRESENTACION LEGAL : LA SOCIEDAD, TENDRA UN GERENTE, UN SUPLENTE QUE REEMPLAZARA AL PRINCIPAL, EN SUS FALTAS ACCIDENTALES, TEMPORALES O ABSOLUTAS.

CERTIFICA:

** NOMBRAMIENTOS **

QUE POR ESCRITURA PUBLICA NO. 0000911 DE NOTARIA 45 DE BOGOTA D.C. DEL 18 DE FEBRERO DE 2006, INSCRITA EL 7 DE JUNIO DE 2006 BAJO EL NUMERO 01059890 DEL LIBRO IX, FUE (RON) NOMBRADO (S):

NOMBRE

IDENTIFICACION

GERENTE

TOVAR IVAN

C.C. 000000079781465

CERTIFICA:

FACULTADES DEL REPRESENTANTE LEGAL : EL GERENTE EJERCERA TODAS LAS FUNCIONES PROPIAS DE LA NATURALEZA DE SU CARGO, Y EN ESPECIAL, LAS SIGUIENTES: 1. REPRESENTAR A LA SOCIEDAD ANTE LOS ACCIONISTAS, ANTE TERCEROS Y ANTE TODA CLASE DE AUTORIDADES DEL ORDEN ADMINISTRATIVO Y JURISDICCIONAL. 2. EJECUTAR TODOS LOS ACTOS U OPERACIONES CORRESPONDIENTES AL OBJETO SOCIAL, DE CONFORMIDAD CON LO PREVISTO EN LAS LEYES Y EN ESTOS ESTATUTOS. 3. AUTORIZAR CON SU FIRMA TODOS LOS DOCUMENTOS PUBLICOS O PRIVADOS QUE DEBAN OTORGARSE EN DESARROLLO DE LAS ACTIVIDADES SOCIALES O EN INTERES DE LA SOCIEDAD. 4. PRESENTAR A LA ASAMBLEA GENERAL EN SUS REUNIONES ORDINARIAS, UN INVENTARIO Y UN BALANCE DE FIN DE EJERCICIO, JUNTO CON UN INFORME ESCRITO SOBRE LA SITUACION DE LA SOCIEDAD, UN DETALLE COMPLETO DE LA CUENTA DE PERDIDAS Y GANANCIAS Y UN PROYECTO DE DISTRIBUCION DE UTILIDADES OBTENIDAS. 5. NOMBRAR Y REMOVER LOS EMPLEADOS DE LA SOCIEDAD CUYO NOMBRAMIENTO Y REMOCION LE DELEGUE LA JUNTA DIRECTIVA. 6. TOMAR TODAS LAS MEDIDAS QUE RECLAME LA CONSERVACION DE LOS BIENES SOCIALES, VIGILAR LA ACTIVIDAD DE LOS EMPLEADOS DE LA ADMINISTRACION DE LA SOCIEDAD E IMPARTIRLES LAS ORDENES E INSTRUCCIONES QUE EXIJA LA BUENA MARCHA DE LA COMPAÑIA. 7. CONVOCA LA ASAMBLEA GENERAL A REUNIONES EXTRAORDINARIAS CUANDO LO JUZGUE CONVENIENTE O NECESARIO Y HACER LAS CONVOCATORIAS DEL CASO CUANDO LO ORDENEN LOS ESTATUTOS, LA JUNTA DIRECTIVA O EL REVISOR FISCAL DE LA SOCIEDAD. 8. CONVOCAR LA JUNTA DIRECTIVA CUANDO LO CONSIDERE NECESARIO O CONVENIENTE Y MANTENERLA INFORMADA DEL CURSO DE LOS NEGOCIOS SOCIALES. 9. CUMPLIR LAS ORDENES E INSTRUCCIONES QUE LE IMPARTAN LA ASAMBLEA GENERAL O LA JUNTA

DIRECTIVA, Y, EN PARTICULAR, SOLICITAR AUTORIZACIONES PARA LOS NEGOCIOS QUE DEBEN APROBAR PREVIAMENTE LA ASAMBLEA O LA JUNTA DIRECTIVA SEGUN LO DISPONEN LAS NORMAS CORRESPONDIENTES DEL PRESENTE ESTATUTO. 10. CUMPLIR O HACER QUE SE CUMPLAN OPORTUNAMENTE TODOS LOS REQUISITOS O EXIGENCIAS LEGALES QUE SE RELACIONEN CON EL FUNCIONAMIENTO Y ACTIVIDADES DE LA SOCIEDAD.

CERTIFICA:

** REVISOR FISCAL **

QUE POR ESCRITURA PUBLICA NO. 0000911 DE NOTARIA 45 DE BOGOTA D.C. DEL 18 DE FEBRERO DE 2006, INSCRITA EL 7 DE JUNIO DE 2006 BAJO EL NUMERO 01059890 DEL LIBRO IX, FUE (RON) NOMBRADO (S):

NOMBRE
REVISOR FISCAL

IDENTIFICACION

PULGARIN CRUZ DELIA MENDOZA DE

C.C. 000000051569562

CERTIFICA:

DE CONFORMIDAD CON LO ESTABLECIDO POR LA LEY 962 DE 2005, LOS ACTOS DE REGISTRO AQUI CERTIFICADOS QUEDAN EN FIRME CINCO (5) DIAS HABILES DESPUES DE LA FECHA DE INSCRIPCION, SIEMPRE QUE NO SEAN OBJETO DE RECURSOS EN LA VIA GUBERNATIVA.

* * * EL PRESENTE CERTIFICADO NO CONSTITUYE PERMISO DE
* * * FUNCIONAMIENTO EN NINGUN CASO

* * *

* * *

INFORMACION COMPLEMENTARIA

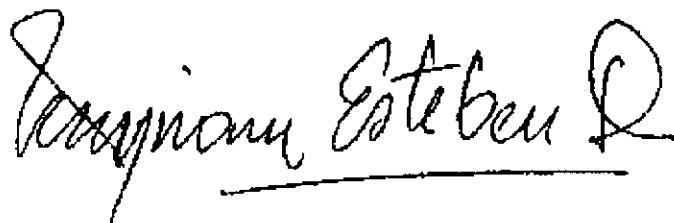
LOS SIGUIENTES DATOS SOBRE RIT Y PLANEACION DISTRITAL SON INFORMATIVOS
CONTRIBUYENTE INSCRITO EN EL REGISTRO RIT DE LA DIRECCION DISTRITAL DE IMPUESTOS, FECHA DE INSCRIPCION : 18 DE FEBRERO DE 2006
FECHA DE ENVIO DE INFORMACION A PLANEACION DISTRITAL : 9 DE JUNIO DE 2006

SEÑOR EMPRESARIO, SI SU EMPRESA TIENE ACTIVOS INFERIORES A 30.000 SMLMV Y UNA PLANTA DE PERSONAL DE MENOS DE 200 TRABAJADORES, USTED TIENE DERECHO A RECIBIR UN DESCUENTO EN EL PAGO DE LOS PARAFISCALES DE 75% EN EL PRIMER AÑO DE CONSTITUCION DE SU EMPRESA, DE 50% EN EL SEGUNDO AÑO Y DE 25% EN EL TERCER AÑO. LEY 590 DE 2000 Y DECRETO 525 DE 2009.

RECUERDE INGRESAR A www.supersociedades.gov.co PARA VERIFICAR SI SU EMPRESA ESTA OBLIGADA A REMITIR ESTADOS FINANCIEROS. EVITE SANCIONES.

EL SECRETARIO DE LA CAMARA DE COMERCIO,
VALOR : \$ 3,700

DE CONFORMIDAD CON EL DECRETO 2150 DE 1995 Y LA AUTORIZACION IMPARTIDA POR LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO, MEDIANTE EL OFICIO DEL 18 DE NOVIEMBRE DE 1996, LA FIRMA MECANICA QUE APARECE A CONTINUACION TIENE PLENA VALIDEZ PARA TODOS LOS EFECTOS LEGALES



ASSIGNMENT

6
REPUBLICA DE COLOMBIA
CESIÓN
NACIONAL DE LA CRUZ

Jaime Enrique Gómez Hernández

Carlos Alfonso Perry Peinado

Wilmer Linares Montañez

Iván Darío Tovar Rueda

by means of this document assign(s) worldwide,
to

por medio de la presente cedo(cedemos) a nivel
mundial, a

AZUAN TECHNOLOGIES S.A.,

a (type of company),
organized under the laws of

una Sociedad Anónima
organizada bajo las leyes de

REPUBLIC OF COLOMBIA,

Domiciled in

domiciliada en

Bogotá, D.C. CR 64 96 17

(hereinafter referred to as the "ASSIGNEE"),
all my (our) rights, including those of priority,
title and interest in and to my (our) invention for
a new and useful improvement entitled and as
fully set forth and described in:

(de ahora en adelante el "CESIONARIO").
todos mis (nuestros) derechos, incluyendo los de
prioridad, título e interés sobre mi (nuestra)
invención tal como describe en:

Mecanismo para Aseguramiento de Transacciones Electrónicas

Bogotá, D.C., Colombia, April 14th, 2011

Jaime Enrique Gómez Hernández

cc 79.436.464

Wilmer Linares Montañez

cc 79.753.799

Bogotá, D.C., Colombia, Abril 14 de 2011

Carlos Perry Peinado

cc 80.844.839

Iván Darío Tovar Rueda

cc 79.781.465

REPÚBLICA DE COLOMBIA
RAMÓN ALBERTO LOZADA DE LA CRUZ
NOTARIA 75 - BOGOTÁ D.C.

