



Instituto Mexicano de  
Contadores Públicos

La coordinación de este número  
de Contaduría Pública estuvo a cargo de:



C.P.C. y C.I.A. Beatriz Castelán García  
Ing. Edmundo Rodríguez Valenzuela

## COMITÉ EJECUTIVO NACIONAL 2004-2005

### Presidente

C.P.C. Pablo Mendoza García

### Vicepresidente General

C.P.C. Alberto Álvarez del Campo

### Tesorero

C.P.C. Luis González Ortega

### Secretario

C.P.C. Aristides Nieto Pérez

### Protesorero

C.P.C. Francisco Javier García Sabaté Palazuelos

### Director Ejecutivo

C.P.C. Federico Ríos León y Vélez

### Auditor

C.P.C. Juan Manuel Ferrón Solís

### Vicepresidentes de Operación

#### Legislación

C.P.C. Luis Moirón Llosa

#### Práctica Externa

C.P.C. Jaime Sánchez-Mejorada Fernández

#### Relaciones y Difusión

C.P.C. José T. Franco Minero

#### Sector Empresas

C.P.C. Raúl González Lima

#### Docencia

C.P.C. Eduardo Ávalos Lira

#### Sector Gobierno

C.P.C. Tirso Agustín Rodríguez de la Gala Gómez

#### Fiscal

C.P.C. Enrique Arturo Manrique Díaz Leal

### Vicepresidencias Regionales

#### Centro

C.P.C. Eduardo Ojeda López Aguado

#### Centro-Istmo-Peninsular

C.P.C. Rodolfo Kantún Kantún

#### Centro-Occidente

C.P.C. Luis Raúl Michel Domínguez

#### Noreste

C.P.C. José Alberto Mota Barragán

#### Noroeste

C.P.C. Valentín Castillo Garzón

#### Presidente de la Comisión de Relaciones,

#### Apoyo y Servicio a Federadas

C.P.C. José Antonio Snell Arguijo

#### Comité de Innovación

C.P.C. Marco Antonio Canales Durán

6



## EDITORIAL

### 4 Seguridad de la información

## SEGURIDAD DE LA INFORMACIÓN

### 6 Los delitos informáticos y el cómputo forense

Ing. Andrés Velázquez, CISSP, BS7799, CSIRT

Cada crimen tiene una escena que puede llegar a ser asegurada para buscar evidencia; pero, en una computadora, los bits y los bytes se esconden.

### 10 Aspectos legales y éticos de la seguridad informática

Ivonne V. Muñoz Torres, MCE

La seguridad informática es uno de los temas que mayor auge tiene en la actualidad desde su promoción hasta su implementación.

### 14 Las certificaciones en seguridad

Ángel G. Espinosa Sarmiento, CISSP, CISM

Estas certificaciones regirán la demanda de profesionales en el mercado formal de estos servicios.

### 18 Amenazas humanas y métodos más comunes para acceder a los recursos computacionales

Mtra. María Teresa Pérez Morales

Cada vez más organizaciones colocan sus negocios en el e-Business, e-Commerce y e-Movil.

### 26 Criptología y la seguridad en internet

Dr. Roberto Gómez Cárdenas

La criptología es la ciencia que estudia los aspectos y contenidos de información en condiciones de secrecía.

### 29 Security Awareness: un factor crítico de éxito en la seguridad de la información

Israel Cortés Ramírez, CISA, CISM

Awareness es un programa que transmite mensajes asertivos para que los empleados estén atentos a la seguridad de la información.

### 32 El ambiente de seguridad en SAP R/3

L.S.C.A. Luis Fernando Orozco H.

La seguridad del SAP R/3 permite un control detallado de los permisos de acceso, pero no está listo para usarse como lo entrega el proveedor.

### 34 Gestión de la continuidad del negocio

L.I.A. Sandra Urías Iris

La evolución de los planes de recuperación para casos de desastre en las empresas ha dado lugar al surgimiento de un nuevo concepto: BCM.

### 36 Seguridad de la información: ¿Dejarla a la suerte?

Guadalupe Castañeda Campos CPA, CISA

Según la 7ª Encuesta Global de Seguridad de la Información de ME&Y muchas organizaciones confían en la suerte sobre seguridad de la información.

### 39 Los medidores del desempeño en la seguridad informática

C.P.C. Edgar de la Rosa Cabello

Los medidores del desempeño en la seguridad son cruciales cuando hay sistemas de información complejos y con una alta dependencia.

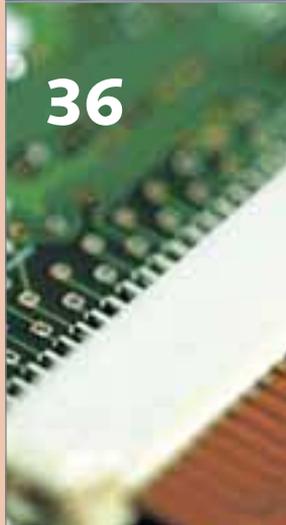
14



29



36



**42 La seguridad informática en México**  
Ing. Gabriel Gálvez Betancourt • Lic. Ángel F. Brindis Nateras  
La seguridad informática es sinónimo de seguridad de la información, la cual se clasifica en: datos, voz e imagen.

**44 Auditoría de seguridad**  
M. A. Zeuz Zamora Herrera  
La ausencia de una cultura preventiva de seguridad, ocasiona que no se valoren los beneficios de realizar inversiones en este tema.

**50 La seguridad informática en el Banco de México. Entrevista con Jesús Vázquez Gómez, Dr. en Seguridad Computacional, Jefe de la Oficina de Seguridad Informática del Banco de México**  
C.P.C. y C.I.A. Beatriz Castelán García • Ing. Edmundo Rodríguez Valenzuela

**54 El reto de la seguridad de la información en México, una estrategia para abordarla. Entrevista con el Lic. Adrián Palma Castillo, Presidente de la ALAPSI**  
C.P.C. y C.I.A. Beatriz Castelán García • Ing. Edmundo Rodríguez Valenzuela

## SECCIONES

### TRANSPARENCIA

**56 La alianza con la sociedad, pieza fundamental para prevenir la corrupción**  
Lic. Benjamín Hill Mayoral  
El siguiente artículo aborda el tema del papel fundamental que ocupa la sociedad en el combate a la corrupción.

### CONPA 50 Aniversario

**58 Enfrentemos con éxito el reto de elevar la calidad de nuestros servicios**  
C.P.C. Fernando J. Morales Gutiérrez  
Análisis de la calidad de los servicios prestados por los auditores externos y la pérdida de confianza del público en la información financiera.

### CERTIFICACIÓN

**60 Examen Uniforme de Certificación. Resumen 1999-2004 de los 10 EUC realizados**  
Lic. Willebaldo Roura Pech  
Este artículo presenta los números de los EUC que, a la fecha, se han presentado con las cifras más relevantes en diferentes aspectos.

### HORIZONTES

**64 Los abusos cibernéticos y algunas medidas preventivas**  
C.P.C. y C.I.A. Beatriz Castelán García  
Ante los problemas de virus, debemos replantear el cuidado en el manejo cibernético de nuestra información.

48



56



60



64



#### COMISIÓN DE REVISTA

<b>Presidente</b>	C. P. C. Gabriel Bustos Porcayo
<b>Secretario</b>	C. P. Fernando Álvarez Zamudio
<b>Miembros</b>	C. P. Eduardo Ávalos Lira C. P. C. José Miguel Barañano C. P. C. Carlos Carpy Morales C. P. C. y C. I. A. Beatriz Castelán García C. P. C. Sergio Cervantes Ruiz-Olloqui C. P. C. Roberto Córdoba Vital C. P. C. Irving A. González Esqueda C. P. C. Jorge L. Hernández Baptista C. P. C. Arturo Luna López C. P. y M. A. Sylvia Meljem E. de R. C. P. C. Luis Moreno Noriega C. P. Nicolás Olea Zuazeta M. D. I. Andrea Ruiz Rivas C. P. Pedro Luis San Martín

#### DIRECTORIO

<b>Gerente Editorial</b>	L. C. G. Jaime A. Cortés Ramírez
<b>Gerente Comercial</b>	Ing. Sandra Zárate Rodríguez
<b>Publicidad y Suscripciones</b>	Elena Ramos Vallarino
<b>Distribución</b>	Luis E. Almorojo Mondragón
<b>Diseño Gráfico</b>	Jorge Aranda Fdez. • Grupo Ajusto

<b>Suscripción anual</b>	República Mexicana \$ 450.00 Extranjero (incluye gastos de envío) Continente Americano U.S. Cy. 125.00 Continente Europeo U.S. Cy. 175.00
<b>Precio por ejemplar</b>	\$ 45.00

Tabachines 44, Bosques de las Lomas, México 11700, D.F.  
Tel.: 52-67-64-00, FAX 55-96-69-50  
E-mail: suscripcion@imcp.org.mx

Tiraje 22,500 ejemplares  
Publicación Certificada por el  
**ivm**  
Instituto Verificador de Medios  
Registro No. 071/12

CONTADURÍA PÚBLICA. Órgano oficial de difusión del IMCP. Es una publicación mensual. Aparece los primeros días de cada mes. Se distribuye entre miembros de los colegios de profesionales y entre ejecutivos que ocupan puestos directivos como: presidente, gerente general, contralor, gerente administrativo, gerente financiero, en universidades, organismos profesionales y entre los principales funcionarios de los sectores público y privado.

#### POLÍTICAS EDITORIALES:

Los artículos publicados expresan la opinión del autor o autores, sin que tenga que coincidir necesariamente con el punto de vista del IMCP, respecto al tema tratado.

Cuando se exprese la opinión del IMCP se especificará claramente. No se permite la reproducción de los artículos publicados sin la autorización escrita del Instituto Mexicano de Contadores Públicos, A.C.

CONTADURÍA PÚBLICA está autorizada como publicación periódica por el Servicio Postal Mexicano. Registro 0130972 de fecha 28 Sep. 72.

Impreso en los Talleres de Imprenta Ajusto, S.A. de C.V.

Tel. 57-40-56-20 Fax 57-40-27-41

Características 228351415.

Certificado de Licitud de Título 1721

Certificado de Licitud de Contenido 995

*La cada vez mayor dependencia tecnológica de las organizaciones e individuos para la realización de sus actividades, traducida en el uso generalizado de la internet y sus servicios, sistemas de información, computadoras portátiles, de escritorio, las agendas electrónicas y las tecnologías inalámbricas han hecho que el acceso a datos e información sea más fácil que nunca antes. Lo que, desde otra perspectiva, ha generado nuevas oportunidades para el surgimiento de problemas relacionados con la tecnología tales como el robo de datos, los ataques maliciosos mediante virus, el hackeo a los equipos de cómputo y redes de telecomunicaciones así como los ataques de negación de servicios, entre otros, que en particular y en conjunto constituyen los riesgos de esta evolución.*

Las fallas de seguridad pueden ser costosas para la organización, las pérdidas pueden ocurrir como resultado de la falla misma o pueden derivarse de la recuperación del incidente, seguidos por más costos para asegurar los sistemas y prevenir fallas. Un conjunto bien definido de políticas y procedimientos de seguridad puede prevenir pérdidas de reputación y financieras, así como ahorrar dinero, al proteger el capital de información contra todos los tipos de riesgos, accidentales o intencionales.

La información es un activo para las organizaciones y bajo esta premisa, la seguridad de la información asume que es necesario protegerla, teniendo como objetivos los siguientes:

- Acceso y uso de los sistemas de información cuando se les requiera, capaces de resistir intrusiones y recuperarse de fallas (disponibilidad).
- Utilización y difusión sólo entre y por aquéllos que tienen derecho de hacerlo (confidencialidad).
- Protección contra modificaciones no autorizadas, errores e inexactitudes (integridad).
- Intercambio de información y transacciones entre organizaciones e individuos confiable (autenticación y no repudio).

Cualquier esfuerzo encaminado a obtener una administración de la seguridad de la información comienza con un fuerte compromiso de la dirección de la organización. Una dirección inteligente comprende que las operaciones y transacciones seguras se traducen en mayor productividad, al evitar pérdidas y reforzar ventajas competitivas. Las orientaciones, políticas y procedimientos de seguridad afectan a toda la organización y, como tal, deben tener el soporte y la participación de los usuarios finales, la dirección, el personal de informática y del área legal. Por lo tanto, las personas que representan a diferentes niveles de toma de decisión deben reunirse a discutir estos problemas para establecer y aprobar las prácticas de seguridad.

La seguridad de la información no es una materia específicamente tecnológica, es de personas y, por tanto, es un problema organizacional de amplio espectro, siempre dinámico.

Todo lo anterior, justifica que dediquemos el presente número de Contaduría Pública a un tema de relevante actualidad e indiscutible trascendencia en la vida de las organizaciones.



Ing. Andrés Velázquez, CISSP, BS7799, CSIRT  
avelazquez@dodomex.com

*Consultor Independiente de Seguridad/  
Examinador Forense Digital*

# Los delitos informáticos y el cómputo forense

*C*ada crimen tiene una escena que puede llegar a ser asegurada para buscar evidencia; pero algunas veces, la evidencia que se tiene que analizar no es una gota de sangre, una huella digital o la fibra de una alfombra. Son los bits y los bytes contenidos en el disco duro de una máquina. En estos casos, los investigadores necesitan tener el conocimiento necesario y la experiencia para obtener evidencia que puede estar dentro de la computadora, pero otras veces se encuentra escondida dentro de la misma.

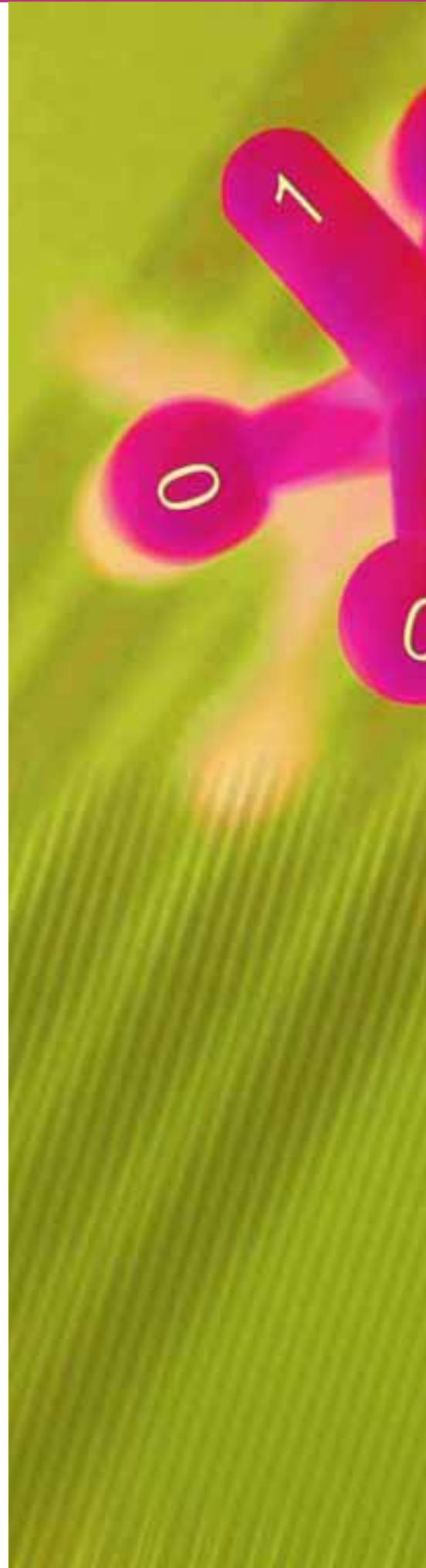
En caso de que el crimen se haya cometido, es necesario hacer la investigación de lo que sucedió con esa computadora, pero si el crimen todavía no se comete, los investigadores deben obtener evidencias para mantener una vigilancia y encontrar al sospechoso.

Pareciera cosa de un programa de investigación de la televisión o el cine; pero ésta es la realidad. Hoy en día, por medio del cómputo forense, se pueden llegar a descifrar muchos delitos informáticos; delitos que son realizados usando la computadora como un medio para cometer el delito o simplemente cuando alguien ataca una computadora para poder sustraer información de ella, algo que

conocemos como robo de secreto de industriales o de información confidencial.

En México se han realizado fraudes por cerca de mil 380 millones de pesos en un año por medio de la internet, según estadísticas de la Policía Federal Preventiva, que cuenta con la Policía Cibernética para seguir delitos principalmente de pornografía infantil y asesorar a la ciudadanía en cuestión de fraudes en la internet.

El cómputo forense es una disciplina que permite identificar, analizar, preservar y presentar evidencia digital obtenida de infraestructura tecnológica, de tal manera que sea válida en un proceso legal, pero muchas veces el proceso se convierte únicamente en interno, ya que muchas



empresas deciden no denunciar al respecto, aunque otras que sí lo hacen.

Esta infraestructura tecnológica puede ser desde un teléfono celular, una cámara digital, una computadora, una impresora, una memoria digital hasta una agenda o un asistente personal (PDA). Todos estos elementos hoy en día tienen memoria, dispositivos que poco a poco se convierten en computadoras; por ejemplo, con un celular ya podemos tomar fotografías y almacenarlas en el mismo teléfono.

Delitos como el secuestro, fraude en portales financieros, fraudes en general, pornografía infantil, narcotráfico y pornografía son hoy por hoy investigados por personas especialistas en el área en todo el mundo. Pero no nada más el cómputo forense se realiza de manera judicial o pericial para presentarlo ante la ley; el cómputo forense también puede ser utilizado como herramienta dentro de las empresas para determinar si alguien está realizando un fraude, ha robado información propietaria o secretos industriales, en pocas palabras, para determinar qué pasó en la computadora o infraestructura de cómputo.

A diferencia de la disciplina forense tradicional, tenemos también una escena del crimen, la cual puede ser una computadora o un archivo. Una de las características principales de la investigación de infraestructura tecnológica es la fragilidad de la evidencia. Por ejemplo, al abrir un archivo de texto, con el simple hecho de darle doble clic a el archivo, se modifica la última fecha de acceso al mismo, por lo tanto, ¿cómo podemos mantener la evidencia sin ningún cambio?

Ésta es una de las partes más difíciles dentro de la investigación, pues con un simple cambio a la evidencia digital, ésta puede ser descartada por el mal manejo que haya tenido el investigador.

Si seguimos con la analogía con un caso normal, el arma dentro de una computadora puede llegar a ser una acción, o un flujo de datos que al llegar a la computadora desaparece y no es posible saber de ella. Por lo mismo, son muchos elementos los que hay que tomar en cuenta para hacer la investigación.