14 ABR. 2011

Presentación Personal

Reconocimiento Firma-Huella NO Certificada

Doy fe que este documento fue presentado personalmente por quien se identificó con

Jaime Enrique Gomez
Hernandez con 99436464

y declaró, que reconoce la firma como

[Firma]
Autorizo Reconocimiento

REPÚBLICA DE COLOMBIA
RAMÓN ALBERTO LOZADA DE LA CRUZ
NOTARIA 75 - BOGOTÁ D.C.

Remando
V.A. SANCHEZ M

REPÚBLICA DE COLOMBIA
RAMÓN ALBERTO LOZADA DE LA CRUZ
NOTARIA 75 - BOGOTÁ D.C.

14 ABR. 2011

Presentación Personal

Reconocimiento Firma-Huella NO Certificada

Doy fe que este documento fue presentado personalmente por quien se identificó con

Carlos Alberto Perez
Pineda con 8084483981

y declaró, que reconoce la firma como

[Firma]
Autorizo Reconocimiento

REPÚBLICA DE COLOMBIA
RAMÓN ALBERTO LOZADA DE LA CRUZ
NOTARIA 75 - BOGOTÁ D.C.

Remando
V.A. SANCHEZ

REPÚBLICA DE COLOMBIA
RAMÓN ALBERTO LOZADA DE LA CRUZ
NOTARIA 75 - BOGOTÁ D.C.

14 ABR. 2011

Presentación Personal

Reconocimiento Firma-Huella NO Certificada

Doy fe que este documento fue presentado personalmente por quien se identificó con

Alvan Dario Tovar Rueda
[Firma] con 99781465

y declaró, que reconoce la firma como

[Firma]
Autorizo Reconocimiento

REPÚBLICA DE COLOMBIA
RAMÓN ALBERTO LOZADA DE LA CRUZ
NOTARIA 75 - BOGOTÁ D.C.

V.A. SANCHEZ
Remando

REPÚBLICA DE COLOMBIA
RAMÓN ALBERTO LOZADA DE LA CRUZ
NOTARIA 75 - BOGOTÁ D.C.

14 ABR. 2011

Presentación Personal

Reconocimiento Firma-Huella NO Certificada

Doy fe que este documento fue presentado personalmente por quien se identificó con

Wilmer Lincres Hernandez
[Firma] con 9975379981

y declaró, que reconoce la firma como

[Firma]
Autorizo Reconocimiento

REPÚBLICA DE COLOMBIA
RAMÓN ALBERTO LOZADA DE LA CRUZ
NOTARIA 75 - BOGOTÁ D.C.

V.A. SANCHEZ
Remando

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800.176.089-2

- / -

Industria y Comercio
SUPERINTENDENCIA

RECIBO DE CAJA

No. 11 - 0038915

Bogotá D.C., Abril 26 de 2011 - 16:24:40

RECIBIDO DE : AZUAN TECHNOLOGIES S.A

NI 900.088.775

*** Soporte del Pago ***

TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	VR PAGO
CONSIGNACION	BANCO DE BOGOTA	062754387	36333555	15/04/2011	571.000.00

*** Conceptos Pagados ***

CANT.	RENTISTICO	CONCEPTO	VR. UNDITARIO	VR. CONCEPTO
1	50005-01-01 SOLICITUDES	1 TRAMITES DE SOL. DE PATENTE DE INVENCIÓN	571.000.00	571.000.00
				\$571.000.00

SON: **QUINIENTOS SETENTA Y UN MIL PESOS MONEDA CORRIENTE**

Responsable: _____

Recibo de Caja Aplicado al Expediente No. _____

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 11-050985- -00000-0000

Fecha: 2011-04-26 16:44:30 Dep. 2020 DIR.NUEVASCR
Tra. 2 PATENTES Eve: 1 REGDEPOSITO
Act. 411 PRESENTACION Folios: 41

Sede Centro: Carrera 13 No. 27 - 00 Pisos 3,4,5 y 10 Bogotá, D.C.- Colombia

Web: www.sic.gov.co e-mail: info@sic.gov.co Conmutador: (571) 5870000 Fax: (571) 5870284 Línea: 018000-910165 Call Center: (571) 6513240

Abril 26 de 2011 - 16:24:40

MECANISMO PARA ASEGURAMIENTO DE TRANSACCIONES ELECTRONICAS

1. Campo de la invención

La invención se relaciona generalmente con computadores y aplicaciones de procesamiento de datos y, más particularmente, al sistema y la metodología de proporcionar un entorno de trabajo seguro para los usuarios finales de aplicaciones transaccionales.

2. Antecedentes.

El uso de servicios virtualizados como las compras por Internet, así como la realización de transacciones electrónicas por este canal, ha hecho que los delincuentes cibernéticos se especialicen en el desarrollo de malware que ataca de forma selectiva a los usuarios de los servicios previamente mencionados.

La proliferación de virus, gusanos, troyanos y todo tipo de malware especializado en el robo de información de los usuarios finales de servicios electrónicos, ha hecho que muchas de las compañías recomienden el acceder a estos servicios desde puntos, redes y equipos plenamente identificados para así disminuir los riesgos el máximo posible. Desafortunadamente estas medidas no son muy útiles, pues los usuarios siguen utilizando sus equipos sin administración ni control por parte de las compañías que ofrecen servicios electrónicos. Esto significa que al momento de ingresar a los servicios, el equipo puede estar en riesgo de infección, o ya se encuentra inmerso con algún tipo de espía que está robando toda la información del usuario.

Los usuarios finales de servicios electrónicos, en la mayoría de los casos, no son conscientes de los riesgos existentes al momento de realizar sus transacciones; sobre todo en Internet (esto no quiere decir que en ambientes aislados no exista riesgo). Es por esto que los usuarios al ver la facilidad del uso de redes compartidas (WLAN en aeropuertos por ejemplo), hacen transacciones donde se intercambia información sensible abiertamente

en este tipo de ambientes. Es aquí donde los equipos informáticos de estos usuarios son más vulnerables, al no conocer los riesgos que representa el solo hecho de hacer uso de esas redes, que por lo general dan acceso ilimitado a sus equipos, de tal forma que estos pueden ser infectados con cualquier tipo de software espía, que espera el momento justo para ejecutar sus comandos de robo y enviar la información sensible a un tercero.

Así como el uso de redes no seguras para intercambios sensibles de información sobre la red, se ve el uso de equipos informáticos desconocidos (cafés internet por ejemplo), donde pueden haber sido manipulados por más de un usuario durante su vida útil, aumentando el riesgo de infección, y haciendo más probable que estos se encuentren infectados con algún tipo de malware.

Otro punto interesante y que viene en alza es el uso de técnicas de ingeniería social. Aunque este problema se escapa del ámbito tecnológico, es mucho más preocupante que cualquier otro, es por este medio por donde más se pierde información que posteriormente se usa para realizar delitos en nombre de terceros.

Las compañías que prestan servicios informáticos se han concentrado en el aseguramiento de su inversión, es decir, de sus equipos. Cuando comienzan los ataques informáticos estos se centran en dañar los servidores de las compañías para que no puedan prestar servicios, sacarlos del aire y en el peor de los casos suplantarlos y así robar información.

Las compañías utilizan políticas donde restringen a los usuarios a escenarios de acceso conocidos, limitando a estos la conveniencia que les representa hacer uso de los servicios en cualquier parte y sobre cualquier red, desnaturalizando así el propósito mismo de la tecnología móvil.

Las compañías con sus políticas de educación están dejando la responsabilidad de la seguridad del punto de acceso (equipo informático del usuario, red usada, etc) en el usuario final. Acciones como el uso de antivirus y mantenimiento de estos (tener las listas

actualizadas, uso de software licenciado y demás restricciones) son aconsejadas pero no controladas por parte de las compañías. Por esta razón los usuarios siguen teniendo problemas de fraude, pues la gran mayoría no poseen el conocimiento suficiente para hacer uso de las mejores prácticas recomendadas por las compañías prestadoras de servicios electrónicos.

La industria tecnológica ha contribuido de forma positiva para que la sensación de seguridad crezca en los usuarios. Uno de los métodos de aseguramiento más aceptados es el uso de los *tokens* o generadores de contraseñas de único uso (OTP, por sus siglas en inglés). Esta es una herramienta que pretende mejorar los niveles de seguridad para los usuarios al momento de autenticarse e intercambiar información con aplicaciones informáticas.