El cómputo forense se divide en cuatro pasos principales:

- Identificación
- Preservación
- Análisis
- Presentación

## **Identificación**

En este paso, es necesario poder identificar lo que tenemos que investigar, desde computadoras, CDROM, memorias e incluso, papeles que pudieran estar cerca de la computadora. Muchas veces en esos papeles podemos encontrar información que puede llegar a servir para completar ciertos procesos de investigación.

En algunos casos, no es necesario ir hasta la escena del crimen, debido a que la misma escena es únicamente la computadora, por lo cual es necesario obtener la computadora.

Si la computadora fue asignada a una persona diferente una vez que se cometió el delito y la otra persona hace uso de

la computadora por un período de tiempo, no es posible regresar o poder hacer la comprobación de que la información contenida en esa máquina fue de esa persona.

Por ello, es muy importante que una vez detectado el fraude o el posible delito, aislar la máquina para que el investigador la pueda obtener sin ninguna alteración.

### Preservación

Es uno de los pasos clave dentro de la investigación. Como lo comentaba anteriormente, es necesario mantener la integridad de la evidencia digital, y para ello usamos varios mecanismos que van desde generar un clon de el disco, llamado Imagen Forense para trabajar sobre él y no sobre la evidencia original. Pero aún así, hay una pregunta clave: ¿cómo podemos asegurar que lo recolectado como evidencia digital es exactamente igual a lo que se analiza y se entrega al finalizar el proceso?

Por medio de una función matemática, podemos generar algo muy parecido a una huella digital de un disco duro. Si un bit (mínima expresión de almacenamiento en medios magnéticos) es alterado, entonces la huella digital del disco duro cambiará.

### Análisis

Una vez que se generó la imagen forense de los medios de almacenamiento, se procede a realizar la investigación, la cual puede llegar a ser tan cansada como el mismo caso. He tenido casos que se resuelven en una semana y otros que se llevan hasta seis u ocho meses de trabajo en un solo caso. Imagine que tiene una computadora normal, con 60 GB (Giga bites) de disco duro, eso es, aproximadamente, haciendo una analogía con papel, como 51 millones y medio de hojas de papel impresas.

En esta etapa, se utilizan diferentes mecanismos y metodologías para obtener evidencia, por ejemplo, si alguna persona guardó un archivo en una memoria externa de USB o si alguien mandó un correo (aunque haya sido borrado).

La recuperación de los archivos borrados de la computadora es un elemento clave dentro de la investigación, ya que normalmente pensamos como usuarios

que borrar o formatear la computadora evitará que los demás accedan a la información. Esto es completamente falso, pues al borrar un archivo simplemente quitamos el índice donde se encontraba, pero el archivo sigue en la computadora y es completamente recuperable. La única manera de no recuperar el archivo es si está sobrescrito ya sea por un proceso o por otro archivo que se alojará en el mismo espacio.

Se puede llegar en algunos casos hasta obtener todas las acciones que el usuario de la máquina ejecutó en los últimos días, por ejemplo, las acciones en la internet, los archivos de sonido, los correos electrónicos, etcétera.

**Una vez detectado el fraude o posible delito, se debe aislar la máquina para obtener la información sin que ésta sea alterada**

### Reporte

Es una de las partes más difíciles que uno se puede llegar a enfrentar como investigador, y esto sucede porque al generar un reporte para explicar qué ocurrió dentro de la computadora, normalmente estos reportes llegan a personas que no conocen de computadoras y por ello hay que realizarlo en un lenguaje coloquial, sin hacer uso de tecnicismos.

Por medio de esta disciplina se han resuelto casos como la identificación y comprobación de personal que está realizando fraudes internos, personas que han atacado a sistemas federales, pedófilos que venden fotografías por medio de la internet, e incluso identificar cuando los bancos son defraudados por medio de la internet.

Una parte fundamental del cómputo forense es establecer la cadena de custodia, un procedimiento para comprobar todo lo que el examinador o investigador ha realizado a la evidencia desde el momento en que identificó la evidencia hasta

su presentación. Esta cadena de custodia permite que si es necesario que otro investigador realice el mismo proceso, debe llegar al mismo resultado.

Pero entonces, ¿por qué no hay mucha información acerca de esta disciplina?

La respuesta es muy sencilla, para realizar esto es necesario tener un marco legal que lo soporte de una mejor manera. En este momento, México cuenta con muy poca legislación al respecto.

En México podemos identificar y aceptar medios electrónicos como pruebas dentro de una denuncia, pero muchas veces la tipificación directa de un delito informático no se encuentra.

Durante un proceso legal, el cómputo forense puede ser utilizado como peritaje para brindar evidencia acerca de acciones que se encontraron dentro de una computadora.

Como ya lo dijimos, quienes van a requerir de esta disciplina van a ser las fuerzas policíacas, los abogados para poder realizar los peritajes de sus clientes, las agencias federales y las empresas. También algo que ha empezado a cambiar dentro del mundo de la tecnología son las aseguradoras, que ya cuentan con seguros para la protección de información o los famosos Seguros contra hackers; por eso, para comprobar que la información fue alterada por un tercero se llega a hacer uso del cómputo forense.

Pero el cómputo forense no sólo se realiza a computadoras como lo dijimos, en México en los últimos años ha venido incrementándose la difamación por medio de correo electrónico, el cual es rastreado por medio de esta disciplina.

El Cómputo forense es una disciplina nueva, muy interesante y que poca gente ha iniciado en ella, pues se requiere conocimiento de diferentes sistemas, un poco de criminalística, técnicas investigativas y legislación. Pero, a diferencia de las demás áreas de la seguridad informática, éste es un proceso totalmente reactivo, ya que se ejecuta cuando algo ha sucedido dentro de la computadora y es necesario volver al pasado por medio de estas técnicas para descifrar lo que ha pasado.

Esperemos que esta disciplina cobre mayor auge en México y que la legislación que requerimos para realizarla se pueda concluir. 



Ivonne V. Muñoz Torres, MCE  
imuñoz@derecho-informático.org

*Abogada, Consultora en temas de derecho y tecnologías de información*

## Aspectos legales y éticos de la seguridad informática

*La seguridad informática, no sólo en México sino en el mundo, es uno de los temas que mayor auge comienza a tener en la actualidad, visto ya sea desde las necesidades de promoverla así como de implementarla.*

Lo anterior atiende a centrar esta disertación en una premisa importante: la seguridad informática no implica en forma única y específica a Internet, la seguridad informática se refiere a todo lo que hace referencia a la preservación, respeto y buen manejo de la información. Para ello, es de vital importancia aclarar que el valor protegido, tanto tangible como intangible, será siempre la información.

Sin embargo, el tema de preservar, respetar y manipular en la forma más correcta a la información, al día de hoy no es un tema fácil de entender, dado que se tiene pensado en el mayor de los casos, que la seguridad informática es un tema que sólo debe aplicarse a casos específicos y no a un todo empresarial, Vg.:

a) La importancia de proteger los archivos electrónicos de un alto ejecutivo en una empresa vs. la falta de importancia de proteger los archivos electrónicos de la persona encargada de llevar el registro de entrada y salida del personal.

b) La constante actualización de programas antivirus en las computadoras personales de los altos ejecutivos en una empresa vs. la ausencia de un programa antivirus en las computadoras personales de las secretarías de dichos ejecutivos.

Ambos ejemplos nos permiten entender la forma en que es visto, en muchos de los casos, el cómo deben ser implementados algunos de los controles en materia de seguridad de la información, ahora veamos las consecuencias de pensar en esta forma:

a) El viernes 20 de febrero una descarga de alto voltaje recae en la empresa, como consecuencia, el procesador y disco duro de la computadora personal del Director de Recursos Humanos sufren daños y por ende pierde su información, sin embargo la consecuencia no es grave dado que su información sí tenía implementado un sistema de respaldo, permitiéndole así no comprometer la integridad y disponibilidad de la misma.

Por otra parte, como consecuencia de la descarga, la computadora del encargado de mantener un registro electrónico del control de entradas y salidas del personal así como de personas externas a la empresa, también sufre daños y la información se pierde. ¿Qué sucederá con el control de asistencias del personal?, ¿cómo determinar quién asistió que días y en qué horario?, en caso de una investigación por robo, ¿en base a qué registro se podrá saber quién accedió a las instalaciones de la empresa?, ¿quién será el responsable ante la ausencia de esta información: el encargado del control o el encargado de sistemas? Más importante aún: ¿a quién despedir por esta negligencia?

b) El lunes 4 de enero a las 9:00 h, un nuevo virus ataca a las computadoras, en esa hora es cuando las secretarías de los altos ejecutivos de una empresa están revisando agendas y ajustando las actividades de la semana laboral. Una de las computadoras de las secretarías es infectada por el nuevo virus, obviamente sin tener conocimiento de que dicho hecho sucede dado que no tiene instalado un antivirus. Al momento de intercambiar información con las demás secretarías y con su propio jefe, ella infecta las computadoras de las otras secretarías y afortunadamente la computadora de su jefe no es afectada. Las consecuencias de ejecutar el virus son fatales dado que empieza a borrar la información así como el acceso a ciertos programas en la computadora, situación que sucede en todas las computadoras de las secretarías de los altos ejecutivos de la empresa. Consecuencia fatal: al inicio de una semana laboral, el área operativa más importante de una empresa es detenida en sus actividades aun cuando la toma de decisiones permanece intacta, sin embargo... ¿cómo pueden ejecutarse las decisiones si el área operativa es inoperable?

De los dos ejemplos anteriores, mismos que reflejan consecuencias mínimas, (existen más graves, como el robo de información, fraudes, revelación de secre-

tos, difamación, etc.), surge la pregunta más utilizada en el tema: ¿quién es el responsable de que sucedan estos hechos?

Para abrir las opciones en esta respuesta, la abordare desde dos puntos de vista: uno será el de los aspectos éticos y el otro de los aspectos legales, no sin antes mencionar que aun cuando separare los puntos de vista, se debe dejar claro que la ética y el derecho son dos temas que siempre van unidos.

### Aspectos éticos

Los medios y el fin, la premisa principal cuando de ética se habla. El fin justifica los medios o los medios justifican el fin, ambas frases son las que salen a relucir cuando estamos frente a un conflicto ético.

Con la intención de no entrar en teorías filosóficas, partamos de una definición objetiva de lo que la palabra ética significa de acuerdo a lo que la Real Academia Española indica:

- Parte de la filosofía que trata de la moral y de las obligaciones del hombre.
- Conjunto de normas morales que rigen la conducta humana.<sup>1</sup>

De ahí que cuando nos enfrentamos a un conflicto ético no es más que cuando uno mismo está en una situación que compromete por una parte a su moral y por la otra a sus obligaciones, es decir, el ser y el deber ser.

Lo que siempre menciono con respecto a este tema, es que indudablemente los valores éticos no son universales, sería imposible asegurar que existe un manual único que enliste cómo debe ser la ética de todos los seres humanos, es por ello que ante las preguntas: ¿quién me dice si soy ético o no? y ¿quién me enseña como ser ético? Existe para la primer pregunta sólo una respuesta: uno mismo; mientras que para la segunda pregunta, la respuesta es que los valores éticos los vamos aprendiendo de nuestro entorno (familia, trabajo y núcleo social) aún así, retornando al *yo*, es uno mismo quien construye su propia ética y por ende, la aplica en forma distinta ante casos específicos.

Para lo que respecta al tema de seguridad informática, el cómo ser ético es definido desde varios aspectos, principalmente por los Códigos de Ética estipulados por Instituciones dedicadas al tema de la Seguridad Informática<sup>2</sup> e incluso

por Autoridades<sup>3</sup> (no gubernamentales, precisamente) dedicadas al tema de las tecnologías de información.

En el tema de Seguridad Informática, el Consorcio para la Certificación Internacional de Seguridad en Sistemas de Información (*ISC2-International Information Systems Security Certification Consortium*) emite una de las más importantes certificaciones en el tema de seguridad informática, conlleva como requisito indispensable el compromiso y conocimiento del Código de Ética establecido por el Consorcio<sup>4</sup>. Dentro de los cánones a seguir, se indica lo siguiente:

- Proteger a la sociedad, a la comunidad y a la infraestructura.
- Actuar en forma honorable, honesta, justa, responsable y legal.
- Proveer servicios diligentes y competitivos a sus superiores.
- Actuar siempre protegiendo y promoviendo el crecimiento de la profesión.

Con respecto a autoridades no gubernamentales que establecen políticas y costumbres en materia de Tecnologías de Información, el Request for Comments 1087: Ética e Internet<sup>5</sup>, generado desde enero de 1989 por DARPA (Defense Advanced Research Projects Agency, *Internet Activities Board*) define, a contrario sensu, lo que se entiende como un comportamiento no ético en internet de la siguiente forma:

- Conseguir accesos no autorizados a los recursos de internet.
- Entorpecer el uso intencionalmente de internet.
- Gasto de recursos en forma innecesaria.
- Destruir la integridad de la información basada en computadoras.
- Comprometer la privacidad de los usuarios.

1 Real Academia Española. <http://www.rae.es/>  
Fuente consultada: 10 de marzo de 2005.

2 ISC2 - International Information Systems Security Certification Consortium <https://www.isc2.org/>

3 Request for Comments Editor <http://www.rfc-editor.org/>

4 Código de Ética de ISC2 <https://www.isc2.org/cgi/content.cgi?category=12>

5 RFC 1087 [http://www.rfc-editor.org/cgi-bin/rfcdoctype.pl?loc=RFC&letsgo=1087&type=ftp&file\\_format=txt](http://www.rfc-editor.org/cgi-bin/rfcdoctype.pl?loc=RFC&letsgo=1087&type=ftp&file_format=txt)



**Aspectos legales**

En lo que respecta al mundo jurídico, es obvio que las personas en ningún momento se encuentran sujetos a normas morales, la situación requiere de un ambiente de obligatoriedad especificada a través de disposiciones y sanciones, es decir: las normas jurídicas.

La relación entre la seguridad informática y el derecho, se ciñe a las preocupaciones existentes en materia de implementación, todas ellas en torno de los siguientes cuestionamientos:

- a) ¿Qué pasa si mis programas de cómputo no tienen una licencia de uso?
- b) ¿Cómo puedo hacer responsable al personal de proteger la integridad de la información?
- c) ¿En qué forma puedo evitar que la información confidencial de la empresa no sea revelada a terceros?
- d) ¿Cómo protejo mis secretos industriales?
- e) ¿Cómo responsabilizo a mi personal cuando le entrego una computadora para que trabaje con ella?
- f) Etcétera.

La situación a resolver con los aspectos legales son sólo dos:

1. Promover una cultura jurídica en materia de TI que en consecuencia impacte en un robustecimiento de las normas jurídicas existentes al día de hoy.
2. Fortalecer la normatividad interna de las empresas con apego siempre a derecho

**Conclusión**

El derecho y la ética, en conjunto, son una herramienta que permite fortalecer la implementación de estrategias de seguridad informática.

- ¿En qué momento interactúa la ética?
- En el momento en que se determina que la seguridad informática es un tema que involucra a todos los miembros de una organización y no sólo a ciertos puestos específicos dentro de la misma. La ética se refleja en la responsabilidad de considerarse parte de un proceso que tiene como fin único el preservar y conservar la integridad y buen

manejo de la información frente al mundo actual lleno de tecnología y, por ende, de riesgos que comprometen a la información.

- ¿En qué momento interactúa el derecho?
- En el momento en que son implementados los procedimientos estipulados en la legislación vigente, ya sea en los procesos como en los marcos normativos internos de las empresas.

- Sabía usted que:

- ¿El daño a la información (vista ésta como un bien mueble) puede ser causa de una rescisión laboral -justificada?
- ¿La revelación de un secreto industrial es un delito?
- ¿El hecho de no contar con licencias en sus programas de cómputo puede afectarle con una multa equivalente a 5,000 días de SMGV<sup>6</sup> o hasta de 10,000 días de SMGV?
- ¿La firma electrónica avanzada le permitirá tener un ambiente legal seguro en sus transacciones realizadas a través de medios electrónicos?

Piense éticamente y actúe legalmente si lo que usted realmente desea es dar soluciones de seguridad informática a su empresa... no se arrepentirá.

- ¿Cuál es el marco jurídico que en materia de seguridad informática existe en México?

A manera de síntesis, en la tabla 1 se resumen las normas jurídicas, entre otras, que en México permiten darle un soporte legal a la implementación y seguimiento de estrategias de seguridad informática. 

**T a b l a 1**

**Implementación y seguimiento de estrategias de seguridad informática en México**

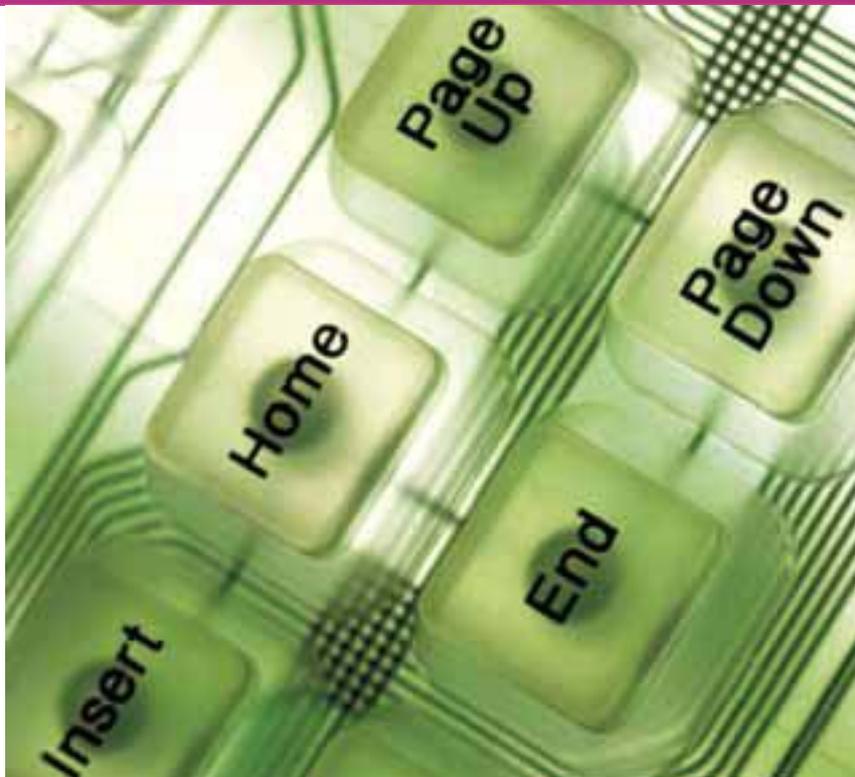
<ul style="list-style-type: none"> <li>• Delitos informáticos</li> <li>• Comercio electrónico</li> <li>• Protección de programas de cómputo</li> <li>• Responsabilidad de personal de TI</li> <li>• Intercepción de comunicaciones</li> <li>• Estándares de Seguridad Física y Lógica</li> <li>• Firma electrónica</li> <li>• Confidencialidad de la información</li> <li>• Secretos industriales</li> </ul>	<ul style="list-style-type: none"> <li>• Código Civil</li> <li>• Código Federal de Procedimientos Civiles</li> <li>• Código de Comercio</li> <li>• Ley Federal de Protección al Consumidor</li> <li>• Reglamento de Prestadores de Servicios de Certificación</li> <li>• Reglas del Reglamento de Prestadores de Servicios de Certificación</li> <li>• NOM 151 SCFI 2002</li> <li>• Código Penal Federal</li> <li>• Códigos penales estatales (D.F., Sinaloa, otros)</li> <li>• Ley Federal del Derecho de Autor</li> <li>• Ley de Seguridad Nacional</li> <li>• Ley Federal contra la Delincuencia Organizada</li> <li>• Ley Federal del Trabajo</li> <li>• Ley Federal de Responsabilidades Administrativas de los Servidores Públicos</li> <li>• Acuerdo que establece las normas que determinan como obligatoria la presentación de las declaraciones de situación patrimonial de los servidores públicos, a través de medios de comunicación electrónica.</li> <li>• Ley de Propiedad Industrial</li> <li>• Ley Federal de Telecomunicaciones</li> <li>• Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental</li> </ul>
--	---

6 SMGV - Salario Mínimo General Vigente



Ángel G. Espinosa Sarmiento  
CISSP, CISM  
correo@alapsi.org

Asociación  
Latinoamericana  
de Profesionales en  
Seguridad  
Informática, A.C.