Estos *tokens* son una gran herramienta pero presentan una serie de inconvenientes que en su mayor parte se encuentran en la logística de su administración, es decir, estos aparatos generan un costo a las compañías que en la mayoría de los casos son transmitidos a los usuarios finales, quienes a su vez no están dispuestos a incurrir en estos nuevos costos.

Adicionalmente durante los últimos dos años se ha venido desarrollando una serie de malware especializado en estos dispositivos (mas exactamente en el robo de la contraseña que generan) haciendo que esta tecnología ya no sea un mecanismo que marque la diferencia en la seguridad para el usuario final; esta contraseña ya es reproducible sin que los usuarios se den cuenta de ello. A manera de ejemplo, existe un malware llamado *Zeus*, que posee una gran familia de ejecutables especializados en el robo de estas contraseñas, por lo cual ha tenido gran éxito en el campo de robo de información.

Otro de los métodos de aseguramiento que es ampliamente utilizado por los usuarios finales de una transacción computacional, es el de antivirus, cuyo problema más grave radica en su incapacidad para proteger contra virus desconocidos. Esto permite que los nuevos virus tengan una ventana de exposición, i.e. un delta de tiempo para una rápida

M

propagación, antes que el software antivirus pueda ser adaptado y actualizado para probar su existencia y detenerlo. Con base en los temas descritos en este documento se encuentra que en el mercado existen productos que pretenden brindar soluciones de seguridad para el aseguramiento de información en el punto final, es decir, el equipo del usuario de las aplicaciones transaccionales. Entre estos productos están las suites de antimalware; los antivirus como por ejemplo Norton Antivirus™ de Symantec, Panda Antivirus™ de Panda Software, Kaspersky Anti-Virus™ de Kaspersky, Avira Antivirus™ de Avira, Avast™, entre otros. En la modalidad de antispyware, software que lucha contra el software espía, Ad-Aware SE Personal™, Spybot - Search & Destroy™, y SpywareBlaster entre otros.

Adicionalmente existen programas de software que permiten el aseguramiento de la información cuando se está utilizando navegadores de internet como por ejemplo ZoneAlarm™ de Checkpoint, que además de integrar antivirus y antispyware, poseen un esquema de aseguramiento para el navegador, el cual no deja ejecutar el software del tipo denominado loggers mientras se está usando el navegador. Sin embargo, como se ha mencionado anteriormente estos programas están dirigidos para aquellos usuarios que desean asegurar su información y no son provistos por las compañías que publican sus servicios en la red, lo cual deja sin protección, así sea parcial, a millones de usuarios que no poseen los medios económicos, tecnológicos o de conocimiento para implementar alguna de estas soluciones, además de aclarar que estas soluciones en su mayoría son parcialmente efectivas.

Otros mecanismos, como el mencionado en el documento US 7725737B2 de propiedad de Check Point Software Technologies, Inc., describe el procedimiento para el aseguramiento del punto final de una transacción. El método consiste en la creación de un marco de trabajo seguro para los usuarios finales, el cual se basa en una serie de políticas configurables por el mismo usuario. La implementación de *hooks* administra ciertas comunicaciones entre las aplicaciones y el sistema operativo. La información que se genera dentro del marco seguro es cifrada para que solo desde allí pueda ser vista. Este

documento describe un método de aseguramiento dirigido a toda la diversidad de dispositivos electrónicos existentes, pero referencia directamente la forma de construir aplicaciones seguras solo en computadores con sistemas operativos Windows™. Este método presenta la posibilidad de configurar los niveles de seguridad, permitiendo que las transacciones bajo esta configuración sean infectadas por malware y así hacer inseguro el sistema donde se ejecuta el método. El uso del método en el equipo donde se harán las transacciones requiere la instalación con permisos de administrador; si el usuario habitual del equipo no posee estos privilegios, el uso del método no puede llevarse a cabo. Todo lo que se ejecute sobre el ambiente seguro que describe el método es cifrado y almacenado, acción que permitiría a los atacantes reconstruir información presente en el disco, además de afectar de manera considerable el desempeño de la maquina, afectando la experiencia del usuario final. Adicionalmente, este método necesita de un componente externo con el que se hace la validación de las políticas mínimas requeridas para la ejecución del marco de trabajo seguro, limitando la posibilidad de implementación de la solución solo para sectores corporativos, donde los puntos finales de conexión poseen un nivel de control desde la compañía que presta el servicio de la aplicación transaccional. Por el contrario, el método de la presente invención no da la facultad al usuario para que elija sus niveles de seguridad cerrando cualquier posibilidad de ataques para el usuario final. Cuando los usuarios poseen la facultad de manipular los niveles de seguridad en una aplicación, generalmente estos niveles no son los óptimos para las necesidades del usuario final, pues el usuario no posee conocimientos técnicos para la configuración apropiada de la seguridad en su máquina. Al no permitir que el usuario pueda configurar la seguridad, permite que la compañía que implementa el método propuesto en esta invención, tenga un margen de riesgo menor al que presentan otros métodos donde los usuarios configuran su seguridad.

Dentro de los métodos ampliamente divulgados para el aseguramiento del punto final de una transacción se encuentra la virtualización de servicios y de sistemas operativos completos donde el malware que reside en el escenario normal del usuario no ataca el ambiente virtualizado. Dos ejemplos de este método se divulgan en los documentos US

2004/0236874A1 y US 2010/0005531A1, donde se describe cómo se hace la virtualización completa de un sistema operativo alternativo al original del usuario, el cual es capaz de convivir y ejecutarse al mismo tiempo con el sistema operativo original del usuario final. Estos métodos que son bien reconocidos en la industria por su eficacia al momento de

5 proteger a los usuarios, no son métodos que se puedan entregar o implementar sobre cualquier ambiente. Los equipos de los usuarios deben cumplir con unas características técnicas en su hardware para suplir los requerimientos mínimos que estos métodos necesitan. Adicionalmente se necesita por parte del usuario un conocimiento medianamente alto para hacer la configuración de los métodos de virtualización, pues

10 virtualizar un sistema operativo es mucho más complejo que virtualizar un servicio. La virtualización de un sistema operativo también requiere de una serie de recursos físicos como, almacenamiento en disco duros, una porción importante de la memoria RAM para su ejecución, así como interfaces (drivers o controladores) que le permitan el uso de los distintos dispositivos periféricos como teclado, cursor o hasta impresoras, estos recursos

15 por lo general son limitados para los usuarios finales, pues no poseen máquinas con una capacidad computacional tan alta.

3. Descripción de las Figuras

La Figura 1 es un diagrama de bloques de los tres principales componentes para

20 aplicaciones transaccionales.

La Figura 2 es un esquema de uso de cualquier aplicación mostrando en qué punto se genera el ambiente aislado.

La Figura 3 muestra los pasos para la generación de un ambiente aislado para el intercambio de información.

25 La Figura 4 muestra el proceso para la implantación de *hooks* para la interceptación de mensajes en el sistema operativo, parte del proceso de aislamiento.

La Figura 5 muestra el orden en que se deben implantar los *hooks* de bloqueo de teclas en el sistema.

La Figura 6 es un diagrama de componentes que expone los principales eventos que ejecuta el motor de generación de basura.

La Figura 7 es un diagrama de flujo del proceso para liberar el equipo del usuario cuando el esquema aislado termina de ejecutarse.

5

4. Breve descripción del invento

La presente invención divulga un método de seguridad informática que permite a todos los usuarios de una aplicación informática poseer niveles superiores de seguridad al momento de intercambiar información sensible con aplicaciones transaccionales. Cualquier usuario
10 (sin necesidad de conocimientos avanzados en tecnologías) desde cualquier lugar, usando cualquier tipo de red puede realizar transacciones electrónicas con un muy bajo riesgo de que su información sea robada o comprometida.

El método de la presente invención consiste en el desarrollo de un escritorio virtual que
15 aísla el ambiente en el cual trabaja el usuario, en donde dicho escritorio virtual es programado de tal manera que se implantan técnicas de *hooking* para interceptar mensajes entre la aplicación transaccional y el sistema operativo del usuario. Adicionalmente el método bloquea las combinaciones de teclas especiales para prevenir la ejecución de código malicioso. Al momento de lanzar escritorio virtual, las aplicaciones que se ejecuten
20 durante la sesión serán ejecutadas dentro de un ambiente aislado y seguro. Durante el uso de la aplicación, el siguiente paso es la generación de eventos basura en el sistema operativo del usuario. Cuando el usuario determine la terminación de la sesión segura, se retorna al escritorio original y el usuario puede seguir usando el equipo de forma normal.

25 El uso de varias técnicas conocidas para el aseguramiento determinan el éxito de este método de aseguramiento. Técnicas como la creación de escritorios virtuales y la implantación de *hooks* son usadas por otros métodos de aseguramiento pero por lo general de forma separada lo que los hace vulnerables a los ataques informáticos. Así mismo, ninguna de las características descritas por este método son removibles, ajustables o

configurables por el usuario, lo que garantiza que la compañía que presta los servicios transaccionales no corre riesgo que su política de aseguramiento sea reducida por acciones de usuario o malware presente en el equipo donde se pretende hacer la transacción.