# Las certificaciones en seguridad

*Las certificaciones en seguridad han ido ganando terreno en el ámbito de la profesionalización de individuos dedicados a esta actividad, al margen de resultar ser un atractivo natural de interacción con beneficios para las cuatro figuras que*

participan en el ambiente: los certificados, los autores o creadores de certificaciones, los promotores de certificación o instancias certificadoras y quienes invierten desde tiempo, dinero y/o esfuerzo individual o de grupo para generar primero intangibles como la satisfacción individual o la reputación de asociaciones y, posteriormente, tangibles de recuperación para el mantenimiento de las certificaciones o creando nuevas.

Surgen como un mecanismo de autenticación del conocimiento de los profesionales, con el cual busca primero identificar al individuo por su nombre y luego verificar dicho nombre contra la lista de personas que han demostrado ante un tercero que tienen y mantienen un nivel demostrable de dominio en seguridad.

## **Certificados, certificaciones y certificadoras en seguridad**

En orden enunciativo, la primera figura son los certificados, aquellos individuos interesados en generar y enviar a un tercero (instancia certificadora) la evidencia requerida para cumplir con lo establecido por

un criterio generalmente aceptado. Tal evidencia está conformada, entre otros, por comprobantes o constancias de experiencia y de conocimientos afines a la certificación de seguridad; por ejemplo, examen de certificación aprobado, grado académico, trabajos realizados en organizaciones o de manera independiente, descripción del rol y los entregables generados en esos proyectos y así como su participación en grupos o asociaciones legalmente establecidos y reconocidos que promueven la seguridad.

En este mismo orden de ideas, la siguiente figura está conformada por los autores o creadores de certificaciones, los cuales son grupos organizados de individuos que vigilan el cabal cumplimiento de las políticas y los procedimientos que soportan a uno o varios programas de certificación, desde su concepción, diseño, promoción, aplicación, valuación y generación del resultado, es decir, un documento llamado certificado.

La figura en turno es la integrada por las instancias certificadoras que en origen nacen de manera autónoma y con la misión de certificar individuos. El proceso de certificación implica generar las preguntas del examen y calificarlo. La actividad de calificar los reactivos se “outsources” a un tercero para no ser juez al definir el examen de certificación y parte al calificarlo. Con el tiempo, estas instancias certificadoras adoptan un segundo rol, el de promotores de sus respectivas certificaciones.

## **¿Quién o qué se puede certificar en seguridad?**

Una certificación en seguridad implica que lo que o quien la ostenta, ya sea gente, proceso o tecnología, debió cumplir con un conjunto de requisitos establecidos

como mínimos durante su existir y que tienen que ver con haber sido calificadas las dimensiones de conocimiento para gente (e.g. *Certified Information Systems Security Professional* de [www.isc2.org](http://www.isc2.org)), de información para procesos (e.g. *Information Security Management System* de la [www.european-accreditation.org](http://www.european-accreditation.org)) y la relación rendimiento-calidad para tecnología de Seguridad (e.g. [www.common-criteriportal.org](http://www.common-criteriportal.org)).

Dado el alcance del presente artículo trataremos sólo la certificación de individuos, dejando para futura ocasión lo referente a las certificaciones en seguridad para procesos y tecnologías de seguridad.

**¿Certificarse o no certificarse? Paradigma**

Existen comunidades en el medio que profesan y ejercen la respetable práctica de evitar algún tipo de certificación con el argumento de que la validación de sus conocimientos por un tercero no es necesaria, se les tiene que creer. Podemos afirmar, entonces, que tenemos a la vista dos paradigmas: el de la no certificación y el de la certificación.

Para el primero y siendo específico me referiré a la privilegiada experiencia con algunos colegas de seguridad integrantes de respetables comunidades como el G-CON ([www.g-con.org](http://www.g-con.org)), quienes, y para tener una idea más clara, asisten anualmente a un centro de reunión y de intercambio de tecnología en México en lo que toca a seguridad informática: es una conferencia por excelencia para consultores de seguridad, hackers y personas en general interesadas por técnicas de explotación, irrupción y rompimiento de seguridad (sic).

Por un lado, resulta un hecho que los integrantes de estas comunidades tienen una notable capacidad y conocimiento en seguridad de la información; por el otro, resulta también totalmente comprensible que algunos opten por no certificarse, lo cual no significa que esté bien o mal, simplemente esto invita a respetar dicha decisión.

Al calce del paradigma de la no certificación, la profesión de seguridad al igual que otras de orden crítico para una organización o individuo, requiere de garantizar al máximo sus resultados. Di-

fícilmente un paciente que se diga gozar de sus facultades dejaría operarse algún órgano vital, por ejemplo, el corazón, por un especialista sin certificación u otro aval equivalente que dé fe y genere en el cliente la confianza de que posee el conocimiento adecuado. Por lo tanto, es claro que el efecto positivo inmediato se da como resultado de obtener y mantener una certificación, pues esta acción tiene una influencia directa en la mitigación de riesgos asociados al quehacer de un profesional en seguridad, el cual responsable de proteger los objetos de información críticos que garantizan la continuidad de las operaciones de un negocio, organización o institución.

En cuanto al paradigma de la certificación en seguridad, éste se ve sustentado en los conceptos de *due-care* (debido cuidado) y de *due dilligence* (debida diligencia). Es decir, cuando el profesional en seguridad obtiene una certificación en seguridad, entonces el debido cuidado estará cubierto. Ciertamente una certificación implica un reto e inversión de tiempo, esfuerzo y dinero para demostrar y obtener de un tercero el aval que le respalde su nivel de dominio de los conceptos en seguridad; sin embargo, sólo se tendrá cumplimiento con la debida diligencia en el momento en que se obtenga y mantenga la recertificación.

**Certificaciones y requerimientos legales**

Como tendencia sustentada por requerimientos legales como el acta *Sarbanes-Oxley* (2002) en Estados Unidos (con alcance implícito para el continente Americano) y su similar en Europa, el *Turnbull Report* (1990), las certificaciones en seguridad tienen un rol cada día más importante en el proceso de selección y reclutamiento de individuos para la protección de los activos (objetos) de información y activos físicos de las organizaciones a escala mundial.

**Tipos de certificaciones en seguridad**

Existe una gran variedad de certificados y para cada uno bien pudiera generarse su correspondiente certificado de especialidad, o lo que se le conoce como un programa de seguridad (conjunto de

certificaciones afines). Resulta notable comentar que para cada certificación en seguridad existe un cuerpo común de conocimientos el cual está integrado por grupos de tópicos o dominios.

Con más de 55 certificaciones en seguridad vendor-neutrales, las más demandadas y reconocidas a nivel mundial son CISSP ([www.isc2](http://www.isc2)), SANS GIAC ([www.sans.org](http://www.sans.org)) y CPP ([www.asisonline.org](http://www.asisonline.org)). Se le considera a SANS GIAC como la pionera en la creación de programas de certificaciones dado que cuenta con una gran variedad y están relacionadas entre sí a manera de carrera.

En un primer nivel básico se puede citar a las certificaciones del CompTIA Security+ ([www.comptia.org](http://www.comptia.org)), SANS GSEC (GIAC-*Security Essentials Certification*) y la (ISC)2's SSCP (*Systems Security Certified Professional* - [www.isc2.org](http://www.isc2.org)). En un siguiente grado se pueden ubicar al resto de las certificaciones del SANS-GIAC y las certificaciones CISSP y CISM, las cuales son consideradas como credenciales intermedias y de nivel Senior respectivamente,

## Las certificaciones en seguridad seguirán rigiendo la demanda de profesionales en el mercado formal de estos servicios

mientras que las certificaciones de la ASIS Internacional ([www.asisonline.org](http://www.asisonline.org)) CPP (*Certified Protection Professional*), el PCI (*Professional Certified Investigator*) y PSP (*Physical Security Professional*) restringen su acceso a solo individuos *Most-Senior* de la comunidad de la seguridad, simplemente porque requieren cinco a nueve años de experiencia profesional en el campo de seguridad.

Lo anterior nos permite afirmar que las certificaciones en seguridad seguirán rigiendo la demanda de profesionales en

el mercado formal de estos servicios y más aún seguirán surgiendo nuevas certificaciones en un afán bivalente: mercadotecnia y acreditación de individuos. Desde el punto de vista de mercadotecnia para sus creadores al diversificar los actuales productos (certificaciones) generando nuevas o basadas en las certificaciones actuales y por el otro a partir de las actuales certificaciones generalistas crear programas que acrediten a los individuos que logren demostrar una especialización. Todo lo anterior, sustentado por el marco regulatorio que invita a las organizaciones a ver la Seguridad como un aspecto de negocio mandatorio.

### Nota:

Ninguna opinión expresada por Ángel Gonzalo Espinosa Sarmiento dentro de este artículo refleja necesariamente el punto de vista de la Asociación Latinoamericana de Profesionales en Seguridad Informática, A.C., o de alguna otra organización o institución con la que el autor ha mantenido o mantiene una relación de trabajo. 



Mtra. María Teresa Pérez Morales  
mterep@yahoo.com

*Profesora de Maestría y  
Licenciatura en la  
Universidad Regiomontana*

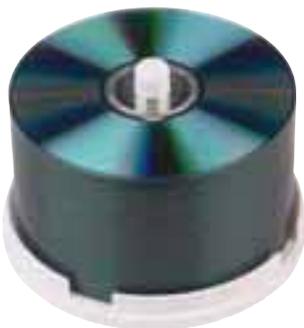
# Amenazas humanas y métodos más comunes para acceder a los recursos computacionales

*Desde que se utilizaron las primeras computadoras comerciales hasta nuestros días, los avances relacionados a la tecnología de la información han sido muy rápidos, esto ha traído consigo una serie de riesgos y vulnerabilidades en todo el ámbito computacional.*

Posiblemente lo más importante que los ejecutivos de las empresas deben comprender hoy en día, es que no es la era industrial sino la era de la información y del conocimiento. Por lo tanto, la información juega un papel crucial para la mayoría de las empresas, ya que es procesada a través de medios electrónicos y se debe estar consciente del valor de la información que se genera a través de los sistemas computacionales. Por lo anterior, es indispensable contar con un esquema de seguridad computacional óptimo para contrarrestar los métodos más comunes de acceso a los recursos computacionales.

Una débil arquitectura de seguridad computacional o un mal diseño de ésta, crea tremendos retos para los accionistas, directores de empresas, gerentes y los profesionales que están involucrados en las Tecnologías de Información (TI) y los Procesos de Negocio (PN), debido a que si se llega a materializar un método (ataque) a sus recursos computacionales, esto puede afectar a su imagen y ocasionar una pérdida financiera.

**Es indispensable  
contar con un  
esquema de seguridad  
computacional para  
contrarrestar  
los métodos más  
comunes de acceso  
a los recursos  
computacionales**



## Qué se entiende por seguridad lógica computacional

**Seguridad lógica computacional.** Puede definirse como la “aplicación de barreras y procedimientos que resguarden el acceso a los recursos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo”.

Pero también es una protección contra el comportamiento inesperado,<sup>1</sup> ya que previene que los atacantes logren su propósito a través de accesos no autorizados o la utilización de los recursos computacionales sin autorización.<sup>2</sup>

La seguridad lógica computacional es el proceso de prevenir y detectar el uso no autorizado de los recursos computacionales. Las medidas de prevención ayudan a detener a los usuarios no autorizados (también conocidos como intrusos) para acceder cualquier área no autorizada. La detección ayuda a determinar si han intentado ingresar a los sistemas, si tuvieron éxito y que es lo que pudieron haber hecho.

La seguridad lógica computacional puede entenderse como el conjunto de medidas que defina la organización o el responsable de seguridad para que sus recursos computacionales queden protegidos y así minimizar el riesgo de que personas internas o externas puedan afectarlos.

## Historia

El siglo XX se considera como la era de la computación, ya que en el año de 1939 se inventa la primera computadora. Desde el invento de la primera computadora hasta nuestros días éstas son menos caras, con mayor almacenamiento, más compactas y pueden generar rápidamente un sin número de operaciones. A continuación se describe la evolución de las computadoras, en cuanto a su tamaño, nivel de procesamiento y almacenamiento y los nombres de algunos científicos que contribuyeron a su avance.

En el año de 1939, los profesores John Atanasoff y Clifford Berry, de la Iowa State University, construyen lo que pudo haber sido la primera computadora electrónica digital, pero nunca la Universidad se preocupó de patentarla. En el mismo año, el ingeniero Alemán Konrad Zuse termina la primera computadora digital programable y su uso era de propósito general. Su función principal fue realizar cálculos de ingeniería. Comenta el Ingeniero: “me daba pereza hacer cálculos, por eso invente la computadora”. Pidió apoyo al gobierno alemán, y se le negó. El objetivo de su construcción fue que los estudiantes de postgrado resolvieran largas

y complejas ecuaciones diferenciales. (Beekman George, 1994).

En el mismo lapso el científico John Mauchly formó equipo con J. Presper Eckert para la construcción de una computadora, que calculara las trayectorias para los nuevos cañones que producían los Estados Unidos -Segunda Guerra Mundial- el resultado fue la computadora ENIAC (*Electronic Numerical Integrated and Computer*); su peso era de 30 toneladas, contaba con 18,000 tubos de vacío y presentaba una avería cada siete minutos. Cabe mencionar que el objetivo por el cual fue ensamblada fracasó debido que se terminó dos meses después de que finalizó la guerra. Después de la guerra Mauchly y Eckert pusieron en marcha una compañía privada y crearon el UNIVAC 1, la primera computadora comercial de propósito general. (Beekman George, 1994.)

En 1944, el profesor Howard Aiken, de la Universidad de Harvard, ensambla la computadora Mark I. La computadora fue para propósito general; su tamaño era de 15 metros de largo por dos y medio de altura; usaba ruidosos relevadores electromecánicos para efectuar cálculos cinco o seis veces más rápidamente que un ser humano. Para este proyecto la empresa International Business Machines Corporation (IBM), lo apoyó con un millón de dólares. (Beekman George, 1994.)

En 1951, la oficina de censos de Estados Unidos compró y empezó a usar la UNIVAC 1. La características de esta máquina es que era muy grande, costosa y de difícil operación; usaba tubos de vacío (tubos de vidrio del tamaño de un foco que albergaban circuitos electrónicos) que también servían para capturar y realizar operaciones estadísticas y realizaban 100,000 sumas por segundo. Las computadoras que usaban tubos

de vacío se les catalogó como computadoras de la primera generación. (Beekman George, 1994.)

En 1956, fue utilizado el primer transistor pero éste había sido inventado en el año de 1948. Descubrieron que podía desempeñar la misma función que un tubo de vacío, pues transfería la electricidad a través de una pequeña resistencia. Las computadoras que usaban transistores eran más pequeñas, confiables y económicas. (Beekman George, 1994.) Asimismo, con el avance del hardware también fue evolucionando el *software*. El resultado fue que las empresas y las universidades se interesaron en la compra de computadoras. A las computadoras que usaban transistores se les clasificó como computadoras de segunda generación.

A mediados de la década de 1960, los investigadores desarrollaron una nueva tecnología que permitió empaquetar cintos de transistores en un circuito integrado, como resultado se inventó el chip de silicio. Con este invento las com-

**Las computadoras  
que usaban tubos  
de vacío se les  
catalogó como  
computadoras  
de la primera generación**

1 Simon Garfinkel y Gene Spafford, Riesgos Tecnológicos y Estratégicos, Seguridad y Comercio en la Web, Mc Graw Hill, O. Rely, junio, 1999, p. 9.

2 [webdia.cem.itesm.mx/dia/ac/rogomez](http://webdia.cem.itesm.mx/dia/ac/rogomez)



organizaciones y son conocidas como: *hackers*, *crackcers*, *scripters*, *phone prackers*, terrorismo y espionaje informático, entre otros, y que se dedican, especialmente, a alterar los recursos computacionales. A continuación se describen cada tipo de persona.

### Usuarios autorizados

Este tipo de personas es probable que tengan alguna meta u objetivo específico, pues tienen acceso legítimo a los recursos computacionales y pueden insertar virus, gusanos, *trojan horse* o monitorear a través del sistema operativo y pueden dañar con o sin intención. Estos tipos de ataques pueden ser extremadamente difíciles de detectar y proteger y además muy costosos.

### Empleados disgustados

Son una amenaza mayor. El ataque puede afectar a todos los recursos computacionales. Los empleados disgustados exploran los errores del sistema operativo o las debilidades de cualquier recurso computacional para hacer que éstos fallen o utilizan otros métodos más poderosos para destruir.

### Hackers

Los hackers son gente que goza del desafío rompiendo recursos computacionales. El término hacker ha cambiado en los últimos años, ahora se utiliza para referir a la gente que rompe los esquemas de seguridad en los sistemas informáticos sin tener autoridad. Pueden transmitir virus, robar información, robar voz, dañar bases de datos, entre otros ataques y esto lo hacen algunas veces como diversión.

### Crakers

Aquella persona que en forma persistente realiza intentos hasta obtener acceso a los recursos computacionales, una vez logrado el acceso produce daños no necesariamente tiene el mismo nivel de conocimientos que el hacker. Todos los hackers son crakers en potencia pero un craker hace lo mismo que un hacker, con una salvedad: el craker no lo hace de forma altruista ni por amor al arte. Los crakers suelen tener ideales políticos o filosóficos, suelen estar movidos por su arrogancia, orgullo, egoísmo, necesidad de darse a conocer o simplemente ambición o avaricia. Un cracker cumple igual que un hacker, pero una vez que accede al sistema no se da por satisfecho, sino que daña los recursos computacionales. Las hazañas típicas son la copia de información confidencial, movimientos de pequeñas sumas de dinero y compras a nombre de otros, etcétera.

### Scripters

Son personas con la capacidad de buscar un programa en la red y ejecutarlo. No hay una meta fija, solamente tienen la necesidad de pertenencia aunque sea sólo por dañar. No hay preocupación por las consecuencias reales de sus actos.

### Phone pracker

Los phone pracker es una rama específica de los hackers y su principal interés está en los sistemas telefónicos. Un pracker es alguien que exhibe la mayoría de las características de un hacker. Un praker talentoso es una amenaza no solamente para los sistemas telefónicos sino también puede tener acceso a los servidores y borrar archivos, entre otros daños.

### Terrorismo informático

Es una forma violenta o pacífica de lograr accesos a los recursos computacionales mediante la cual se persigue la destrucción del orden establecido o la creación de un clima de temor e inseguridad. El terrorismo informático es una manera de hacer daño común a la sociedad actual.

Es uno de los métodos más usados tanto por personal interno como externo para atacar los recursos computacionales.

Las personas internas y externas pueden tener un sinnúmero de métodos para atacar los recursos computacionales. Algunos de los métodos más usados se definen a continuación.

### Virus

Un virus infecta programas en existencia insertando código nuevo su función es reproducirse, pueden también introducir datos que destruyen.

### Trojan horse

Es un programa que puede realizar una función útil, pero también puede tener una acción inesperada es una forma de virus; es decir, es un programa malévolo que se esconde dentro de un programa amistoso o simula la identidad de un programa con características legítimas, mientras que realmente causa daño en los sistemas. Este método puede ser particularmente difícil de detectar, pues aparentan ser programas legítimos y útiles pero en realidad no lo son.

### Bomba

Una bomba se puede definir como un programa al que se le inserta una línea de código con ciertas características y puede afectar a un evento importante o específico. Ejemplo, hacer un programa para borrar todas las facturas del cliente núm. 55555 y ejecutarlo el día 12/12/2012 a las 12:00. Es una bomba de tiempo y se ejecuta en un tiempo especificado.



## Trap door

La trap door le permite a un usuario tener acceso a sistemas funcionando y que éstos le han sido autorizados. Estos privilegios de acceso se pueden obtener con una condición del teclado *start-up* abortando el sistema. Una vez que la computadora obtenga el acceso, el usuario puede manipular, cambiar, adicionar o destruir datos de otros usuarios.

## Gusano

Un gusano se diferencia de un virus porque se reproduce por sí mismo; es decir, no requiere un programa anfitrión. Las características incluyen la réplica y un programa autónomo que cuando se activa crea el proceso. Cabe mencionar que la réplica de los gusanos ocurre con más frecuencia al recibir mensajes a través de la red. Un gusano es similar a un virus, excepto que puede ser propagado e infectar archivos sobre la red. Los gusanos no necesitan ser adjuntados a otros programas para ser propagados; una vez que un gusano es ejecutado, éste puede ser propagado rápidamente y algunas veces infecta a millones de computadoras alrededor del mundo, lo cual sucede en minutos u horas.

## web defacing

Se entra ilegalmente en los servidores (*host*) de las organizaciones y se pueden cambiar los contenidos de las páginas que están en la web.

## Negación del servicio (*Denial of service*)

Los ataques de negación de servicio requieren generalmente del poder de una red de computadoras que trabajen simultáneamente, hacen que se deshabiliten o desconecten de la red y logran que los servicios no estén disponibles. Estos ataques pueden destruir los servicios del servidor dejando de operar o pueden interrumpir sistemas críticos. Un ataque de negación de servicio ocurre cuando los recursos de la red son tomados por un individuo no autorizado, típicamente el ataque es realizado a los servidores. Esta acción aumenta significativamente el tráfico en la red abrumando los servidores y haciéndolos imposibles para que los usuarios legítimos introduzcan o lean información.

Los ataques más frecuentes son los del ruteo a las tablas, esencialmente el blanco, obteniendo direcciones de datos y cambiándolos de una a otra computadora. Este tipo de ataque modifica las tablas de ruteo enviando todos los datos a otras direcciones en la red. Aunque estos ataques apagan los servidores, no afectan los datos de la víctima, pero pueden ser extremadamente costosos.

## Data diddling

Esto implica cambiar los datos antes de la captura, durante el proceso o la salida de datos. El cambio puede realizarse por cualquier persona que tenga acceso a la información, pues puede adicionar, modificar, borrar o actualizar datos. Algunos ejemplos son: forzar documentos a la falsificación, cambio de soportes magnéticos (cintas, cartuchos, discos etc.), por los reemplazos preparados, violaciones a la infor-

mación del documento fuente, entre otros. La manipulación en la entrada, proceso y salida de datos es el método más común para perpetrar fraudes.

## Técnica del salami

Este método se presenta cuando se roban pequeñas cantidades de dinero; el robo puede ser realizado de diferentes maneras; por ejemplo, robar algunos centavos de cada cuenta de cliente y ser depositada a una cuenta personal. La mayoría de las veces pasa inadvertida por los clientes debido a que los totales de la cuenta son mantenidos en balance. La técnica del salami puede también ser realizada por el método de redondeo *round-down* y estas cantidades son movidas a las cuentas de los perpetradores.

## Superzapping

Uso no autorizado de programas utilitarios para modificar, destruir, copiar, divulgar, insertar, utilizar o negar datos. Un programa utilitario poderoso puede violar controles de seguridad tanto del sistema operativo como del control de accesos.

## Ataques asincrónicos

Son ataques indirectos contra programas alterando datos legítimos o códigos de los programas, este ataque se realiza en el momento que los programas están ociosos.

## Piggybacking

Es un método para acceder a áreas de acceso controladas; puede ocurrir en sistemas en línea donde se están utilizando terminales y la identificación es verificada automáticamente por el sistema, cuando se activa una terminal la computadora autoriza el acceso, generalmente con base en una identificación del usuario y una clave de acceso. La violación puede ocurrir cuando una terminal oculta está conectada en la misma línea a través del equipo telefónico y se activa cuando el usuario legítimo no está utilizando su terminal, la computadora no podrá distinguir o reconocer los dos terminales, pero detecta solamente un terminal y a un usuario autorizado.

## Impersonalización

Es el proceso donde una persona asume la identidad de otra. El acceso físico o electrónico a las terminales se requiere de la identificación de un usuario, la verificación se basa en una cierta combinación, algo que el usuario sabe (ejemplo: una claves de acceso secreto), o algo que el usuario es (una característica fisiológica, tal como huella digital, geometría de la mano o la voz) y algo que el usuario posee, (ejemplo, una llave magnética, una tarjeta), etcétera. Cualquier persona con la combinación correcta de las características de la identificación puede personificar a otro individuo.

## Wiretapping

Escuchar o interceptar una conversación vía telefónica durante la transmisión de mensajes o voz. También ocurre cuando los flujos de datos que pasan por los diferentes medios de transmisión son interceptados.

### Spooftng

Es un método que atrapa las identificaciones de usuarios autorizados y contraseñas correspondientes y los almacena en un archivo, el archivo lo envían a las computadoras de los perpetradores y así se consigue el acceso.

### Scavenging/browsing

Método para obtener información y puede ser leída alrededor de un sistema informático o después de la ejecución del trabajo. Incluye la búsqueda física o electrónica de información. Por ejemplo, el barrido físico busca copias de papel carbón en la basura de los sistemas en operación que sean útiles, el barrido electrónico busca datos residuales en programas en memoria y en soportes magnéticos después que se ejecuta del trabajo.

### Ingeniería social

Se refiere a la capacidad que tiene una persona de utilizar otra personalidad y hace uso de sus conocimientos y habilidades sociales para robar la información que está relacionada con los recursos computacionales tal como; llaves físicas o electrónicas, códigos, tarjetas de acceso, llamadas o

dar contraseñas a otras personas. Implica forzar a usuarios o administradores que usan los recursos computacionales de proporcionar información.

### Conclusión

Una empresa puede tener un staff de gente de primera, pero si tiene sistemas computacionales sin medidas de seguridad lógica computacional mínimas, y si voluntaria o involuntariamente sufre un ataque a sus recursos computacionales, esto le puede ocasionar pérdida de imagen, dinero, clientes y hasta llegar a la ruina financiera. A la empresa le constaría más trabajo salir adelante o quedarse hundida.

En la actualidad, más y más organizaciones están pasando de una manera tradicional de hacer negocio a una manera vía *world wide web* (www), colocando sus negocios en un mundo de e-Business, e-Commerce y e-Movil. Esto trae consigo que los perímetros de seguridad lógica computacional amplíen, actualicen o cambien para que se logre proteger los recursos computacionales, los responsables de la seguridad deben estar a la vanguardia en cómo están emigrando los nuevos métodos de ataque y por consecuencia buscar modelos de seguridad lógica computacional que se adapten a éstos. 



Dr. Roberto Gómez Cárdenas  
rogomez@itesm.mx

*Profesor Investigador  
Instituto Tecnológico de  
Estudios Superiores de  
Monterrey, Campus Estado de  
México*

# Criptología y la seguridad en internet

*La internet surge en EE.UU., como una necesidad de interconectar diferentes redes de computadoras diseminadas en todo el territorio estadounidense. Lo importante era asegurar la conexión entre las computadoras, sin interesar la seguridad de estas conexiones.*

A medida que la internet fue ganando terreno en el área comercial y en los hogares, se empezó a dar importancia a la seguridad de la información que circulaba por ésta. El gusano de Morris de 1988 puso en evidencia lo vulnerable que estaba la red en sí y no sólo la información que circulaba en ella. Es importante recordar que la internet de 1988, no era la misma que conocemos hoy en día. El correo electrónico no contaba con las interfaces de actuales y no todo mundo tenía acceso a ella. Por otro lado, no era común el contar con una computadora en casa, la web aún no surgía y el *chat* no era otra cosa que un programa llamado *talk*, que permitía a dos personas comunicarse a través de una terminal virtual.

La seguridad informática se define como el conjunto de políticas y mecanismos que nos permiten garantizar la confidencialidad, la integridad y la disponibilidad de los recursos de un sistema. En este caso los recursos a proteger es la información que circula por internet

y los nodos (computadoras, ruteadores, *switches* y otros dispositivos) que la componen. Una de las herramientas utilizada para cumplir con este objetivo es la criptología.

La criptología es la ciencia que estudia los aspectos y contenidos de información en condiciones de secrecía. Se divide en criptografía y criptoanálisis. La criptografía se encarga de transformar la información de tal forma que sólo las partes involucradas en la comunicación entiendan el contenido. Por otro lado, el criptoanálisis abarca las diferentes metodologías y técnicas que permiten recuperar la información que ha sido previamente tratada por un procedimiento criptográfico, sin conocer a priori la técnica utilizada.

Un criptosistema es el algoritmo o método utilizado para encriptar y/o decriptar un mensaje. Todos los criptosistemas computacionales se basan en el concepto de llave. Dependiendo del tipo de llave usada, los criptosistemas se dividen en simétricos y asimétricos.



Los criptosistemas simétricos son aquellos en que la llave de encriptación es la misma que la de decriptación. Consideremos dos usuarios, Alicia y Beto, que desean intercambiar información de forma segura. Alicia encripta el mensaje a enviar usando una llave que comparte con Beto y se lo envía. Cuando Beto recibe el mensaje lo decripta con la misma llave que Alicia usó para encriptarlo. La desventaja de este tipo de criptosistemas es que Alicia y Beto deben ponerse de acuerdo en la llave. Lo anterior no representa problema alguno si los dos trabajan en la misma oficina, pero no es lo mismo si los dos residen en países diferentes y sólo se pueden comunicar por internet. Ejemplos de este tipo de criptosistemas son DES y su variante Triple DES, AES, IDEA, *Blowfish*, *Twofish* y otros.

El problema anterior dio origen a la criptografía asimétrica, cuya característica principal es que llave de encriptación es diferente a la de decriptación. Una persona cuenta con dos llaves: una pública, conocida por todo el mundo y una privada que solo debe conocer el usuario. Tomando el ejemplo anterior, Alicia encripta el mensaje con la llave pública de Beto y se lo envía. Una vez que el mensaje es recibido, Beto lo decripta con su llave privada. Las llaves están relacionadas de tal forma que no es posible decriptar un mensaje encriptado con una llave pública usando esta misma llave. Sólo la persona que posea la llave privada puede decriptar el mensaje. Los tres principales criptosistemas asimétricos son RSA, El Gamal y Rabin.

Los objetivos de la criptografía son dos: por un lado, mantener la confidencialidad del mensaje y garantizar la autenticidad tanto del mensaje como del par remitente/destinatario. El primer objetivo implica que la información contenida en el mensaje permanezca secreta. El segundo objetivo asegura que el mensaje no sufrió modificación alguna durante su transmisión y que remitente y destinatario son quienes dicen ser y no remitentes y/o destinatarios fraudulentos.

Una internet segura requiere, entre otras cosas, cumplir con los dos objetivos anteriores, a través de protocolos criptográficos. Este tipo de protocolos están designados para llevar a cabo una tarea específica usando como herramienta algún algoritmo

criptográfico. Existe una amplia variedad de protocolos criptográficos que dan respuesta a diferentes objetivos. Se pueden agrupar en dos grandes familias, los que definen las Redes Virtuales Privadas (VPN, por sus siglas en inglés) y los que proporcionan un medio de autenticación para un usuario con respecto a un servidor.

### Las redes privadas virtuales

Si la compañía ACME se desea comunicar en secreto con la compañía BACARA tiene dos opciones. La primera de ellas consiste en tender un cable de comunicación entre las dos compañías, lo cual puede llegar a tener un costo considerable. La segunda opción es utilizar la infraestructura pública de comunicación, pero manipulando la información que circula por ella de tal forma que sólo las dos compañías puedan interpretar los datos que circulan por ella. Esta última opción es el principio de funcionamiento de las Redes Privadas Virtuales (VPN, por sus siglas en inglés).

Una VPN tiene por misión asegurar un canal público de comunicación encriptando toda la información que circule por ella y autenticando a las partes involucradas. La comunicación se puede asegurar a diferentes capas. A nivel de capa aplicación los programas trabajan de *host a host* y sólo se protege el *payload* del paquete y no el paquete. Ejemplos de software usado para este propósito son PGP o SSH. A nivel de capa transporte el contenido de la comunicación es protegido, pero no así los paquetes. Un ejemplo de este tipo de protocolos es SSL. La capa red es protegida por el protocolo IPsec el cual no sólo encripta el payload sino que puede encriptar el encabezado TCP/IP del paquete.

PGP, *Pretty Good Privacy*, es un software cuyo objetivo primario era poner a la disposición del público lo mejor de la criptografía académica para proporcionarles privacidad en sus comunicaciones. Hoy en día es una herramienta usada para encriptar y firmar información enviada por correo electrónico. El software se puede obtener de [www.pgpi.org](http://www.pgpi.org) y proporciona encriptación, firma de correo y borrado seguro.

SSH, *Secure SHell*, es una opción para contar con una conexión segura entre un

host y un servidor. La conexión es encriptada y no corremos el riesgo de que alguien capture el *password* con un sniffer. Es un buen sustituto para telnet, ftp y los comandos r. El software del cliente es libre y se puede obtener en internet. Sin embargo, la versión del servidor es comercial, pero existe una versión libre para Linux: *OpenSSH*.

El protocolo por excelencia usado para proteger la transmisión de información entre servidores web y los browsers de los clientes es SSL (*Secure Sockets Layer*). Este protocolo es el que se usa cuando un usuario accede a una página web con el objetivo de adquirir un producto. La parte del cliente es completamente transparente para el usuario, y no es necesario que el usuario instale software alguno. Toda la lógica de la aplicación (i.e. cuando es necesario encriptar, cuándo no y con qué protocolo) se lleva a cabo en el servidor. Es el desarrollador de la página web el que debe hacer lo necesario para encriptar la información en el momento necesario.

La actualización del protocolo de internet IPv4 a IPv6 se enfocó principalmente a tres aspectos: contar con más direcciones IP, incorporar QoS al protocolo y el proporcionar mecanismos para asegurar la comunicación. La gente de internet decidió que no había que esperar que IPv6 estuviera adoptado por todos los dispositivos para usar los mecanismos de seguridad. Se tomó la parte de seguridad de IPv6 y se integró en un protocolo conocido como IPsec. Este protocolo permite asegurar la comunicación a nivel paquete, pudiendo encriptar y/o autenticar la información que viaja en el payload o en el encabezado de los paquetes. Se cuenta con tres protocolos, IKE que permite un intercambio de llaves entre las partes, ESP permite encriptar la información del paquete y AH es el encargado de autenticar, sin encriptar, la información dentro del paquete. IPsec cuenta con dos modos de funcionamiento, si lo que se desea asegurar es el payload del paquete se usa el modo transporte; por otro lado el modo túnel permite asegurar los datos del encabezado del paquete. Este protocolo no es simple de instalar como los anteriores, ya que es necesario modificar el núcleo del sistema operativo donde se vaya a usar. Es forzoso intervenir la máquina del cliente y servidor para que se pueda usar.

Se cuenta con varias opciones para asegurar un canal de comunicación. No existe una única opción y todas proporcionan autenticación, firma y encriptación de la información. Asimismo, es posible usar más de un protocolo para proporcionar mayor seguridad. Es decir, es posible encriptar un enlace con IPsec y después usar SSH, SSL o PGP para conectarse a un servidor, acceder a una página web o enviar un correo. Tan sólo hay que recordar que la principal desventaja de las VPN es el desempeño, ya que es necesario encriptar/decriptar toda la información que entra y sale a un host; la velocidad de transmisión se puede ver afectada.