- 5 A diferencia del arte previo, el invento descrito en este documento no necesita de características especiales en hardware o software para su ejecución. De la misma forma, los usuarios no deben aprender a realizar configuraciones o instalaciones engorrosas para que los métodos de aseguramiento operen de forma eficaz. El método de la presente invención no posee una verificación de políticas con algún tercero el cual puede ser
- 10 infectado para atacar después los usuarios finales. El método de aseguramiento de la presente invención, no necesita que se hagan instalaciones en el equipo del usuario. Es la aplicación transaccional quien entrega el modelo de seguridad y por tanto no es una decisión del usuario percatarse.
- 15 Basado en los métodos de entrega, la forma en que opera y la cantidad de usuarios que lo pueden usar, el método inventivo permite que las aplicaciones informáticas en las que se intercambia información sensible sean seguras desde cualquier parte. Es decir, cualquier equipo informático utilizado desde cualquier red al momento de intercambiar información o sobre la totalidad de la ejecución de la aplicación si ésta lo desea, al implementar el
- 20 método de la presente invención va a funcionar como un equipo/red segura, cumpliendo y en muchos casos excediendo las especificaciones de seguridad recomendadas por los proveedores de aplicaciones transaccionales.

5. Descripción Detallada

25 Glosario.

Punto final de la transacción. Hace referencia a la pieza de hardware desde la cual se está realizando la transacción. Se conoce como punto final por ser el último dispositivo, contando desde el servidor origen de la información, en el que se despliega la aplicación a utilizar.

Hooking. En programación informática, el término *hooking* cubre una amplia gama de técnicas utilizadas para modificar o aumentar el comportamiento de un sistema operativo, aplicaciones, o de otros componentes de software mediante la interceptación de llamadas a funciones o mensajes o eventos pasados entre componentes de software. El código que

5 maneja tales llamadas a funciones, eventos o mensajes se llama un *hook*.

Hook. Un *hook* es un punto en el mecanismo del sistema de administración de mensajes donde una aplicación puede instalar una subrutina para controlar el tráfico de mensajes en el sistema y procesar cierto tipo de mensajes antes de llegar al procedimiento de la ventana de destino.

10 I/O. En computación, entrada/salida, o I/O, se refiere a la comunicación entre un sistema de procesamiento de la información (tal como un ordenador), y el mundo exterior, tal vez un ser humano, o cualquier otro sistema de procesamiento de la información. Las entradas son las señales o datos recibidos por el sistema, y las salidas son las señales o datos enviados desde la misma. El término también puede ser utilizado como parte de una

15 acción, "realizar I/O" para realizar una operación de entrada o de salida. Dispositivos I/O son usados por una persona (u otro sistema) para comunicarse con una computadora. Por ejemplo, un teclado o un ratón puede ser un dispositivo de entrada para un equipo, mientras que los monitores y las impresoras se consideran dispositivos de salida de un ordenador. Dispositivos para la comunicación entre computadoras, tales como módems y

20 tarjetas de red, por lo general sirven para la entrada y salida.

Shortcuts. Esta expresión hace referencia a las combinaciones de teclas en un sistema operativo que invocan una aplicación o permiten acceder a operaciones particulares cuando son digitadas por el usuario en un teclado de computador.

Clipboard. El portapapeles (*Clipboard*) es una instalación de software que puede ser

25 utilizada para el almacenamiento de datos a corto plazo y/o transferencia de datos entre documentos o aplicaciones, a través de las operaciones de copiar y pegar. Es una parte de un entorno gráfico y se implementa normalmente como un bloque temporal de memoria anónima que se puede acceder desde la mayoría de los programas en el medio a través de interfaces de programación definidas. Una aplicación típica de los accesos por la entrada

de la funcionalidad del portapapeles de asignación de usuarios (combinaciones de teclas, las selecciones de menú, etc) para estas interfaces.

Lista de un antivirus. Las actualizaciones de los sistemas de antivirus son realizadas usualmente basadas en un archivo (Lista) que recuperan remotamente desde los servidores de los fabricantes de antivirus. Esta lista contiene las actualizaciones del sistema para evitar las vulnerabilidades nuevas que ya fueron procesadas por el fabricante y que el antivirus puede ahora interceptar.

Agente. En informática, un agente de software es una pieza de software que actúa para un usuario u otro programa en una relación de agencia, que se deriva del latín *agere* (hacer): un acuerdo para actuar en nombre de un tercero. Tales "acciones en favor de" implican la autoridad para decidir cual acción es la más apropiada. La idea es que los agentes no son estrictamente invocados para una tarea, pero pueden activarse a sí mismos.

Kernel. En informática, el núcleo (Kernel) es el componente central de la mayoría de sistemas operativos; es un puente entre las aplicaciones y el procesamiento de datos reales hecho a nivel de hardware. Las responsabilidades del núcleo incluyen la gestión de los recursos del sistema (la comunicación entre los componentes de hardware y software)

Aplicación cliente. Aplicación cliente se refiere a una aplicación, programa o ejecutable que puede ser un navegador web, una aplicación cliente servidor de escritorio o cualquier aplicativo que se desee proteger.

Escritorio virtual. Es un ambiente de trabajo alterno al que el usuario conoce y trabaja normalmente. Este ambiente se implementa en la misma máquina del usuario y no es necesario un componente servidor que haga las veces de "virtualizador" de servicios.

Descripción detallada.

El método reclamado proporciona un escritorio virtual aislado del ambiente en el cual trabaja el usuario donde no se tiene acceso a las funcionalidades por defecto del sistema operativo. En este escritorio virtual se implantan técnicas de *hooking* para interceptar los mensajes de I/O entre la aplicación transaccional y el sistema operativo del usuario final. Con estas técnicas de *hooking* se ejecutan procesos que bloquean las combinaciones de

teclas especiales; se realiza el bloqueo de todos los accesos rápidos a funcionalidades o *shortcuts*; y se deshabilita el *Clipboard*. Al momento de asegurar el escenario del usuario, éste queda disponible para ejecutar una aplicación cliente. Luego de tener el ambiente seguro ejecutado, se implementa un programa llamado motor de generación de basura (el

5 cuál será explicado más adelante). Cuando el usuario decide terminar la transacción o la aplicación, se desmonta el escritorio virtual, retornando al escritorio primario de tal manera que el usuario puede seguir usando el equipo de forma normal.

El método inventivo de la presente invención puede ser implementado en una amplia

10 variedad de dispositivos electrónicos tales como: un ordenador o computador, un ordenador portátil, estos dos anteriores bajo sistemas operativos Microsoft Windows, entornos UNIX, Linux, MacOS, Novell, etc. En modalidades preferidas el método inventivo se implementa en Sistemas Operativos Microsoft de la familia NT, x86, x32, x64. También puede ser implementado en un asistente personal de datos, un organizador

15 de datos personales, un teléfono celular, un teléfono móvil, un dispositivo de navegación en internet, un electrodoméstico o un teléfono inteligente. Para los entornos donde la implementación se realiza en computadores de escritorio o portátiles, la descripción del presente invento está dirigida a equipos informáticos cliente que trabajan con sistemas operativos Microsoft™.

20

Las compañías pueden distribuir el método de seguridad de la presente invención a las aplicaciones que ya poseen, solamente agregando los pasos al momento de intercambiar información sensible con el usuario. Para aplicaciones informáticas en arquitecturas tipo cliente/servidor, se ejecutan programas informáticos predefinidos por el proveedor de

25 aplicaciones que deben estar alojados en el equipo del usuario final.

Cuando el método inventivo está dirigido para la entrega de aplicaciones en arquitecturas web, se ejecutará un navegador web restringido. Todos los navegadores poseen métodos de ejecución seguros, en donde las funciones de navegación, interacción con contenido,

descarga y demás funciones que tienen los usuarios finales son restringidas y operan basadas en métodos de aseguramiento como listas de comportamiento, que son una buena práctica al momento de navegar por Internet. El método de la presente invención no necesita de las listas o de análisis de comportamientos para la detección de software espía o malicioso en el equipo informático del usuario, pues la finalidad del método no es alertar sobre los problemas de usuario, si no llevarlo a un ambiente seguro donde pueda intercambiar información con la aplicación informática sin el peligro de que un tercero pueda *hackear* la información.

La implementación del método de aseguramiento de la presente invención afecta mínimamente el rendimiento de software y hardware del usuario final. Esto se logra focalizando el uso del método solo para aquellos momentos en que se intercambia información sensible con aplicaciones informáticas. Con el método de la presente invención el usuario final no debe preocuparse por adquirir software, hardware o dispositivos especiales para la utilización del mismo, ya que en una de las modalidades preferidas, la forma de entrega puede ser a través de distribuciones de software conocidas como archivos .exe, .jar, o preferentemente controles de tipo ActiveX™ y Applets.

Haciendo referencia a la Figura 1, el método de la presente invención permite a las compañías tener control de los tres componentes que hacen parte en el intercambio de información: i) sus servidores (11), los cuales están protegidos desde sus centros de datos y donde se encuentran los proveedores de servicios como e-Commerce, e-Learning, correo electrónico, SaaS, CloudComputing, etc, ii) la red (13), que va desde Internet (el caso más deseable), entornos empresariales o redes pequeñas, asegurada con métodos informáticos tecnológicos y iii) los agentes externos (15) que son los puntos de acceso finales desde donde se despliega el método inventivo .

A diferencia de los métodos tradicionales para la detección y corrección de problemas de seguridad, el método inventivo no utiliza componentes servidores para hacer monitoreo, registro o auditoría de los contenidos ni de los comportamientos de ejecución. Como se ha

especificado, esta solución solo opera al momento del intercambio de la información o donde el proveedor de la aplicación informática lo desee.

Haciendo referencia a la Figura 2, el método inventivo comienza a funcionar desde un ambiente no protegido (21) donde se ejecuta cualquier aplicación (exploradores web, aplicaciones empresariales, ofimática, etc.) (23). Mediante la instrucción de un agente externo (v.gr. un usuario), el método inventivo determina que la aplicación informática con la cual el usuario desea trabajar inicia un proceso de intercambio de información sensible (25), dando acceso a las API (Application Programming Interface, v.gr. API para crear procesos, CreateProcess) para la creación del ambiente aislado (27). Esta acción de acceso a las API se puede realizar entregando agentes (software) a los usuarios, que se ejecutan al momento del intercambio de información o usando tecnologías como ActiveX™ o Applets que pueden acceder a funcionalidades del sistema operativo. El ambiente seguro o aislado no interactúa con partes del sistema que no sean necesarias para la transacción, de tal forma que ni el método inventivo permite que otras aplicaciones que se estén ejecutando en el sistema vean las funciones de la aplicación protegida, ni la aplicación protegida puede ver o acceder a funciones de otras aplicaciones, por lo que puede asegurar que no se encuentra comprometido por los diversos riesgos latentes en el sistema. Para su creación es necesario del uso de varias técnicas informáticas plenamente conocidas en el sector. Esta serie de técnicas están basadas en el uso de las API de Windows™ para la creación, administración y destrucción del ambiente aislado sin necesidad de la intervención del usuario final en el proceso, como la instalación de agentes o configuraciones especiales dentro sus navegadores (si la aplicación que desea entregar este método inventivo es web). Con las API del sistema operativo Windows™ se obtiene acceso a todas las funcionalidades del sistema operativo, incluyendo funciones en el *kernel*, como interfaces entre aplicaciones informáticas ya existentes.

Al momento de finalizar el uso de la aplicación en el ambiente aislado y esta se cierra (211), se utilizan estas mismas API para realizar el proceso de eliminación de todos los

componentes usados para la entrega del ambiente seguro. Al terminar este proceso al usuario se le entrega de nuevo su ambiente de trabajo normal (213) o escritorio por defecto.

5 La Figura 3, que describe los pasos para la generación de un ambiente aislado para el intercambio de información. Al empezar el intercambio de información, la aplicación informática crea un escritorio virtual (31) haciendo uso del API del sistema para este fin. Es en este entorno donde se ejecutarán las aplicaciones, servicios y funcionalidades que se necesiten para intercambiar información con el usuario. El entorno virtual creado permite
10 controlar todos los mensajes de sistema que llegan al escritorio virtual (33), se implantan *hooks* adicionales para la administración de las combinaciones de teclado conocidas como accesos rápidos o *shortcuts* (35). Los mismos *hooks* deshabilitan herramientas que permitan la administración de procesos (37) y el portapapeles o *ClipBoard* (39). Al finalizar la implantación de estos mecanismos de seguridad se procede a la presentación de
15 la aplicación transaccional (311) con la cual desea trabajar el usuario final y con esta se ejecuta el motor generador de basura (312), el cual genera eventos I/O de aplicación y de usuario aleatorios en el sistema. Así el usuario posee un escenario seguro para hacer sus transacciones electrónicas.

20 Haciendo referencia a la Figura 4, con la creación del escritorio virtual se realizan acciones complementarias como la implantación de *hooks* (33) (ver Figura 3) de ejecución en la cola de mensajes del sistema operativo. Estos *hooks* permiten la administración a nivel de la aplicación, de los mensajes para la ejecución de las funciones de cursor (41), teclado (43), pantalla (47), dispositivos externos y aplicaciones del sistema. Al implantar estos *hooks* se
25 pretende que todos los mensajes sean procesados primero por el nuevo escritorio virtual y no por el escritorio habitual de trabajo del usuario.

Haciendo referencia a la Figura 5, al momento de administrar los mensajes de I/O en el sistema operativo, se bloquea el uso de comandos de teclado (45) (ver Figura 3) tales como CTRL+ALT+DEL (51), CTRL+ESC (53), CTRL+TAB (55), TECLA WINDOWS (57)

(en los sistemas soportados) y usando *hooks* específicos para estos mensajes se puede evitar la ejecución de aplicaciones informáticas no deseadas durante el proceso de intercambio.

- 5 Haciendo referencia a la Figura 3, el administrador de procesos, por ser una herramienta tan importante y potente dentro del sistema requiere de un manejo adicional, el cual involucra la modificación del *kernel*, por ejemplo el registro de Windows. Siguiendo el ejemplo en Windows, se busca modificar las claves de registro de Windows que permiten la ejecución y presentación del administrador de procesos al usuario final, y así esta
- 10 aplicación también es bloqueada (37). Se realiza este proceso adicional para suplir la vulnerabilidad persistente en entornos Windows 6 en adelante donde la combinación CTRL+ALT+DEL es una combinación propia del *kernel*, donde cualquier otra aplicación que no sea el *kernel*, no puede administrar la combinación de teclas CTRL+ALT+DEL.
- 15 Haciendo referencia a la Figura 5, las aplicaciones informáticas, para términos de facilidad de uso y supliendo requerimientos no funcionales, por lo general implementan dentro de sus rutinas de ejecución los accesos directos a funciones de la misma. Estos accesos son la combinación de teclas como por ejemplo CTRL+P, entre otras. El ambiente aislado, proporcionado por el método inventivo de la presente invención, hace uso de las API del
- 20 sistema operativo que permiten el bloqueo de todas las combinaciones conocidas y las no conocidas para obtener control sobre la ejecución de las aplicaciones que se ejecutan sobre el ambiente aislado (59).

- Siguiendo con la secuencia en la Figura 3, al momento en que el motor de *hooking* ha sido
- 25 implementado dentro del ambiente aislado se bloquea el servicio de *ClipBoard* (39) para que no registre la información usada en la transacción y posterior uso del usuario o la toma de pantallas.

Con la implementación de todas las técnicas descritas anteriormente se establece un ambiente aislado (27) (ver Figura 2) protegido contra las amenazas conocidas para el robo de información, donde las aplicaciones del ambiente original del usuario siguen funcionando pero no operan dentro del nuevo ambiente aislado (27). En este escritorio se le entrega al usuario la interfaz de intercambio de información con la aplicación informática (311) (Figura 3) donde se puede realizar la transacción de manera segura (313). Es decir, cuando el ambiente aislado es ejecutado en su totalidad, el usuario verá el formulario digital, pagina web o cualquier otra interfaz de usuario final que el proveedor de aplicaciones informáticas desee.

10

Dentro del método inventivo de la presente invención se especifica la creación, ejecución y posterior destrucción de un motor de generación de basura que crea eventos aleatorios (312) en el sistema. Este motor permite que, dentro del ambiente aislado o protegido (27) (Ver Figura 2), se creen eventos basura. De esta manera, si existe algún tipo de software espía o malicioso que logra capturar información, le sea complejo discernir qué información es real y cuál es falsa.

15

Haciendo referencia a la Figura 6, este motor está compuesto por una serie de funciones separadas que permiten la generación de eventos de cursor (61), dentro de los cuales se registran movimientos, cambios de posición y generación de clics por parte del usuario, aunque este no haga ninguna acción real en el equipo. También hay un generador de eventos de teclado (63) que simula el funcionamiento de un teclado físico externo como si el usuario estuviera presionando teclas. Igualmente, se registra el uso del teclado aunque, como en el caso del cursor, el usuario no haga uso del dispositivo. La generación de eventos visuales (65), como cambios en la pantalla, en botones e imágenes que se le presentan al usuario, es relevante para evitar ataques desde componentes de software como *screenloggers* o capturadores de pantalla y delitos como la captura de la pantalla por medio de cámaras fotográficas o web.

20

25

También se pueden adicionar otro tipo de eventos (67) como el arrastrar y pegar, cargar páginas de internet, entre otros. Cabe aclarar que en este punto, el método inventivo puede integrar la generación de cualquier evento que sea requerido.