### La autenticación de usuarios en internet

Se define como autenticación al hecho de que una computadora verifique que un usuario es quien dice ser. El mecanismo de autenticación más usado es el de *password*. El usuario le proporciona a la computadora su identidad y el *password* asociado a éste. La máquina verifica que el *password* proporcionado está relacionado con la identidad proporcionada; si éste es el caso, el usuario está autenticado; en caso contrario, el usuario no podrá acceder al sistema. El problema de este tipo de protocolos surge cuando un atacante cuenta con un *sniffer* y captura la identidad y el *password*. A partir de este momento el atacante puede autenticarse en el servidor como si se tratara del usuario.

Es posible usar los conceptos criptográficos para ayudar en la definición de protocolos de autenticación, la mayoría de los cuales están basados en el concepto de secreto compartido. Este secreto no es otra cosa que una llave, simétrica en muchos casos, que comparten el host donde se encuentra el usuario y el servidor en donde se desea autenticar. El usuario proporciona su identidad al servidor realizando una operación criptográfica en un número que el servidor le proporciona.

Por ejemplo, si un usuario A se desea autenticar con un servidor B, el usuario envía su identidad al servidor. El servidor genera un número (conocido como reto) y lo envía al usuario. Cuando el usuario recibe el reto, lo encripta con el secreto que comparte con el servidor (la llave) y lo envía encriptado al servidor. Este últi-

mo lo decripta y verifica que sea el mismo que envió en un principio. Si lo es, el usuario está autenticado, sino la autenticación falló.

El protocolo usa una llave simétrica junto con algún algoritmo como DES o IDEA. Un atacante no puede impersonalizar al usuario A basado en lo que capture con un *sniffer*, ya que la próxima vez el servidor enviará un reto diferente. Sin embargo, la autenticación no es mutua, ya que el servidor autentica al usuario, pero éste no autentica al servidor. Esto se resuelve si el usuario le envía un reto al servidor.

No todos los protocolos de autenticación están basados en criptografía simétrica. Es posible modificar el protocolo anterior para que el secreto compartido sea una llave pública y no una llave simétrica. En este caso se encripta el reto con alguna de las llaves y se decripta con la otra. También es posible aplicar un *hash* al reto o firmar éste.

Un *hash* (traducido como digestivo por varias personas) consiste en una función que, dada una entrada de información de tamaño variable, produce un número de identificación único de la información proporcionada. Si la información se cambia en un bit la información de entrada y se vuelve a calcular el hash, el número es totalmente diferente. Se considera una función de un solo sentido, ya que es posible producir un número a partir de una entrada, pero es imposible deducir la entrada a partir del número arrojado por la función hash. Dependiendo del tipo de algoritmo usado, el número es de 128, 160, o 512 bits. Entre los principales algoritmos hash podemos mencionar MD5, SHA-1 y SHA-512.

El protocolo S/KEY es un protocolo de autenticación basado en el uso de una función hash y en secretos compartidos. El usuario introduce una semilla al servidor y este lleva a cabo  $n$  operaciones hash sobre la semilla, donde  $n$  es un número cercano a 100. El servidor almacena el último valor calculado y el resto de los valores se mapean a valores ASCII y se imprimen. Esta lista se le entrega al usuario para que use uno a uno los *passwords*. La primera vez que se autentique usa el primer *password* de la lista y lo elimina de ésta, el servidor lo compara con lo que tiene almacenado y

autentica. En caso de que la autenticación tenga éxito calcula el siguiente valor hash. Cuando el usuario requiera autenticarse de nuevo, usa el siguiente *password* en la lista y lo presenta al servidor. Si un usuario captura el *password* no lo puede usar para impersonalizar al usuario debido a que éste ya no es válido. Las propiedades de la función hash, impiden que un atacante pueda deducir cuál es el siguiente *password* a partir de los *passwords* capturados.

Uno de los inconvenientes del protocolo anterior es el hecho de que el usuario cuenta con una lista de los *passwords* en claro. Si el usuario pierde esta lista, o le es robada de alguna forma, alguien puede autenticarse ante el sistema a su nombre. Lo anterior lo resuelven los sistemas OTP, (*password* de una sola vez, por sus siglas en inglés).

Un sistema OTP garantiza un nuevo *password* en cada conexión. El usuario establece un secreto en el servidor remoto y cuenta con una calculadora en software o en hardware. A nivel hardware esta calculadora toma la forma de un token, sincronizado de alguna forma con el servidor. Al autenticarse, el servidor envía su reto en forma de *string* al usuario. Una vez que el usuario recibe el reto, lo introduce a su calculadora para calcular la respuesta a dicho reto. El resultado es enviado al servidor que verifica lo enviado y procede a la autenticación de acuerdo a lo recibido por parte del usuario.

Internet proporciona un ambiente de comunicación para los usuarios. La cantidad de servicios que se ofrecen basados en internet va en aumento. Podemos comprar varios artículos a través de internet, podemos comunicarnos con texto, imagen y sonido con personas que se encuentran en diferentes países. Sin embargo, las amenazas están presentes y el riesgo de ser víctima de algún ataque en el que se vea comprometido alguno de nuestros recursos es real. Es nuestro deber estar preparados para aminorar este riesgo y, desde el punto de vista de desarrolladores, proporcionar un medio más seguro a los usuarios de usar internet. Pero también es responsabilidad del usuario el estar consciente de los riesgos y tomar las acciones pertinentes para dificultar la tarea de los atacantes. 



Israel Cortés Ramírez, CISA, CISM  
icortes@insys-corp.com.mx

*Insys-Soluciones Integrales de  
Seguridad en TI  
Gerente de Consultoría de Riesgos  
en TI*

## Security Awareness: un factor crítico de éxito en la seguridad de la información

*Probablemente el aspecto más difícil para crear un programa de seguridad de la información exitoso, es lograr la participación proactiva y continua del personal de las organizaciones en todas las escalas. La elaboración de políticas, estándares y guías de seguridad, es sólo el principio de un programa de seguridad de la información; sin embargo, por sí solas no llevan a cabo funciones ni restringen o instruyen al personal con respecto a las prácticas de seguridad que deben seguir y el conocimiento que deben tener.*

Un programa de seguridad de la información será menos efectivo si no tenemos un proceso continuo que nos proporcione la certeza de que los empleados reconocen la importancia de la seguridad, así como del rol y responsabilidad que llevan a cabo para el éxito de la misma.

Tal vez el primer paso para desarrollar un programa de *Awareness* es precisamente comprender ¿qué es el *Awareness*? y ¿Cuál es su objetivo principal?, sobre todo si consideramos que una gran cantidad de planes de *Awareness* fracasan por la poca claridad del concepto y su propósito. El principal error que existe es confundirlo *Awareness* con entrenamiento y pretender que en los esfuerzos de *Awareness* se enseñen las políticas, estándares, guías y, en muchos casos los procedimientos, instructivos y herramientas relacionados con la seguridad, sin antes haber “vendido” y “comprado” la idea de la seguridad de la información basada en los beneficios individuales y en el valor que aporta al negocio.

**Awareness es el proceso para lograr una conciencia de seguridad de la información. Debe lograr que los individuos reconozcan la seguridad, se preocupen por ella y respondan adecuadamente**

De esta forma, se clarifica la idea de la seguridad de la información como un problema de gente, por lo que resulta fundamental el desarrollo de una estrategia que proporcione a los empleados información adecuada sobre los diferentes temas y beneficios de la Seguridad, que basada en las necesidades reales de práctica y entendimiento, garantice que la gente comprenda, aplique y sea parte de la solución integral de seguridad de la información.

### **Security Awareness: un proceso de cambio organizacional**

Con frecuencia, vemos en los artículos que el *Awareness* es un proceso muy similar al *marketing*, y en algunos casos los autores se atreven a afirmar que es exactamente igual.

Sin embargo, la experiencia en este tipo de esfuerzos me permite aseverar que el proceso de *marketing* no es suficiente para lograr la conciencia de seguridad de la información en una organización, en todos los casos es necesario establecer una estrategia más compleja que permita enfocarse al factor humano no como un mercado, sino como un elemento clave que debe ser gestionado como parte de un cambio organizacional, de tal forma que el resultado del proceso de *Awareness* perdure lo suficiente para que la organización y las personas lo puedan madurar paulatinamente, hasta que forme parte de sus hábitos personales y de cultura laboral. Lo anterior permitirá garantizar que la seguridad de la información sea una moda o un impulso, sino un principio de negocio que permitirá al negocio operar de manera segura y confiable.

Este proceso de cambio requiere evidentemente esfuerzos mayores al *marketing* si tenemos en cuenta que el resultado esperado no será una labor trivial y que será necesario involucrarse con la forma y cultura de la organización.

*Security Awareness*. Una estrategia

Si contamos con una estrategia adecuada para resolver este problema, la situación se simplifica notablemente y la posibilidad de éxito será mayor al enfocar nuestros recursos y esfuerzos de forma asertiva y estructurada.

Es fundamental que la estrategia de *Awareness* esté basada en las carencias reales de entendimiento y prácticas de seguridad existentes en la organización, y que sea difundida por medio de los canales de comunicación de mayor preferencia e impacto entre el personal.

Las etapas de una metodología a otra pueden ser tan variadas o limitadas como los enfoques que utilizan y los objetivos

que pretenden. La siguiente metodología describe en siete fases un esquema estructurado y probado que permite lograr un *Awareness* asertivo y con un alto grado de efectividad.

#### **Fase I. Inicio**

Establecer la planeación de la ejecución de cada una de las fases con sus etapas respectivas y la definición de los roles y responsabilidades de las entidades involucradas, dentro de un marco de tiempo y formas adecuados para obtener el resultado esperado.

En esta etapa es fundamental definir ¿qué es *Awareness*? y ¿cuál es el objetivo?, además de conseguir un patrocinador o *sponsor* del proyecto.

#### **Fase II. Diagnóstico**

Obtener un estatus real del nivel de concientización actual de los usuarios para una determinación del nivel de vulnerabilidad organizacional en la gente, así como las preferencias sobre los medios de comunicación utilizados en la organización para difundir información oficial y autorizada.

La selección de técnicas para recopilación de esta información suele ser muy variado, y va desde cuestionarios automatizados en la intranet, hasta sesiones de trabajo y en algunos casos *focus group*; sin embargo, deberá analizarse la cultura organizacional y los métodos establecidos y, con ello, determinar si es posible seguirlos en caso de que sean confiables, o bien, establecer uno alternativo para lograr el objetivo deseado.

Como dato adicional, algunas estadísticas de clientes en México nos revelan situaciones interesantes que en algunos resultan alarmantes para las organizaciones, sobre todo si consideramos que, aproximadamente, 30% de usuarios comparte o ha compartido alguna vez su contraseña, 13% aceptó la posibilidad de fugas de información del negocio, 68% no sabría que hacer inmediatamente después de una infección de virus en la red y 83% de usuarios no ha realizado respaldos de sus equipos personales en los últimos seis meses.

Aun cuando estos datos son muy reveladores, no podemos basar completamente el programa de *Awareness* en este resultado; debemos combinar otros elementos en caso de tenerlos disponibles.

#### **Fase III. Unificación de requerimientos y definición de medios**

Determinar asertivamente los rubros de seguridad de la información hacia los cuales deberán enfocarse los esfuerzos



de *Awareness*, de acuerdo con la situación real que vive el negocio, considerando:

- Resultado del diagnóstico (etapa anterior).
- Análisis de riesgos. Es indispensable considerar esta entrada de información en caso de tenerla disponible, en virtud de que los esfuerzos de *Awareness* deberán estar orientados también a los riesgos más significativos de la organización.
- Normatividad existente. La normatividad no será utilizada en el proceso de *Awareness*, pero debe ser estudiada para no contradecir ningún lineamiento existente en materia de seguridad.

#### Fase IV. Definición de la estrategia

Integrar los elementos de la estructura de la estrategia de *Awareness* y las diferentes herramientas que garanticen su aplicación y desarrollo adecuado dentro de un marco de tiempo apropiado, a través del uso de medios de comunicación de mayor preferencia y elementos gráficos, ya sean electrónicos, impresos o presenciales.

Un factor indispensable en la definición de la estrategia de *Awareness*, es lograr una adecuada definición y clasificación de audiencias, no podemos llevar los mismos mensajes en forma y fondo a la alta dirección que a la gerencia media, lo siguiente puede proveer una claridad mayor al respecto. (Ver tabla 1)

T a b l a 1

Audiencia	Técnicas	Medios	Resultados esperados
Alta gerencia	<ul style="list-style-type: none"> <li>• Justificación de costos</li> <li>• Comparación con la Industria</li> <li>• Reportes de auditoría</li> <li>• Análisis de Riesgos</li> </ul>	<ul style="list-style-type: none"> <li>• Presentación</li> <li>• Video</li> <li>• Reportes de violaciones</li> </ul>	<ul style="list-style-type: none"> <li>• Fondos</li> <li>• Apoyo</li> </ul>
Gerencia media	<ul style="list-style-type: none"> <li>• Demostrar beneficios en el trabajo</li> <li>• Ejecutar revisiones de seg.</li> </ul>	<ul style="list-style-type: none"> <li>• Presentación</li> <li>• Artículos de Seguridad</li> <li>• Videos</li> </ul>	<ul style="list-style-type: none"> <li>• Apoyo</li> <li>• Recursos de apoyo</li> <li>• Adherencia</li> </ul>
Usuarios	<ul style="list-style-type: none"> <li>• Firma de declaraciones de responsabilidad</li> <li>• Políticas y procedimientos.</li> </ul>	<ul style="list-style-type: none"> <li>• Presentación</li> <li>• Periódicos y noticias</li> <li>• Video</li> </ul>	<ul style="list-style-type: none"> <li>• Apoyo</li> <li>• Adherencia</li> </ul>

#### Fase V. Ejecución

Ejecutar, con estricto apego al Plan de *Awareness*, los programas y cronogramas de actividades elaborados durante la definición de la estrategia.

Algunas fechas que pueden ser usadas como referencia o apoyo son las siguientes:

- Mayo 10 - *International Emergency Response Day*
- Septiembre 8 - *Computer Virus Awareness Day*
- Noviembre 30 - *International Computer Security Day*

#### Fase VI. Mecanismos de evaluación

Medir y evaluar el desempeño de las técnicas, procedimientos y la metodología que fueron empleados para difundir los conceptos y otros conocimientos sobre seguridad de la información para identificar los puntos de mejora.

Algunos de los elementos que pueden ser usados para medir la efectividad del *Awareness* pueden ser:

- Cuestionarios.
- Observación.
- Entrevistas con usuarios finales.
- Tickets of help desk.
- Incidentes de seguridad.

#### Fase VII. Retroalimentación

Identificar todas aquellas propuestas de mejora a la estructura y desarrollo de la estrategia para determinar su factibilidad de aplicación y ejecución.

#### Conclusión

La seguridad de la información requiere elementos adicionales a la existencia de políticas, estándares, guías, procedimientos, herramientas y tecnologías de seguridad, es más que recomendaciones de auditoría y requerimientos de autoridades; entre estos elementos, siempre encontraremos el convencimiento del negocio y el factor de la gente. En lo que respecta al segundo elemento, debemos tener presente que con el *Awareness* tenemos que cambiar prácticas y formas de hacer las cosas de muchos años atrás, y cuando esto se lleva a cabo con gente de por medio, el riesgo a fracasar es alto: debemos tener en mente que vamos a cambiar a la gente y, con ello, a la organización misma.

También es necesario considerar que, antes de exigir a los empleados que cumplan con los requerimientos del programa de seguridad de la información, primero deberán estar concientes de la importancia de la seguridad y de los beneficios que la misma aporta al trabajo diario y al negocio; de esta forma, existirá la apertura y, por consiguiente, el convencimiento de que las actividades que deberán realizar de forma adicional a su trabajo diario traerán como consecuencia buenos resultados.

Finalmente, tenemos que reconocer que el *Awareness* no debe ser una capacitación para los empleados, sino un programa que tiene como misión transmitir mensajes asertivos por diferentes métodos y mecanismos para que logren la atención de los empleados hacia la seguridad de la información. Una vez que esto se ha logrado, el *Awareness* puede ser considerado exitoso; sin embargo, no deberá perderse la secuencia, pues en seguida viene el entrenamiento, mediante el cual los empleados incrementaran sus aptitudes para colaborar de manera formal y activa con la seguridad, sin olvidarse de proveer los medios para llevar a cabo el cumplimiento de los requerimientos de seguridad existentes. 



L.S.C.A. Luis Fernando Orozco H.

*Gerente de Administración  
de Riesgos Operacionales  
y de Sistemas,  
PricewaterhouseCoopers, S.C.*

# El ambiente de seguridad en SAP R/3

*Ya en otra ocasión hemos hablado de las debilidades que la automatización de los procesos está generando con respecto a la seguridad de los datos en las organizaciones. Esto debido entre otras cosas a:*

1. La incorporación de controles de seguridad no se acomete al principio de los proyectos de implantación y despliegue de sistemas, sino al final, donde no es extraño encontrar que los presupuestos ya se han agotado. De este modo, la seguridad queda entre los elementos que se atienden de forma insuficiente.
2. La poca visibilidad de los controles automatizados con respecto a los controles físicos, en este caso los controles de seguridad. Es fácil que cualquiera pueda detectar que existe un guardia de seguridad en una sucursal bancaria, como también es fácil observar si es que en un establecimiento se está guardando el dinero —producto de las ventas— en un cajón bajo llave o si se deja amontonado sobre el mostrador; ambos casos hablan de controles físicos. Sin embargo, ya no es tan fácil observar si un sistema SAP R/3 impide el

uso de contraseñas obvias, tales como México, el nombre de la empresa, abc, etc. Mucho menos fácil es observar si los objetos de autorización que resguardan el acceso a las transacciones de contabilidad, se encuentran activados o no. Estos dos ejemplos son controles automatizados, inmersos en las aplicaciones de su sistema SAP R/3.

3. El punto anterior nos introduce al tercer elemento que ha provocado debilidades en los controles de seguridad en las aplicaciones, el cual es el alto nivel de especialización que se requiere para conocer, implantar y evaluar la eficacia de los controles automatizados. La disponibilidad de recursos humanos con los conocimientos necesarios se torna complicada.

Lo anterior nos permite vislumbrar por qué una de las fortalezas de mayor importancia de los sistemas SAP R/3, también puede operar como una de sus más grandes debilidades, la cual es su entorno de seguridad.



El entorno de seguridad del sistema SAP R/3 es muy robusto, quizá de lo más robusto en aplicaciones ERP en el mercado; permite un control muy detallado de los permisos de acceso, sin embargo; no viene pre-configurado, es decir, no está listo para ser usado tal como es entregado por el proveedor (SAP AG).

El entorno de seguridad de SAP R/3 tiene que ser configurado. No obstante, SAP ofrece muchos elementos modelos que se pueden copiar para ser usados en la instalación de su empresa, dichos elementos no dejan de ser genéricos; es decir, no han considerado las particularidades de su organización ni el número y complejidad de puestos de trabajos existentes en su empresa ni las necesidades específicas de acceso o denegación de accesos requeridas en su organización.

Así como el entorno de seguridad de SAP R/3 es de los más robustos existentes, también es de los más complejos de configurar; lo cual puede comprenderse natural, ya que para soportar una sofisticación de permisos y denegación de accesos, es lógico que deba emplearse un igualmente sofisticado sistema de configuración de seguridad.

Si consideramos que muchos proyectos dejan los temas de seguridad hasta al final y con poca prioridad; que se requieren altos niveles de especialización para configurarla e incluso para entenderla y evaluarla. Tenemos que los entornos de seguridad de los sistemas SAP R/3 en México (los cuales son generalmente jóvenes de nueva implantación), se encuentran en situaciones de alta exposición, en otras palabras, con grandes debilidades. Lo anterior deja una situación preocupante, ya que el resguardo, confidencialidad y acceso restringido a los datos y transacciones se encuentra comprometidos.

Como muestra expondremos un caso:

Sucede que su oficial de seguridad de su instalación SAP R/3 ha realizado un excelente esfuerzo (y largo, ya que pudo llevarle meses), en afinar todas las definiciones de perfiles de acceso de su instalación SAP R/3. En este esfuerzo, los perfiles se han definido siguiendo las especificaciones de la descripción de puestos del área de recursos humanos (que es un tema bastante amplio; ¿la descripción de puestos de su organización se encuentra actualizada a las tareas que realmente ejecutan su personal?)

Los perfiles, a su vez, han sido configurados de forma tal que no sólo restringen el acceso a las transacciones exclusivamente necesarias para ejecutar las responsabilidades de cada puesto, sino que han sido restringidos para acceder únicamente a las áreas de la estructura organizativa de su empresa a las cuales tengan competencia. Por ejemplo, el perfil de grupo de compradores de Guadalajara no podrá acceder los datos del grupo de compradores de Monterrey.

Adicionalmente, su oficial de seguridad junto con las áreas de negocio ha realizado un excelente (y no fácil de encontrar en las instalaciones SAP R/3 de México) estudio con respecto a la segregación de funciones; donde se expone que los perfiles no tienen asignadas transacciones que pudieran considerarse incompatibles, ya que otorgarían excesivos derechos a un usuario sin supervisión, tales como registrar facturas de proveedores y generar el pago a los proveedores.

Todo parece perfecto. Gracias a que el proyecto ha sido cuidadosamente ejecutado y todos los detalles se han considerado, los *logs* de auditoría también han sido considerados y se han activado.

Posteriormente, durante la auditoría del año, se realiza una auditoría de control interno y del aplicativo SAP R/3 de su organización (la cual está a prueba de todo). Sin embargo, la auditoría detecta, gracias a los *logs* de auditoría que se encuentran activados en el sistema (¿los *logs* de auditoría de su instalación se encuentran activados?), algunos usuarios con varios acceso a transacciones de que no han sido autorizados.

La definición de los perfiles de dichos usuarios establece claramente que no tienen permisos de acceso a dichas transacciones. Sin embargo, los *logs* de auditoría han revelado que, en efecto, han accedido a dichas transacciones y en varias ocasiones.

¿Cómo puede suceder esto? No es un caso ficticio, son cosas que pasan en realidad.

Sucede que el proyecto de afinación de perfiles, paso de largo considerar si los elementos de configuración de seguridad (llamémosle objetos de autorización) se encontraban activado o no.

Los permisos a transacciones no autorizadas fueron posibles debido a que los objetos de autorización se encontraban

desactivados, lo cual en el entorno de seguridad de SAP R/3 significa que las validación que el sistema SAP R/3 hace con respecto a esos objetos es inexistente; es decir, independientemente de que se halla especificado claramente que no tenían acceso, el sistema no valida la restricción y no impide el acceso.

¿Cree usted que con activar los dichos objetos de autorización, ya se tienen suficientes garantías de que los perfiles de acceso tan perfectamente definidos serán efectivos y controlarán efectivamente los accesos?

La respuesta es negativa, ya que los objetos de autorización también pueden ser desactivados globalmente; además, existen parámetro del perfil de su instalación SAP R/3 que de no ser configurados adecuadamente, también estropearían todo el trabajo de su oficial de seguridad y también su confort con respecto a los accesos a su sistema.

Por desgracia, la seguridad no es un tema que pueda ignorarse. No puede dejar usted a su banco sin guardias de seguridad, solo porque estos son complejos y difíciles de configurar. Tampoco hay soluciones mágicas o entornos de seguridad pre-configurados, ya que éstos tendrán que venir pre-configurados a las características de operación, tamaño y estructura organizacional de su propia empresa; es decir, tendría usted que comprarle a una empresa idéntica a la suya dicha configuración. En otras palabras, tendría usted que comprar dicho entorno de seguridad, a usted mismo.

¿Se encuentran todos los elementos de necesarios configurados en su instalación SAP R/3? ¿Tiene usted derecho al confort de que su instalación reside en un ambiente de control?

Un trabajo de auditoría que cuente con la independencia, objetividad, nivel técnico y profesional necesarios y que describa de forma clara y real su situación, podría ayudarle a responder la pregunta anterior.

Ahora bien, el siguiente paso es evaluar si al tema de seguridad SAP R/3 se le ha otorgado la prioridad que merece en su organización. El resguardo de la información de su sistema y las responsabilidades y compromisos con los mismos, ante sus empleados, clientes, proveedores accionistas, gubernamentales, pudieran estar comprometidos. 



L.I.A. Sandra Urías Iris  
saurias@dtmx.com

*Gerente de Consultoría en Business  
Continuity Management (BCM)  
Galaz, Yamazaki, Ruiz Urquiza, S.C.*

# Gestión de la continuidad del negocio

*La evolución de los planes de recuperación para casos de desastre en las empresas ha dado lugar al surgimiento de un nuevo concepto: Gestión de la Continuidad del Negocio (Business Continuity Management, BCM).*

La gestión de la continuidad del negocio es un proceso de administración integral que identifica impactos potenciales que amenazan a una organización y ofrecen un marco de referencia para brindarle flexibilidad y la capacidad para tener una respuesta efectiva que salvaguarde los intereses de sus accionistas, así como la reputación, la marca y las actividades de valor agregado de la misma.

El BCM se concibe como un proceso que debe pertenecer y estar completamente integrado en la empresa como parte crítica del proceso administrativo.

El BCM tiene como objetivos:

- Mejorar la flexibilidad de una organización.
- Identificar por adelantado los impactos potenciales de una amplia variedad de interrupciones repentinas en la habilidad de la organización para responder exitosamente.
- Priorizar los esfuerzos de varios especialistas con el propósito de obtener flexibilidad en sus áreas de experiencia, tales como seguridad, instalaciones y tecnología de información.

El BCM está enfocado en el desarrollo de la flexibilidad de las organizaciones, lo cual le permite sobrevivir la pérdida de una parte o de toda su capacidad operacional. También



debe dirigirse a la supervivencia de pérdidas significantes de recursos, tales como personal o equipo. Debido a que la flexibilidad del BCM de una organización depende de su personal de administración y de operación, así como del de tecnología y su diversidad geográfica, la empresa debe estar preparada para responder y ser flexible, desde los altos niveles ejecutivos hasta los más básicos, a través de todas las localidades (incluida la cadena de suministro).

Si bien es posible calcular las pérdidas financieras de una interrupción, la contingencia de mayor impacto usualmente se refleja en daños a la reputación o pérdida de confianza, como resultado de un incidente mal administrado.

## **¿Cómo beneficiará la Gestión de la Continuidad del Negocio (BCM por sus siglas en inglés) a mi empresa?**

El propósito principal del BCM es asegurar que la organización tiene manera de responder a interrupciones mayores que amenazan su existencia. Mientras que este análisis tiene un valor por sí solo, existen otros beneficios que pueden obtenerse al contar con un BCM como parte de una disciplina administrativa.

Algunas organizaciones tienen que cumplir con requerimientos de ley y de regulación, ya sean específicos para el BCM o, en general, para la administración de riesgos. Un plan de BCM adecuado satisfará tanto los requerimientos específicos como a la contribución de riesgos específicos y la toma de conciencia de riesgos de una organización. Sin embargo, el principal factor a considerar para el BCM debería ser siempre que se asume la responsabilidad porque agrega valor a una empresa, más que por consideraciones de regulación.

El BCM exige que exista un grupo de ejecutivos del más alto nivel, integrado —de ser posible— por los líderes o dueños de las áreas de negocio más importantes de la empresa, ya que si la dirección no se involucra, este plan no tendrá éxito, pues requiere de la aprobación de inversiones para definir las estrategias de recuperación y de continuidad que deban ser implantadas.

Dichas inversiones son considerables porque se puede requerir de un proveedor que proporcione un sitio alternativo para recuperar la infraestructura e información del centro de cómputo y establezca un centro de comando para el manejo y control de la contingencia, así como un centro de trabajo alternativo para operar las áreas de negocio críticas hasta que se restablezca la operación normal.

Otro aspecto importante a considerar es la necesidad de efectuar pruebas del plan y ejecutarlas de diferentes formas, con el propósito de validar aspectos importantes, como identificar las interrelaciones correctas entre las diferentes áreas del negocio.

Desafortunadamente, la renuencia del mercado mexicano a estar preparado para reaccionar ante situaciones de desastre, se ha hecho evidente frente a la enorme cantidad de catástrofes que han ocurrido en el mundo, de tal manera, que aquel empresario o ejecutivo que considere que no le sucederá nada a su empresa, denotará una escasa visión. Asimismo, quienes piensan que van a salir adelante después de un desastre con tener sólo los respaldos de su información se equivocan: pues se requiere de toda una logística, de una preparación y de trabajo en equipo para identificar todos los aspectos a considerar y contar con un BCM en forma.

Los altos ejecutivos de toda empresa conocen cuáles son las operaciones más importantes del negocio; pero no pueden identificar cuánto pueden llegar a perder en uno o dos días si no se encuentran disponibles dichas operaciones; es decir, los impactos operativos y económicos que representarían el no contar con sus áreas de negocio más importantes. Ésos y otros datos de importancia se obtienen al aplicar un análisis de impacto al negocio, una de las principales actividades a desarrollar cuando se está haciendo un BCM.

## ¿Existe ROI con el BCM?

Muchas empresas preguntan cuál es el retorno de inversión al desarrollar un BCM y la respuesta es que para desarrollarlo se tiene que hacer una fuerte inversión. Es como comprar un seguro, ya sea de vida, de automóvil o de gastos médicos: no regresa nada hasta que sucede lo inevitable. El BCM es la protección de la entidad y representa la confianza que se les proporciona a los clientes, empleados, proveedores e inversionistas de que el negocio va a tener una continuidad, aun cuando sucedan diferentes tipos de desastres. De esta forma, el ROI del BCM es más grande que cualquier otra inversión, porque le da la oportunidad a la empresa de seguir o continuar existiendo ante el evento de una contingencia. Por eso, es de gran importancia cuidar lo que se ha invertido.

**El BCM es la protección de la entidad y representa la confianza que se les proporciona a los clientes, empleados, proveedores e inversionistas de que el negocio va a tener una continuidad**

## ¿Por qué las empresas necesitan gestión de la continuidad del negocio?

Recientes investigaciones en el impacto de un evento no planeado han revelado algunos datos preocupantes. Una de cada cinco organizaciones sufrirá un incendio, inundación o tormenta, falla en la energía eléctrica, terrorismo y algún desastre en el hardware o software. De aquéllos que no cuentan con un plan de continuidad del negocio:

- Nunca reanuda operaciones: 43%.
- Cerrará sus operaciones dentro de los 13 meses siguientes: 80%.
- De los que reclaman un seguro, nunca se recuperan de las pérdidas causadas por el desastre 53%. (Fuente: Aveco)
- De los negocios que pierden datos en un desastre, son forzados a cerrar las operaciones dentro de los dos años de ocurrido el desastre: 90%.
- De los negocios que han experimentando una pérdida en los servicios de cómputo, serán forzados a cerrar sus operaciones dentro de los cinco años siguientes: 50%. (Fuente: London Chamber of Commerce)
- La interrupción de los sistemas mayores tiene un costo para 15% de las organizaciones de más de \$100,000 USD por hora. (Fuente: Information age)

Es importante destacar que los motivos para incorporar un BCM en la empresa deben ser claramente definidos desde el inicio, pues esto previene una posible confusión más adelante en el proyecto. Cualquiera que sean estos motivos, es necesario obtener el soporte y la aprobación de los altos niveles ejecutivos, de otra forma, el proceso no tendrá éxito. 



Guadalupe Castañeda Campos CPA, CISA

*Socia del Área de Control y Administración de Riesgos Electrónicos (CARE) de Mancera Ernst & Young.*

## Seguridad de la información: ¿Dejarla a la suerte?

*Los resultados de la 7ª Encuesta Global de Seguridad de la Información de Mancera Ernst & Young<sup>1</sup> revelan que muchas organizaciones “dependen de la suerte” al tratarse del tema de seguridad de la información. Y usted, ¿cuánto confía en la suerte?*

La información es uno de los activos más importantes y valiosos de cualquier organización. Su adecuado manejo es clave para la continuidad de cualquier negocio y para el cumplimiento de los objetivos estratégicos de las organizaciones. Es por esto que la seguridad de la información es un habilitador fundamental para el negocio, ya que permite crear y mantener la confianza que hoy exigen las relaciones empresariales.

Cualquier organización puede ser blanco de ataques por agentes internos y/o externos que busquen sustraer, alterar o lucrar con su información. Bastaría un solo ataque exitoso que involucre el obtener información confidencial para tener consecuencias incalculables en la continuidad de sus operaciones, finanzas, imagen y prestigio, así como para dañar la confianza de clientes e inversionistas en su organización.

<sup>1</sup> Encuesta realizada en el ámbito global durante 2004, en donde participaron 1,230 organizaciones en 51 países. México ocupó el 5º lugar en el número de encuestados, después de Estados Unidos, India, Australia e Italia.

No obstante, los resultados de la 7ª Encuesta Global de Seguridad de la Información revelan que muchas organizaciones están tomando una postura reactiva en cuanto al tema, al confiar más en la suerte que en un sistema de control diseñado para mitigar riesgos relacionados con la seguridad de la información en forma continua.

La encuesta también reveló que en México la falta de presupuesto es el principal obstáculo para desarrollar estrategias efectivas de seguridad de la información, seguido por la dificultad para mostrar a la alta dirección el valor estratégico que implica el contar con esquemas de seguridad, y por la falta de conciencia del tema a nivel organizacional. Sin embargo, son precisamente estos mismos temas los que tienen menor prioridad para los responsables de la función de seguridad, tanto dentro como fuera de México.

Mientras que en México 97% de los encuestados (93% en el mundo) reconocieron que la seguridad de la información es “muy importante” o “Importante” para alcanzar los objetivos de negocio, otros resultados de la encuesta parecen indicar lo contrario.

### **Atención por parte de la alta dirección**

Los resultados de la encuesta resaltan la escasa prioridad y participación de la alta dirección en temas de seguridad de la información al ceder la responsabilidad del tema al área de tecnología, incluso a mandos medios. La participación de la alta dirección en este tema es fundamental para un programa de seguridad efectivo.

La tabla 1 presenta las calificaciones promediadas de la importancia que los ejecutivos de las organizaciones dieron al tema. Como se puede apreciar, los resultados no son muy contundentes.

T a b l a 1

Declaraciones	1	2	3	4	5
En mi organización, el tema de seguridad de la información es una de las prioridades del Director General (CEO)				●▲	
Los directores del más alto nivel consideran las inversiones en seguridad de la información como un costo necesario para hacer negocios			●▲		
Los líderes de las unidades de negocio o propietarios de los procesos aprecian el valor que la seguridad de la información trae a la organización			●▲		

Nota: La puntuación es de 1 a 5, siendo 1 muy en desacuerdo y 5 muy de acuerdo  
 ▲ Global ● México

Además, sólo 28% de los encuestados en México estuvieron de acuerdo con que sus organizaciones perciben la seguridad de la información como una prioridad a nivel CEO (*Chief Executive Officer* - Director General).

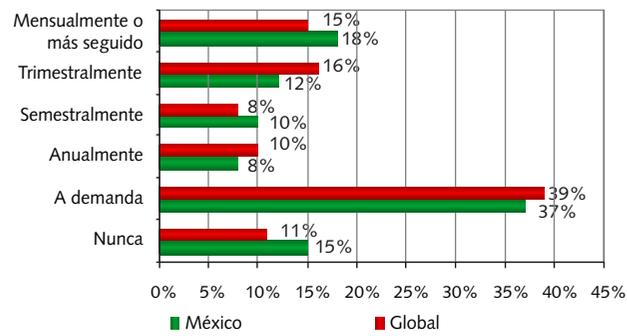
### Valor estratégico de la seguridad de la información

A pesar de que uno de los principales obstáculos para un programa efectivo de seguridad de la información es la dificultad para mostrar a la alta dirección su valor estratégico, los esfuerzos por presentarles el tema son insuficientes.

Tanto en el ámbito nacional como en el global, sólo 40% reporta al consejo de dirección o su equivalente sobre temas relacionados con la seguridad de la información en forma mensual, trimestral o semestral. Reporta de manera anual, poco frecuente o nunca: 60%. (Gráfica 1)

G r á f i c a 1

### Valor estratégico de la seguridad de la información



### ¿Con qué frecuencia se reporta a su consejo de dirección o equivalente sobre temas relacionados con seguridad de la información?

La encuesta también reveló que sólo 55% de los responsables de seguridad de la información en México se reúnen con los líderes de las unidades de negocio en forma mensual, trimestral o semestral. Por otra parte, 45% lo hace en forma anual, no tan seguido o nunca.