- 5 Haciendo referencia a la Figura 7, sin importar el resultado de la transacción al finalizar el intercambio de información (71), la aplicación informática con la cual está trabajando el usuario debe retornar el control de todas las funciones y aplicaciones del escritorio predeterminado o por defecto. Para esto se debe: cerrar la aplicación (75), automáticamente el método inventivo debe eliminar el motor de generación de basura (76),
- 10 habilitar el *clipboard* (77), habilitar el administrador de procesos del sistema residente (79), eliminar toda la infraestructura de *hooking* implementada (711) y por último, eliminar el escritorio virtual (713). Todo este proceso ocurre de manera transparente para el usuario, ya que no existe ninguna clase de mensajes que le permitan al usuario percatarse de la existencia o eliminación de funciones de bloqueo.

15

El usuario después de realizar las transacciones utilizando el método de la presente invención, retorna (715) a sus labores sin sensación de realizar procesos engorrosos para poder asegurar su información.

- 20 El método inventivo está dirigido a complementar los métodos ya utilizados (v.gr. Intercambio de información por medio de certificados SSL) por los proveedores de servicios como e-commerce, e-learning, SaaS, Cloudcomputing, etc., para que sus usuarios finales puedan hacer uso de sus servicios desde cualquier red segura o insegura y desde cualquier dispositivo informático conocido o desconocido tanto para el usuario como para
- 25 la compañía que provee la aplicación.

El método inventivo permite que las compañías elijan cualquier forma de entrega, de tal manera que éste puede estar inmerso en un archivo ejecutable que se descargue desde una zona determinada por la compañía y alojado en el equipo informático del usuario final. La

identidad del control está asegurada utilizando certificados de autenticación de código. Para la modalidad preferida de la invención se deben usar con Microsoft Autenticode Sign; estos certificados garantizan que los ejecutables pertenecen a compañías válidas y confiables.

5

La modalidad preferida para la entrega del método inventivo es la construcción de controles *ActiveX*TM y *Applets*TM embebidos en las aplicaciones informáticas. A estos métodos se les debe dar también certificados de autenticación de código.

10 Se debe entender que la presente invención no se halla limitada a las modalidades descritas e ilustradas, pues la presente invención comprende muchas variaciones y modificaciones posibles que no se apartan del espíritu de la invención, el cual solo se encuentra definido por las siguientes reivindicaciones.

15

RESUMEN

La presente invención divulga un método de seguridad informática que permite a usuarios de una aplicación informática poseer niveles superiores de seguridad al momento de intercambiar información sensible con aplicaciones transaccionales. Cualquier usuario (sin necesidad de conocimientos avanzados en tecnologías) desde cualquier lugar, usando cualquier tipo de red puede realizar transacciones electrónicas con un muy bajo riesgo de que su información sea robada o comprometida.

20

El método consiste en el desarrollo de un escritorio virtual que aísla el ambiente en el cual trabaja el usuario, implantando técnicas de *hooking* para interceptar mensajes entre la aplicación transaccional y el sistema operativo del usuario. Adicionalmente el método bloquea las combinaciones de teclas especiales para prevenir la ejecución de código malicioso. Durante el uso de la aplicación, se generan eventos basura en el sistema operativo del usuario. Cuando el usuario determine la terminación de la sesión segura, se retorna al escritorio original y el usuario puede seguir usando el equipo de forma normal.

25

REIVINDICACIONES

1. Un método para efectuar una transacción electrónica segura, caracterizado porque comprende los siguientes pasos:

5

- a. abrir una sesión de un escritorio virtual sobre un Sistema Operativo (SO) mediante la implementación de una Interfaz de Programación (API);
- b. implementar técnicas de hooking que incluyen una función del SO seleccionada del grupo que consiste de:

10

- i. inactivación del servicio del portapapeles nativo del SO; y
 - ii. inactivación del administrador de procesos del SO;
- c. ejecutar una Aplicación segura del Cliente; y
- d. finalizar sesión del escritorio virtual.

15

2. El método de la Reivindicación 1, donde las técnicas de hooking del paso (b) también incluyen una función del SO seleccionada del grupo que consiste de:

- i. mensajes de datos entre el SO y la Aplicación;
- ii. bloqueo de combinaciones de teclas especiales nativas del SO;
- iii. bloqueo de accesos rápidos nativos del SO y de las aplicaciones del cliente;

20

3. El método de la Reivindicación 2, caracterizado porque en las funciones del grupo (i), los mensajes entre el SO y la Aplicación incluyen funciones de entrada/salida (I/O).

25

4. El método de la Reivindicación 3, caracterizado porque las funciones I/O son servicios entre el SO y cualquier dispositivo externo.

5. El método de la Reivindicación 2, caracterizado porque la administración de las funciones de bloqueo (ii) y (iii) se ejecuta en la cola de mensajes del SO.
6. El método de la Reivindicación 5, caracterizado porque las funciones de bloqueo (ii) y (iii) son mensajes dirigidos al bloqueo de las funciones de cursor, teclado, pantalla, dispositivos externos y aplicaciones del sistema.
7. El método de la Reivindicación 4, caracterizado porque los mensajes de I/O en el SO bloquea el uso de combinaciones de teclas tales como CTRL, ALT, SHIFT, TAB, ESC, DEL, y TECLA WINDOWS.
8. El método de la Reivindicación 1, caracterizado porque antes del paso (c), comprende el paso de generar eventos basura.
9. El método de la Reivindicación 8, caracterizado porque los eventos basura incluyen eventos aleatorios de I/O, de aplicación y de usuario en el sistema.
10. El método de la Reivindicación 9, caracterizado porque los eventos basura incluyen eventos de cursor, dentro de los cuales se simulan movimientos, cambios de posición y generación de clics por parte del usuario.
11. El método de la Reivindicación 8, caracterizado porque los eventos basura simulan el funcionamiento de un teclado físico externo como si el usuario estuviera presionando teclas.
12. El método de la Reivindicación 9, caracterizado porque los eventos basura simulan la generación de eventos visuales, como cambios en la pantalla, en botones e imágenes de la Aplicación.

13. El método de la Reivindicación 1, caracterizado porque ninguna otra aplicación que se esté ejecutando en el SO puede interactuar con la Aplicación segura.

5 14. El método de la Reivindicación 1, caracterizado porque la Aplicación segura no puede acceder a funciones de otras aplicaciones.

15. El método de la Reivindicación 1, caracterizado porque el escritorio virtual controla el tráfico de todos los mensajes y servicios generados por el SO y la Aplicación.

10 16. El método de la Reivindicación 1, en donde la implantación de hooks ocurre de manera transparente para la Aplicación y para el Cliente.

15 17. El método de la Reivindicación 1, caracterizado porque el paso (d) de finalizar sesión del escritorio virtual, incluye eliminar los componentes de software implementados.

18. El método de la Reivindicación 8, caracterizado porque el paso (d) de finalizar sesión del escritorio virtual, elimina el motor de generación de basura.