### Conciencia del personal en torno al tema

Otro obstáculo importante en México para un programa de seguridad de la información eficaz es la falta de conciencia del tema a nivel organizacional. No obstante, la encuesta reveló que:

- Menos de la mitad de los encuestados ofrece a sus empleados entrenamiento continuo en seguridad y controles.
- Poco más de 55% entrena a sus usuarios para identificar y reportar actividades sospechosas.
- El incrementar la conciencia de seguridad entre el personal ocupa la décima posición entre las prioridades de los responsables de la función de la seguridad de información.
- De los encuestados, 20% no cuentan con un presupuesto para la seguridad de la información.

### Efectividad de la seguridad de la información

Aunado a los resultados presentados previamente, los encuestados no mostraron estar muy preparados para hacer frente a sus vulnerabilidades (ver tabla 2). Adicionalmente, un alarmante 22% de las organizaciones mexicanas encuestadas reconoció no tener las habilidades para cuantificar los daños causados por incidentes de seguridad en sus organizaciones durante el año 2004.

T a b l a 2

### ¿Qué tan de acuerdo está con las siguientes declaraciones?

Declaraciones	1	2	3	4	5
El nivel de protección de mi organización es adecuado para hacer frente a ataques externos				●▲	
Mi organización es efectiva para identificar vulnerabilidades en los sistemas de información			●▲		

Nota: La puntuación es de 1 a 5, siendo 1 muy en desacuerdo y 5 muy de acuerdo  
 ▲ Global ● México

### Recomendaciones

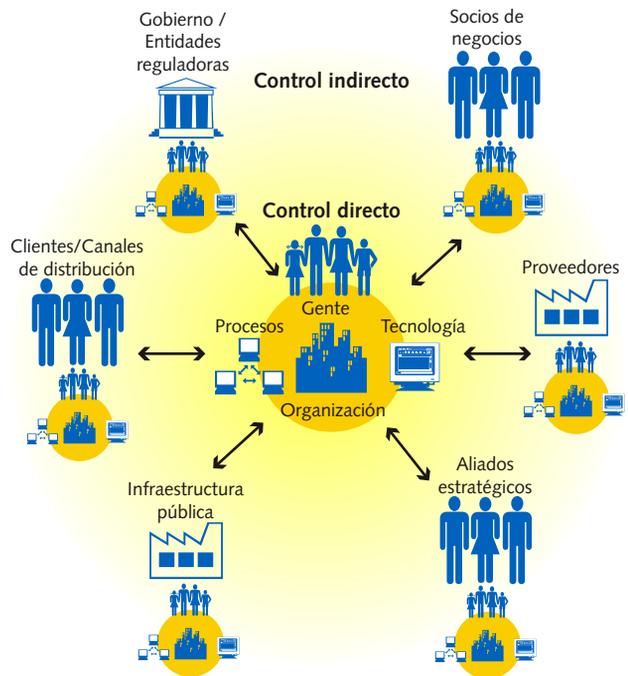
En resumen, los resultados de la encuesta muestran que las organizaciones no están dando un enfoque proactivo al tema de la seguridad de la información. Pocas han hecho esfuerzos integrados y efectivos para analizar sus riesgos referentes a este tema, lo cual hace imposible tomar las acciones requeridas. A continuación encontrará recomendaciones específicas para analizar el tema:

1. Realizar un análisis de riesgos integral. Éste debe involucrar a la alta dirección y a los mandos medios, tener una visión amplia de la organización y, en consecuencia, el tema a nivel de estrategia de negocio.
2. Definir una estrategia de seguridad de la información, alineada a la del negocio, que considere:
  - a. Ampliar el enfoque tecnológico, hacia la gente y los procesos. (Ver gráfica, página siguiente)
  - b. Desarrollar una conciencia de seguridad de la información en todo el personal de la organización como base.
  - c. Entrenar, capacitar y educar al personal que lo requiere.



sistema de control diseñado para mitigar riesgos relacionados con la seguridad de la información en forma continua. 

**Outsourcing** Gráfica 2



d. Exigir niveles de seguridad a terceros y hacer que se cumplan. Es sumamente importante tener en cuenta los riesgos que corren las organizaciones al tener este tipo de relaciones de negocio - *outsourcing*, proveedores, socios de negocio, clientes y canales de distribución, entre otros. (Gráfica 2)

3. Hacer de la seguridad de la información un proceso continuo e intrínseco a los procesos del negocio.

La formalización de estas recomendaciones le ayudará a ser más proactivo, confiando menos en la suerte y más en un



C.P.C. Edgar de la Rosa Cabello  
delarosa.edgar@kpmg.com.mx

*Socio de KPMG  
Miembro de la Academia  
Mexicana de Auditoría Integral  
y al Desempeño, A. C.*

# Los medidores del desempeño en la seguridad informática

*C*ada día se requiere de información actualizada y confiable que, a través de procedimientos de control y medidores del desempeño, detecten posibles desviaciones a la misma, para reducir los riesgos y medir la eficiencia, eficacia, los efectos y el costo-beneficio de sus actividades.

El papel de los medidores del desempeño en la seguridad es crucial cuando existen sistemas de información complejos y con alta dependencia de los mismos.

Últimamente hemos sabido de casos donde se ha violado la privacidad y confidencialidad de las empresas por medios cibernéticos. Muchos de ellos se han debido a la exposición que se tiene al intercambio de la información a través del comercio electrónico, del uso de internet o el acceso a los sistemas de información a personas externas a las organizaciones. Sin embargo, estos factores, entre otros, a veces son inevitables por las actividades que deben desarrollar las empresas para permanecer como negocio en marcha. Sin duda, uno de los aspectos importantes es el contar con medidas de seguridad que mitiguen los riesgos antes mencionados.

Las medidas de seguridad que se tengan implantadas deben ser acordes con las necesidades y sistemas de información de la empresa de que se trate, sin menoscabar los aspectos tecnológi-

**El papel de los medidores del desempeño en la seguridad es crucial para una empresa que desea continuar como negocio en marcha**

cos que le rodean, como pueden ser las transacciones inalámbricas (*wireless*), entre otras. Asimismo, deben estar en línea con las actividades preponderantes de las empresas, las cuales garantizan la permanencia de las mismas. De ahí se desprende que deben ser medibles, lo que implica contar con medidores del desempeño que coadyuven al logro y funcionamiento de la seguridad en los sistemas de información. Estos medidores deben ser capaces de detectar o prevenir una situación de riesgo y permitir de manera oportuna reaccionar a los responsables de la seguridad.

¿Pero qué son los medidores del desempeño? Son mecanismos establecidos que permiten evaluar cualitativamente y cuantitativamente los programas, operaciones y actividades que se ejecutan en una organización para la consecución de sus objetivos, lo que enfocado a la seguridad mitigaría al máximo los riesgos a los cuales está expuesta una entidad. El desarrollo de las medidas de seguridad debe permitir conocer a qué grado cubren el riesgo, la eficiencia y el costo-beneficio de las mismas. En este tenor, se deben definir las metas y los objetivos perseguidos de acuerdo con las áreas a cubrir, así como qué atribuciones son vulnerables (matriz de riesgos), para formular los indicadores y generar un modelo integral de desempeño, el cual debe ser dado a conocer a todos los participantes y áreas involucradas. Asimismo, es importante definir el mecanismo para administrar la información de los indicadores para su adecuado monitoreo.

Si partimos de la base de que toda entidad busca hacer negocio con un nivel óptimo de riesgo, es necesario que antes de desarrollar la matriz de riesgos se analice si todos los requerimientos del negocio y las necesidades de los usuarios están soportados por las funciones y procesos de Tecnología de Información (TI), ya que esto no puede estar en línea con los objetivos, las estrategias y los planes futuros de la organización, generando pérdidas por:

- Prácticas ineficientes, interfaces innecesarias y procesos duplicados.
- Inadecuado manejo de los riesgos de TI debido a una falta de entendimiento de dichos riesgos por la administración.

- Gastos innecesarios e inversiones que no soporten la estrategia y los planes del negocio.

En este sentido, los medidores del desempeño deben enfocarse a lo que se describe en los párrafos posteriores.

### Activos de la información

Los activos de la información se refieren al riesgo a que está expuesta una entidad por la naturaleza de los datos y el valor que éstos tengan.

Las pérdidas pueden ser importantes, al grado de poner en duda la continuidad del negocio, ya que directamente se pueden infiltrar en la información financiera, como podría ser el caso de fraude o robo, o indirectamente, a través del impacto sobre la reputación de la organización, al modificar o referenciar hacia otros sitios cibernéticos la página ubicada en el sitio de internet (*web site*), o el perder información sensible para el negocio o de propiedad intelectual (por ejemplo: fórmulas, maestro de clientes y proveedores, entre otros).

### Dependencia de la tecnología de información

La dependencia de la tecnología de información reviste importancia, pues las actividades y procesos de una entidad podrían no llevarse a cabo, si es que los sistemas no se encuentran disponibles, ya que existen diversidad de controles automatizados que no lograrían ser eficientes, como los relativos al servicio a clientes, lo cual generaría la no satisfacción de los mismos. En este tipo de riesgo, el impacto podría ser mayor al no tener acceso al proceso de la información para la toma de decisiones.

Para este medidor se deben considerar aspectos como el número y tamaño de los sistemas automatizados para controlar los procesos, el ambiente de uso de papel (*paperless*), la sofisticación de los sistemas y el tiempo de supervivencia sin el uso de TI; así como indicadores de la utilización de los equipos, capacidad de los servidores, uso de correo electrónico, etcétera.

Por otro lado, también se debe evaluar la naturaleza y el grado de dependencia sobre el personal (incluido el especializado) que integra el departamento de sistemas, ya que esto puede representar pérdida

de conocimiento y de las habilidades de ciertos individuos que lo conforman, o el mantener personal con habilidades inadecuadas. Los medidores del desempeño deberán ir dirigidos hacia la evaluación de las habilidades relevantes que son necesarias para las necesidades actuales y futuras, hacia los niveles de entrenamiento, el número necesario de personal y sobre su desempeño, así como la rotación del mismo (por ejemplo: planes de cambio de personal, estabilidad, etcétera).

Estos aspectos también deben ser considerados cuando la dependencia es con terceras partes, ya que puede darse el caso de que no exista un adecuado entendimiento por parte de la compañía contratada de la operación del negocio, mermando el desempeño del mismo, y esto represente costos excesivos sobre la conveniencia de manejarlo internamente en la organización. Los medidores deben estar enfocados al nivel de servicio, lo que incluye el soporte, el centro de ayuda y la administración de los sistemas.

### Seguridad de los sistemas

La falta de seguridad en los sistemas de información provoca pérdidas importantes en las organizaciones, lo cual se representa por la inconsistencia o falta de integridad en los procesos de información. Lo anterior causa la inversión en trabajos para remediar y/o rectificar los problemas de los procesos, y la posibilidad del uso de información que no sea confiable en la toma de decisiones.

Uno de los indicadores importantes del desempeño es el monitoreo de la frecuencia de errores y problemas en los procesos actuales, lo cual indicaría el nivel de seguridad de los sistemas en este aspecto. Esto es, si los operadores requieren realizar un reproceso al finalizar el día, o si soporte técnico lleva a cabo correcciones a los sistemas en línea. Adicionalmente, si los usuarios pueden manipular la información y la existencia de problemas de conciliación de cuentas (entre mayor general y auxiliares).

### Cambios en TI

Los procesos relativos a cambios en los sistemas están expuestos por el simple hecho de intercambiar lo que existe por algo nuevo. Los medidores deben concentrarse



en entender cómo se pueden manejar las situaciones de ineficiencia o de arranque, cuando los cambios no trabajan de acuerdo con las necesidades del negocio, así como en la existencia de errores y pérdida de seguridad en las aplicaciones implantadas debido al mantenimiento continuo y cambios menores, y lo más grave, cuando los cambios no fueron totalmente comprendidos por los usuarios finales.

Sin duda, no se deben descuidar los aspectos reguladores, como los del ámbito fiscal.

### Medidores del desempeño

En general, algunos ejemplos de medidores del desempeño, serían como sigue:

- Reducción de incidencias de un periodo a otro
  - Caída de los servidores
  - Quejas de usuarios
  - Cambios mínimos a los sistemas
  - Uso de software ilegal
  - Nivel de servicio
  - Accesos inapropiados
- Número de pruebas a desarrollar para determinado propósito
  - Plan de contingencias
  - Cambios en plataformas
  - Uso de software legal
  - Políticas de seguridad
  - Manuales de procedimientos
  - Auditorías internas y externas
  - Pruebas de penetración externas (*wireless*)

- Reducción de costos
  - Proyectos de inversión
  - Uso de licencias
  - Mantenimiento
  - *Outsourcing*
  - Mantener costos competitivos en relación con un tercero
- Plataformas, sistemas, aplicaciones y desarrollos
  - Uso de los servidores
  - Capacidad de los servidores
  - Cumplimiento con regulaciones
  - Respaldo de la información
  - Plan de recuperación en caso de desastre
- Recursos humanos
  - Entrenamiento
  - Plan de cambio de ciertos puestos
  - Evaluaciones de actuación

Sin embargo, los indicadores del desempeño deben desarrollarse a la medida de las operaciones de la entidad de que se trate, ya que éstos se alinearán a las estrategias y los objetivos que persiga y éstos le proporcionarán la información que permita evaluar el alcance de los mismos. Lo anterior se logrará al medir la eficiencia, la eficacia, los efectos y el costo-beneficio de sus actividades, que para este caso en particular, sería sobre la seguridad y exposición de los riesgos que la acechan, que con ello, serviría de base para tomar las medidas correctivas necesarias.

Finalmente, es importante mencionar que los errores humanos más que los desperfectos tecnológicos son el origen de las violaciones a la seguridad. El cambio que deben hacer las organizaciones es el de fomentar una cultura de seguridad, conociendo sus efectos e impactos, lo que les permitirá conocer los riesgos en las actividades que desarrollan para poder así manejarlas de manera segura.

Desafortunadamente, en muchos casos, no se invierte en este tipo de programas y a la larga los costos por reactivar las operaciones o por robo de información, representan impactos importantes en la situación financiera de una entidad. La cultura debe cambiar para no ver estas erogaciones como gastos sino como inversiones cuyo retorno, desde mi punto de vista, es inmediato pues evitan exposiciones de riesgo a las entidades.

La era de la comunicación electrónica ha llegado y evoluciona a pasos agigantados. E-commerce era un futuro lejano que ya se materializó, por lo que el auge de la seguridad ha tomado gran importancia en el quehacer de los negocios. El que no esté preparado perecerá, ya que se encontrará vulnerable a las guerras cibernéticas de los *hackers*, a través de accesos no autorizados, virus, fraude o robo, con la intención de desaparecerlo del mercado. 



Ing. Gabriel Gálvez Betancourt  
afbmx@yahoo.com.mx

*Estudios de Maestría por el CIG-IPN, Profesor de las Academias de Informática y Computación desde 1984*



Lic. Ángel F. Brindis Nateras  
afbmx@yahoo.com.mx  
*Estudios de Maestría en Administración de Negocios, Profesor de las Academias de Tecnología Informática y de las Academias de Informática desde 1992*

# La seguridad informática en México

## Introducción

*Para tener un buen inicio de este artículo lo consideramos de notable importancia comentar que hoy en día la información bien administrada es poder, recursos económicos y oportunidades de éxito.*

En el pasado tanto a escala mundial como nacional, el término seguridad informática no era tema de gran importancia; sin embargo, al pasar los años, la delincuencia ha utilizado la tecnología informática.

Estos hechos lejos de disminuir van en aumento dramáticamente. Un factor muy importante es que en muchos casos los delincuentes cuentan con herramientas tecnológicas más sofisticadas y de mayor desempeño que los mismos cuerpos policíacos. Este aspecto en México es más latente, por lo anterior consideramos hacer un llamado de atención en este problema que cada vez es más grande y se presenta con mayor frecuencia en nuestro país.

Para tales efectos en nuestro estudio consideraremos la seguridad informática como un sinónimo de la seguridad de la información la cual clasificaremos en: datos (caracteres alfanuméricos y especiales), voz (música, audio, etc.), e imagen (fotos, videos, etcétera).

## ¿Qué es la seguridad informática en México?

Al resguardo, custodia y protección de la información durante su manejo, almacenamiento, procesamiento y envío/recepción, mediante la implementación de tecnologías que garanticen la integridad, la disponibilidad y la confidencialidad de la información.





Para poder incorporar este esquema de la integridad, confidencialidad y disponibilidad de la seguridad de la información, es necesario que se implementen varios tópicos. Algunos de los más relevantes son los siguientes:

- Seguridad de la integridad del personal.
- La seguridad física de los activos informáticos.
- La seguridad lógica de los activos informáticos.
- La seguridad en internet.
- La seguridad en el comercio electrónico.
- La seguridad en las bases de datos.
- La seguridad en el desarrollo de sistemas.
- La seguridad en las telecomunicaciones.
- La administración de riesgos.
- Vulnerabilidades.
- Amenazas.
- Controles de acceso.
- Mantenimiento del esquema.
- Planes de contingencia.
- Clasificación de la informática.
- Políticas de seguridad.
- Aspectos legales.
- Aspectos del entorno político de la empresa.
- Metodología para la encriptación de la información.
- Capacitación y concientización del personal
- Autorización e implementación del esquema por parte de la alta dirección de la empresa.

Es importante mencionar que aún implementados todos estos tópicos no es posible garantizar 100% la seguridad de la información.

### La seguridad informática en México

Es lamentable comentar que la presencia de la seguridad informática en México es prácticamente nula a nivel de la micro, pequeña y mediana empresa y si consideramos que el mayor número de empresas en México están catalogadas dentro de esta clasificación, la problemática se torna muy importante y con riesgos muy elevados que pueden poner en juego la existencia de estas empresas.

En cuanto a las empresas muy grandes y especialmente las transnacionales, podríamos decir que sí cuentan con este esquema aunque no en su totalidad.

Otro factor muy importante es la falta de una legislación en materia de seguridad informática en nuestro país.

Aunado a estos problemas el personal capacitado profesionalmente en seguridad informática en nuestro país es escaso, ya que el personal que actualmente se encarga de estos tópicos podríamos decir que tiene otras especialidades y no la formación académica en seguridad informática.

Por último, el costo de la tecnología contribuye también a que la seguridad informática en las micro, pequeñas y medianas empresas en México, no se implemente con la velocidad que hoy en día se necesita.

Si consideramos que el mayor número de fraudes, robos de información, robos de activos informáticos, etc., ocurren con el personal que labora dentro de la empresa, el problema de no contar con las medidas de seguridad informática, hacen aún más crítico el problema. Otro factor a considerar es la ubicación geográfica de nuestro país y especialmente de la ciudad de México, la cual se encuentra en una zona extremadamente sísmica; vale la pena recordar la catástrofe ocurrida el 19 de septiembre de 1985 en donde lamentablemente miles de personas murieron y de igual forma muchas empresas desaparecieron o tuvieron muchos problemas de información por no contar con un esquema de seguridad informática (planes de contingencia).