20

FIGURA 1

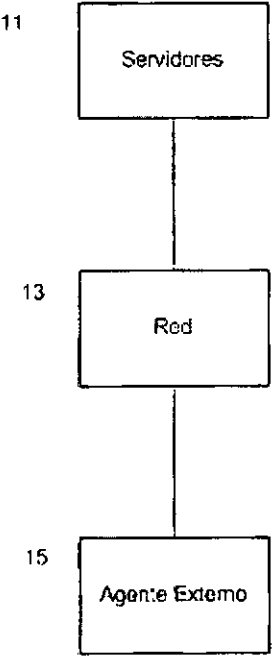


FIGURA 2

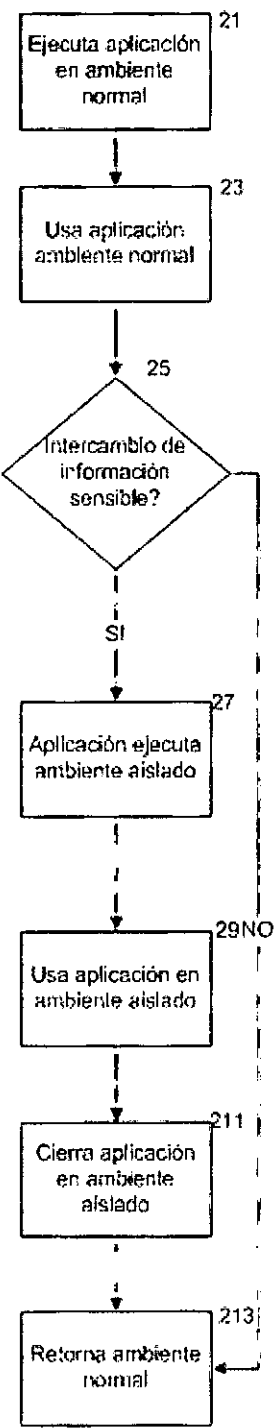


FIGURA 3

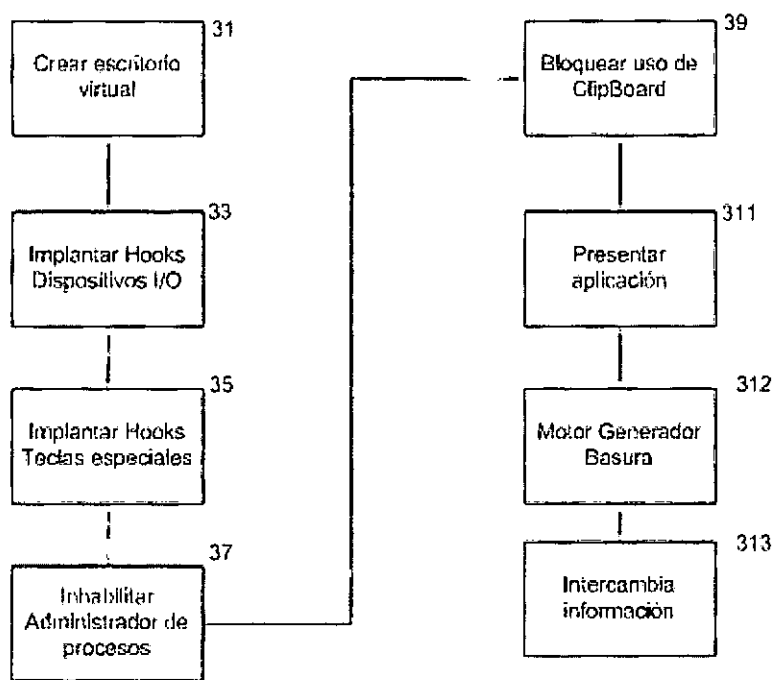


FIGURA 4

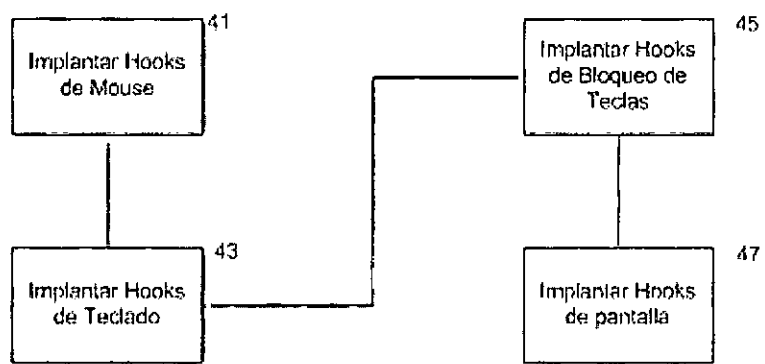
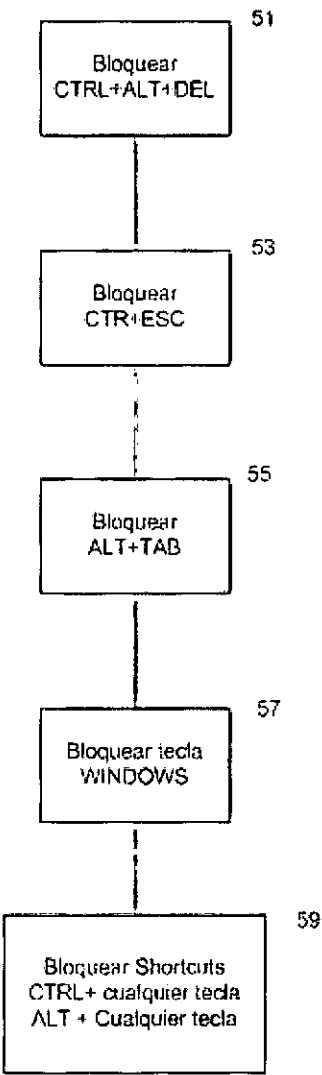


FIGURA 5



3A

FIGURA 6

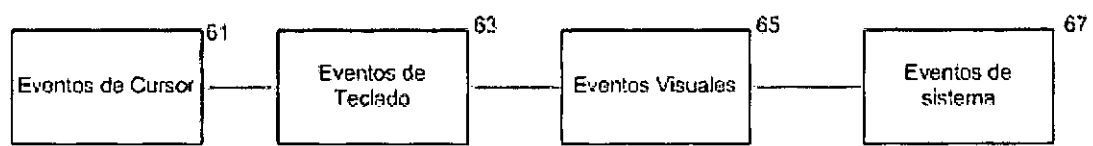
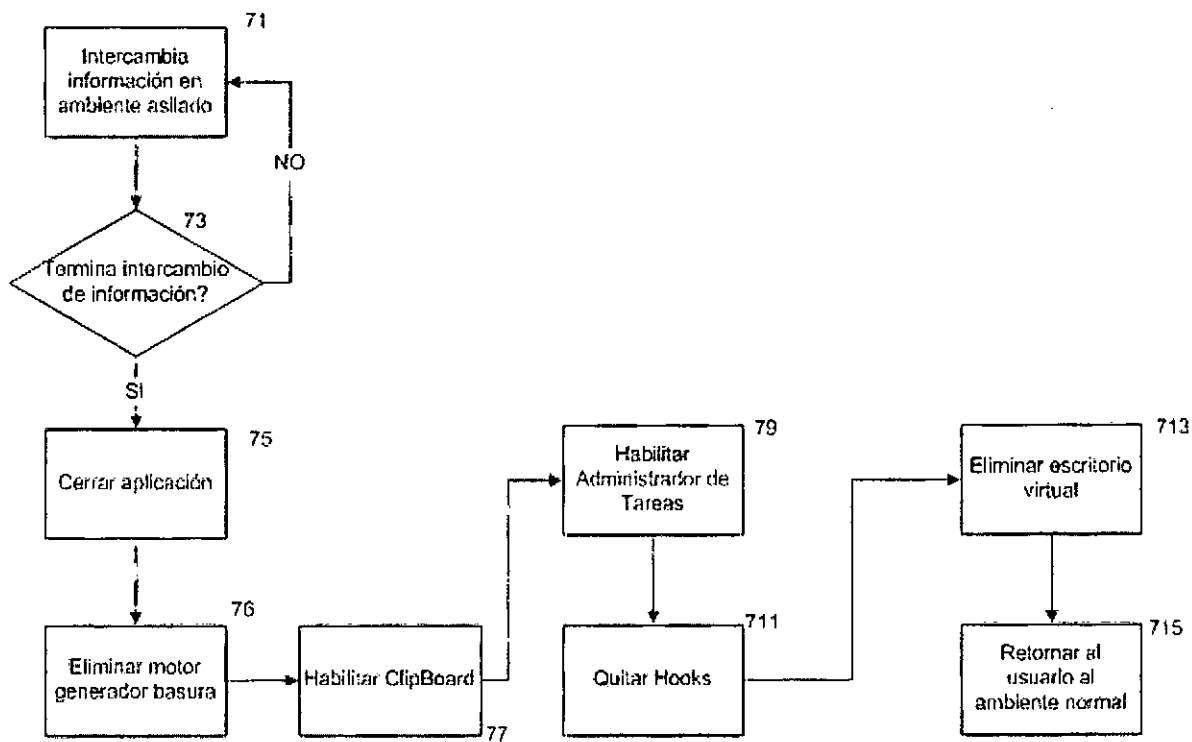
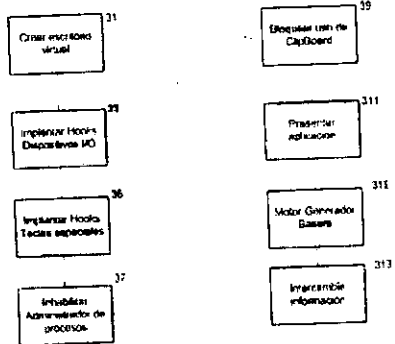
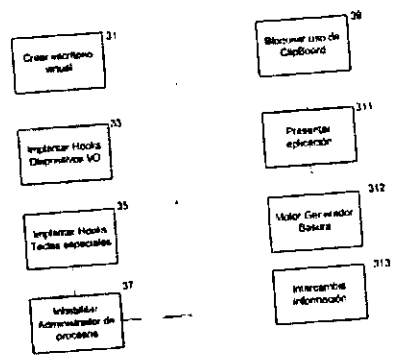
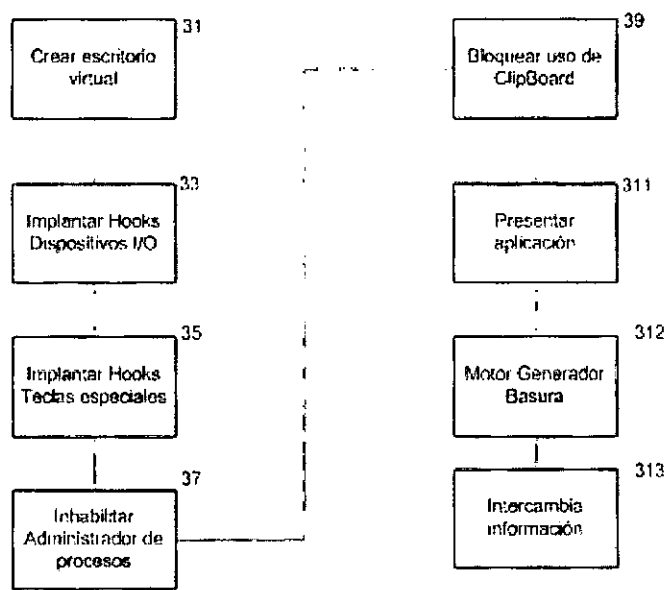


FIGURA 7



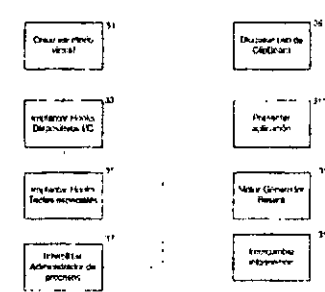






 Industria y Comercio SUPERINTENDENCIA		SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DIVISION DE NUEVAS CREACIONES TARJETA ARCHIVO PROPIETARIOS	
		PATENTE DE INVENCION ☒ PCT ☐ MODELO DE UTILIDAD ☐ DISEÑO INDUSTRIAL ☐	
(21) N° de solicitud:		(22) Fecha de solicitud: 26 DE ABRIL DE 2011	
(51) Clasificación Internacional:			
(71) Solicitante(s) AZUAN TECHNOLOGIES S.A.			
(72) Inventor(es) JAIME ENRIQUE GÓMEZ HERNÁNDEZ, CARLOS A. PERRY PEINADO, WILMER LINARES MONTAÑEZ, IVÁN DARÍO TOVAR RUEDA.			
(74) Apoderado: CARLOS R. OLARTE			
(30) Prioridad	(31) No. Prioridad	(32) Fecha	(33) País
(85) Fecha inicio fase nacional:		(87) Publicación internacional	
(86) Datos relativos a la presentación de la solicitud PCT		Fecha: Fecha (dd/mm/aa)	
Fecha de presentación de la solicitud: Fecha (dd/mm/aa)		N° publicación: WO	
No. de solicitud PCT/			
(54) Título: MECANISMO PARA ASEGURAMIENTO DE TRANSACCIONES ELECTRONICAS			

40

 Industria y Comercio SUPERINTENDENCIA		SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DIVISION DE NUEVAS CREACIONES TARJETA ARCHIVO TEMATICO	
PATENTE DE INVENCION <u> X </u> PCT <u> </u>		MODELO DE UTILIDAD <u> </u> DISEÑO INDUSTRIAL <u> </u>	
(21) N° de solicitud: _____ (22) Fecha de solicitud: 26/04/2011			
(51) Clasificación Internacional: _____			
(71) Solicitante(s) AZUAN TECHNOLOGIES S.A.			
(72) Inventor(es) JAIME ENRIQUE GÓMEZ HERNÁNDEZ, CARLOS A. PERRY PEINADO, WILMER LINARES MONTAÑEZ, IVÁN DARÍO TOVAR RUEDA.			
(74) Apoderado: CARLOS R. OLARTE			
(30) Prioridad _____ (31) No. Prioridad _____ (32) Fecha _____ (33) País _____			
(85) Fecha límite inicio fase nacional: _____ (86) Datos relativos a la presentación de la solíc. PCT Fecha de presentación de la solicitud: _____ No. de solicitud PCT/ _____		(87) Publicación internacional: Fecha: _____ No. Publicación : WO _____	
(54) Título: MECANISMO PARA ASEGURAMIENTO DE TRANSACCIONES ELECTRONICAS			
(57) Resumen: La presente invención divulga un método de seguridad informática que permite a usuarios de una aplicación informática poseer niveles superiores de seguridad al momento de intercambiar información sensible con aplicaciones transaccionales. Cualquier usuario (sin necesidad de conocimientos avanzados en tecnologías) desde cualquier lugar, usando cualquier tipo de red puede realizar transacciones electrónicas con un muy bajo riesgo de que su información sea robada o comprometida. El método consiste en el desarrollo de un escritorio virtual que aísla el ambiente en el cual trabaja el usuario, implantando técnicas de hooking para interceptar mensajes entre la aplicación transaccional y el sistema operativo del usuario. Adicionalmente el método bloquea las combinaciones de teclas especiales para prevenir la ejecución de código malicioso. Durante el uso de la aplicación, se generan eventos basura en el sistema operativo del usuario. Cuando el usuario determine la terminación de la sesión segura, se retorna al escritorio original y el usuario puede seguir usando el equipo de forma normal.			

AL DILIGENCIAR POR FAVOR NO VARIAR EL TAMAÑO DE LA TARJETA

ESTA SE IMPRIME EN CARTULINA BLANCA

 Industria y Comercio SUPERINTENDENCIA		SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO DIVISION DE NUEVAS CREACIONES EXTRACTO PARA PUBLICACIÓN SOLICITUD DE PATENTE DE INVENCION	
(21) N° de solicitud: 22) Fecha de solicitud: (30) Prioridad (31) <i>No. Prioridad</i> 32) <i>Fecha</i> (33) <i>País</i>		(51) Int Cl: (71) Solicitante(s) AZUAN TECHNOLOGIES S.A. (72) Inventor(es) JAIME ENRIQUE GÓMEZ HERNÁNDEZ, CARLOS A. PERRY PEINADO, WILMER LINARES MONTAÑEZ, IVÁN DARÍO TOVAR RUEDA. (74) Apoderado: CARLOS R. OLARTE	
(54) Título: MECANISMO PARA ASEGURAMIENTO DE TRANSACCIONES ELECTRONICAS			

Reivindicación(es):
 La presente invención divulga un método de seguridad informática que permite a usuarios de una aplicación informática poseer niveles superiores de seguridad al momento de intercambiar información sensible con aplicaciones transaccionales. Cualquier usuario (sin necesidad de conocimientos avanzados en tecnologías) desde cualquier lugar, usando cualquier tipo de red puede realizar transacciones electrónicas con un muy bajo riesgo de que su información sea robada o comprometida.

El método consiste en el desarrollo de un escritorio virtual que aísla el ambiente en el cual trabaja el usuario, implantando técnicas de hooking para interceptar mensajes entre la aplicación transaccional y el sistema operativo del usuario. Adicionalmente el método bloquea las combinaciones de teclas especiales para prevenir la ejecución de código malicioso. Durante el uso de la aplicación, se generan eventos basura en el sistema operativo del usuario. Cuando el usuario determine la terminación de la sesión segura, se retorna al escritorio original y el usuario puede seguir usando el equipo de forma normal.



No. 11-050985-00000-0000

Fecha: 2011-04-26 16:44:30 Dep. 2020 DIR.NUEVASCR
Tra. 2 PATENTES Eve: 1 REGDEPOSITO
Act. 411 PRESENTACION Folios: 41

PATENTE DE INVENCION ☒

MODELO



Indicación que se solicita una patente.

Datos de identificación del solicitante o de la persona que presenta la solicitud

Descripción de la invención

Dibujos de ser estos pertinentes

Comprobante de pago de las tasas establecidas (De ser el caso formato de descuento)

Completa ☒

Incompleta ☐

PATENTE DE INVENCION PCT ☐ MODELO DE UTILIDAD PCT ☐ Art.33 Decisión 486/00, Circular Única



Indicación que se solicita una PCT



Copia de la solicitud en español, tal como fue presentada inicialmente (capítulo descriptivo, reivindicatorio, resumen)



Dibujos de ser estos pertinentes



Comprobante de pago de las tasas establecidas (de ser el caso formato de descuento)

Completa ☐

Incompleta ☐

DISEÑO INDUSTRIAL ☐

(Art. 119 Decisión 486/00)



Indicación que se solicita 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 ☐

(Art. 92 Decisión 486/00)



Indicación que se solicita un esquema de trazado



Datos de identificación del solicitante o de la persona que presenta la solicitud



Representación gráfica de un esquema de trazado



Comprobante de pago de las tasas establecidas

Completa ☐

Incompleta ☐



Bogotá D.C.,
2020

Doctor(a)
OLARTE GARCIA CARLOS REINALDO
Apoderado(a) y/o Representante de
AZUAN TECHNOLOGIES S.A

REFERENCIA	Radicación No.	11 050985
	Trámite	2
	Evento	1
	Actuación	430
	Oficio No.	

008835

Teniendo en cuenta que el capítulo reivindicatorio presentado excede de diez reivindicaciones, es necesario que cancele la tasa establecida por cada reivindicación adicional presentada, de conformidad con lo dispuesto en la resolución de tasas vigente para la fecha de presentación de la solicitud, so pena de que no sean tenidas en cuenta dentro del presente trámite administrativo.

En consecuencia, con fundamento en lo previsto por el artículo 12 del Código Contencioso Administrativo, se le requiere para que dentro del término de dos (2) meses siguientes a la fecha de notificación del presente oficio atienda el requerimiento aquí señalado. Lo anterior, con el alcance que para tal efecto establece el artículo 13 de la misma codificación, respecto de las reivindicaciones adicionales.

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.

JOSE LUIS SALAZAR LOPEZ
Director de Nuevas Creaciones (c)

02 JUN. 2011

El anterior requerimiento fue notificado por fijación en lista de fecha _____.
adpa11