La UPIICSA ha venido trabajando en la construcción de su propio esquema de seguridad; para ello, ha participado como comité organizador junto con las Academias de Tecnología Informática para el Segundo Congreso Iberoamericano de Seguridad Informática llevado a cabo del 28 al 31 de octubre de 2003 en la ciudad de México, y en la Segunda Semana de Seguridad Informática en el IPN trabajando con la SEPI de ESIME CULHUACÁN, llevado a cabo del 26 al 30 de agosto de 2004. <http://www.portaltecinf.upiicsa.ipn.mx/congreso.htm>

### Conclusión

- Es urgente que el poder legislativo en México redacte e implemente leyes en materia de seguridad informática.
- Es necesario que a la seguridad informática en México se le dé la importancia que merece.
- Es conveniente que existan más escuelas en nuestro país a nivel profesional que forman y capacitan al alumnado en seguridad informática.
- Es indispensable que después de que sean implementados estos tópicos se les dé el mantenimiento permanente para que con esto siempre se garantice un nivel muy aceptable en la seguridad informática. 

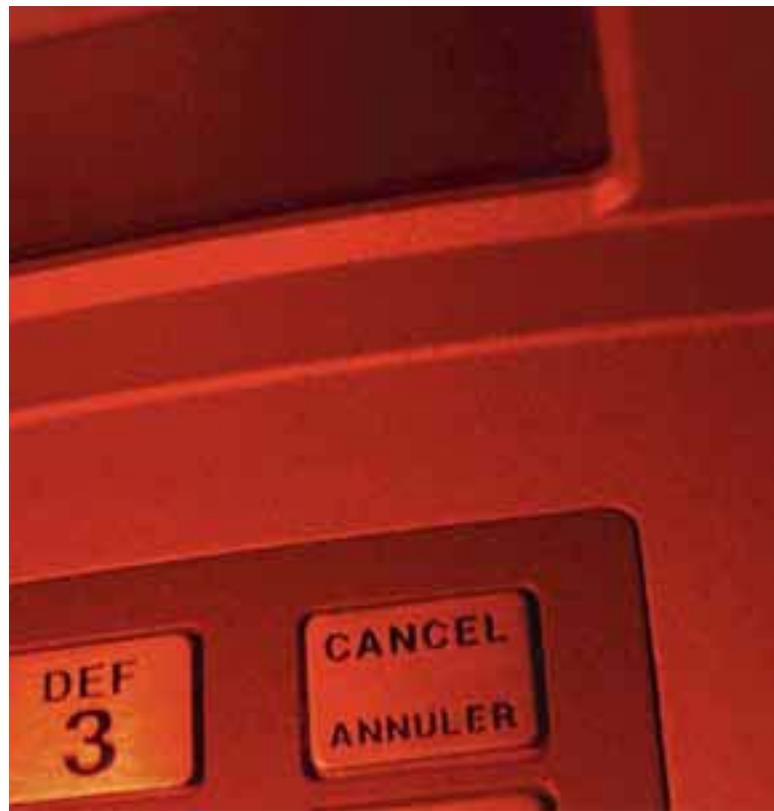


M. A. Zeuz Zamora Herrera  
zeuz.zamora@cna.gob.mx

*Auditor Adjunto de la Comisión  
Nacional del Agua*

# Auditoría de seguridad

*D*urante la historia de las sociedades, el concepto de seguridad ha incrementado su importancia, ya que día con día abarca diferentes aspectos de las actividades cotidianas y sin duda alguna, su influencia en las instituciones es de suma importancia debido a los altos índices de vulnerabilidad y daños ocasionados por la falta de una cultura al tema de la seguridad, lo que provoca un aumento en los niveles de riesgo. Se puede destacar que la seguridad impacta como problemática en aspectos organizacionales, de diseño y tecnológicos, entre otros.



En el ámbito organizacional, las instituciones con frecuencia olvidan considerar la función de seguridad de manera formal, desde su misma estructura orgánica, lo cual genera la ausencia de funciones y responsabilidades relacionadas con la misma; los canales de comunicación se tornan oscuros y discrecionales para atender los incidentes de seguridad, por lo que generalmente se basan en medios informales y poco comprobables.

Por lo anterior, se ha identificado que los esquemas de seguridad carecen de consistencia, ya que no se encuentran alineados a la organización, lo que implica que dichas actividades no están definidas en el respectivo marco de referencia que regula el funcionamiento de la organización, tales como manuales de organización, políticas, procedimientos, etc., y de forma natural,



nadie asume la responsabilidad de los riesgos, ni la implantación de medidas de seguridad, ya que generalmente se adoptan de manera parcial, una vez que el riesgo se ha materializado.

Sin embargo, la ausencia de una cultura preventiva, ocasiona que no se valoricen los beneficios inmediatos de realizar inversiones razonables en el tema de seguridad, lo que se traduce en algún momento de la existencia de la institución, en pérdidas no sólo económicas, sino de imagen.

Desde el punto de vista tecnológico, aun cuando el software y hardware son elementos de soporte a las operaciones de la institución, si no se encuentran inmersas en un proyecto de seguridad, difícilmente se obtienen los resultados esperados. Si consideramos que los avances tecnológicos no cubren 100% de las necesidades en seguridad y además existe una excesiva confianza en este tipo de soluciones, ingresamos al ámbito de “ojalá no pase nada” lo cual induce a afrontar riesgos sin conocimiento de causa.

En este orden de ideas, la situación real suele ser que en las empresas se implementan soluciones de seguridad de acuerdo con aspectos específicos, que no contemplan una adecuada definición de estrategias, normas, procedimientos, etc., que fortalezcan los sistemas de control enfocados a asumir determinado nivel de riesgo y así fortalecer la toma de decisiones correspondientes.

Actualmente, y dados los avances tecnológicos que han venido surgiendo, se constata que cada vez es más prioritario para los proveedores, legisladores, auditores, usuarios y accionistas el contar con elementos que permitan controlar y evaluar los diferentes aspectos de la tecnológica de la información, principalmente lo relacionado con la seguridad, ya que se reconoce como factor crítico para el éxito y la supervivencia de las organizaciones, que su infraestructura en tecnologías de información sea administrada efectivamente. Lo anterior, debido a que la disposición de la información sin restricciones de tiempo, distancia y velocidad, hacen que se genere una creciente dependencia en información en los sistemas que la proporcionan; que exista una gran vulnerabilidad, amenazas y ataques que están dirigidos a bloquear la información que se produce y una gran escala y el costo de las inversiones actuales para la generación y seguridad de la información.

En todo el mundo y principalmente para la mayoría de las empresas, la información y la tecnología que la soporta, representan los activos más valiosos, ya que verdaderamente la información y sus sistemas se encuentran incrustados en las mismas, desde los usuarios finales, hasta su infraestructura tecnológica.

En este sentido, las empresas tanto del sector público como del privado, han venido reconociendo los beneficios potenciales

que la tecnología puede brindar, y se ha creado una carrera desenfrenada en la que el éxito de las organizaciones, depende de cómo se comprenden, administran, regulen y se controlen los riesgos asociados con la implementación de recursos de tecnología y su vinculación con los procesos de negocios de las organizaciones.

Por lo anterior, los administradores se encuentran atados al paradigma de determinar la inversión razonable en tecnología y su control, y la forma en la cual se debe equilibrar la relación de riesgo e inversión controlada en un ambiente tecnológico, el cual es absolutamente impredecible.

Con el fin de contar con elementos que permitan mantener la relación de riesgos e inversiones controladas y en equilibrio, el concepto de control y regulación ha generado en la actualidad conceptos confusos en la tarea ardua de implementar buenos controles en tecnologías de información, los cuales soporten exitosamente la cadena de valor de cada una de las organizaciones.

Para lograr determinar una evaluación adecuada con respecto a los controles en tecnologías de información, de

manera sustancial, los auditores han tenido que tomar el liderazgo en estos esfuerzos, ya que se enfrentan cotidianamente a la necesidad de soportar y sustentar sus opiniones frente a la administración, acerca de los controles internos que garantizan razonablemente la confiabilidad de la información que en ellos que se genera y por ende el cumplimiento de sus metas y objetivos.

En este sentido, la auditoría de seguridad deberá valorar aspectos relacionados con los sistemas operativos, software comercial, de comunicaciones, de bases de datos, de proceso, de aplicaciones e indudablemente las instalaciones y aspectos físicos. A continuación se describen algunos puntos que deben contemplarse al

realizar una auditoría de seguridad,<sup>1</sup> y determinar si existen controles adecuados para proteger la integridad y confiabilidad de los equipos, software e información, contra usos y modificaciones no autorizados, por daño y/o pérdida.

### **Organizacional**

- Determinar si las responsabilidades relativas a la seguridad física y lógica se encuentran debidamente asignadas.
- Revisar las normas, políticas y procedimientos dictados para garantizar la seguridad de los activos del centro (equipo, software e información) y determinar si éstos definen claramente las responsabilidades de los usuarios, administradores y personal en general.
- Determinar si las tareas asignadas garantizan la seguridad de los activos y si son difundidas y entendidas en forma correcta. Verificar asimismo, que éstas sean consistentes con las políticas de seguridad comúnmente aceptadas.

### **Los avances tecnológicos**

**no cubren 100%**

**de las necesidades**

**en seguridad y**

**además existe una**

**excesiva confianza en este**

**tipo de soluciones**

- Determinar el grado de conocimiento general de los grupos usuario e informático sobre la importancia de la seguridad física y lógica de los activos para su adecuada salvaguarda.
- Revisar el organigrama para determinar si existe un área responsable de la administración de la seguridad e información.

## Seguridad física

### Ubicación física de las instalaciones

Determinar si la ubicación del centro de cómputo es adecuada para proteger la integridad de los activos (equipo, software e información).

Verificar que la sala de cómputo tenga una ubicación física segura, considerando que de preferencia esté ubicada en un lugar alejado de aeropuertos, instalaciones eléctricas (ej. radares, microondas, etc.), áreas urbanas en mal estado, tráfico pesado, materiales volátiles, gasolineras etcétera.

Que de preferencia esté ubicada en el centro de la construcción, es decir, no cerca de las paredes exteriores ni en el sótano ni en el último piso.

Obtener un plano de las instalaciones y realizar las siguientes acciones:

- Identificar todos los posibles accesos a las instalaciones, por ej. techos, ventanas no necesarias, etc.
- Determinar si estos accesos son restringidos por el uso de llaves, tarjetas o de otros dispositivos de seguridad.
- Si se usa una clave o cualquier otro medio que active un código interno, verificar que éste se cambie periódicamente.

Visitar la sala de cómputo y verificar que no existen señales exteriores que indiquen su ubicación a extraños.

Revisar el directorio telefónico y la documentación emitida por la organización, para asegurarse de que la ubicación la sala de cómputo no es identificable a través de ella.

### Acceso a las instalaciones

Determinar si las medidas de seguridad implementadas para regular el acceso a las instalaciones son adecuadas.

Verificar que existan procedimientos, tales como los que se describen a continuación, para regular el acceso a las instalaciones:

- Eliminar puertas no esenciales al centro de cómputo, ubicando una sola puerta de acceso con control continuo
- Colocar, donde sea necesario, un guardia o recepcionista, en el punto de entrada durante todo el tiempo que el centro de cómputo esté trabajando
- De ser posible, utilizar una sola ruta de evacuación en caso de emergencia

- Equipar todos los puntos de entrada y salida con mecanismos de control de acceso
- Restringir el acceso al área de computadoras sólo al personal autorizado
- Requerir que todas las personas autorizadas a efectuar operaciones dentro del área de computadoras se registren en una bitácora, en donde indiquen su nombre, firma, propósito y hora de entrada y de salida
- Identificar al personal autorizado a través de una credencial con fotografía
- No permitir el acceso al área de cómputo a los programadores o analistas, excepto bajo condiciones estrictas de control

Determinar si los procedimientos para prevenir el acceso de personal no autorizado, son adecuados y si se aplican en todos los accesos posibles.

Obtener una lista del personal autorizado para acceder a las instalaciones y determinar si su acceso es necesario, verificar si esta lista es regularmente revisada para decidir si el acceso de este personal sigue siendo válido.

Observar el funcionamiento de las instalaciones en diferentes oportunidades y a diversos horarios para verificar que únicamente se permite el acceso a personal autorizado.

Asegurarse de que cuando la sala de cómputo se encuentre vacía exista una vigilancia permanente, ya sea a través de observación directa o por la existencia de alarmas o monitores que prevengan el acceso no autorizado.

Realizar visitas no anunciadas al centro de cómputo, particularmente en el segundo y tercer turno, para comprobar la efectividad de las medidas de seguridad para el control de acceso.

Verificar que el acceso al equipo del centro de cómputo sólo lo realice el personal autorizado.

### Visitas guiadas

Asegurar que cualquier persona con acceso temporal, porte su identificación y se encuentre debidamente acompañada por un miembro del personal autorizado.

Verificar que existan procedimientos para identificar y acompañar a los visitantes durante el tiempo que permanezcan en las instalaciones.

Verificar que se supervisan estrechamente las visitas autorizadas, mediante mecanismos de control tales como:

- Todos los visitantes a los cuales se les otorgó permiso para realizar una visita por el centro de cómputo, deben ser acompañados por personal autorizado
- No permitir visitas en grupos difíciles de controlar
- Recuperar todas las tarjetas de identificación dadas a los visitantes



## Protección contra incendios

Determinar si las previsiones contra incendio del centro de cómputo están acordes con los estándares generalmente aceptados para tales medidas de protección.

Revisar los estándares generalmente aceptados para protección contra incendio que publican las organizaciones nacionales e internacionales y verificar si las medidas que se adoptan en el centro de cómputo están de acuerdo con estos estándares, por ejemplo:

- Que no exista material combustible en las instalaciones de la sala de cómputo
- Que los cableados eléctricos y de comunicaciones se encuentren protegidos con material aislante y bajo el piso falso
- Que la parte inferior del piso falso se encuentre en buen estado y libre de polvo
- Que exista un sistema contra incendio o que al menos haya extinguidores, así como verificar su vigencia
- Que dentro de la sala de cómputo exista señalización de evacuación de emergencia y que se realicen simulacros de evacuación periódicamente

Determinar a través de entrevistas con el administrador del centro de cómputo y sus colaboradores, qué tanto conocen y piensan que son adecuadas las medidas contra incendio del centro, comparadas contra los estándares generalmente aceptados.

Revisar ocasionalmente el seguro contra incendio de la organización para verificar su vigencia.

Requerir la apreciación del jefe de bomberos sobre lo adecuado de la póliza, de acuerdo con las medidas contra incendio implementadas en el centro y los cambios planeados.

Inspeccionar el centro de cómputo para determinar si se aplican las medidas contra incendio.

## Entrenamiento en procedimientos de seguridad y su difusión

Asegurarse de que el personal del centro de cómputo recibe entrenamiento periódico sobre procedimientos y controles de seguridad.

Verificar que el personal recibe un entrenamiento adecuado sobre los procedimientos que deberán seguir en caso de emergencia por fuego, agua o cualquier otro incidente que cause alarma.

Determinar por observación directa y entrevistas, si el personal del departamento de servicios tiene conocimiento de la ubicación de las alarmas contra incendio, extinguidores, interruptores regulares y auxiliares de electricidad, interruptores de aire acondicionado, mascarillas y cualquier otro dispositivo de emergencia que ellos pudieran usar.

## Condiciones de proceso

Verificar la existencia de equipo de aire acondicionado y si las operaciones realizadas en el centro lo ameritan, que exista otro equipo de respaldo.

Verificar que exista equipo de energía ininterrumpible (UPS) y que su mantenimiento preventivo y correctivo sea llevado por medio de una bitácora de mantenimiento.

Verificar que existan medidores de temperatura (termómetros) y ésta sea menor de 20° C y mayor de 17° C, así como medidores de humedad relativa, la que deberá ser mayor de 40 y menor de 80%.

Verificar que elementos tales como: luz solar, lluvia, viento, etc., no incidan directamente sobre los equipos de la sala de cómputo.

Verificar que los manuales de administración de los equipos estén bien protegidos y sólo puedan ser accedidos por personal autorizado.

Verificar que exista suficiente espacio físico dentro de las instalaciones de la sala de cómputo, de acuerdo con la densidad de equipos y a los planes a futuro.

## Seguridad lógica Administración de passwords

Garantizar que el acceso lógico al equipo esté restringido por procedimientos y políticas de acceso utilizando *passwords*.

Verificar que existan procedimientos autorizados para la asignación y actualización de las claves de acceso a los equipos.

Solicitar al administrador de los equipos las listas, tablas o matrices de las claves de acceso y verificar si se incluyen las claves de acceso a dispositivos periféricos (discos, impresoras, unidades de cinta, etcétera).

Revisar los procedimientos para la administración de *passwords* y determinar si:

- Están definidas de acuerdo con una norma establecida
- La solicitud y autorización se hace por escrito
- Las características de longitud, composición (que permita letras mayúsculas y minúsculas, números y caracteres especiales), encriptado, etc, son adecuadas para que éstos no sean fácilmente deducidos
- Previén que los *passwords* no sean difundidos en forma inadvertida ni desplegados durante el proceso de acceso a la red o impresos en alguna salida
- Previén que los *passwords* sean almacenados en archivos encriptados
- Contemplan políticas de cambio frecuente de éstos Por ejemplo, usar una fecha de expiración asociada a los *passwords* o limitar su uso a un número determinado de accesos para obligar su cambio
- Previén la eliminación de las claves de acceso de aquellos individuos que cesan su relación de trabajo con la empresa
- Previén la desconexión automática cuando transcurren algunos minutos de haber realizado el último acceso al sistema (última instrucción tecleada)
- Previén la suspensión del código de acceso, o la deshabilitación del equipo en caso de que haya varios intentos de acceso fallidos durante el mismo día
- Especifican la aplicación de sanciones por el mal uso de los *passwords* y divulgación de éstos a otras personas

Corroborar que el personal (operativo y usuario) está consciente de los riesgos y problemas derivados de divulgar su clave de acceso, por ejemplo, el posible mal uso de la información.

Verificar la aplicación de las sanciones especificadas en los procedimientos para la divulgación y mal uso de los *passwords*.

Determinar si los usuarios son restringidos a terminales específicas o días y horarios específicos.

Verificar que el acceso al equipo de monitoreo es controlado, mediante prácticas, tales como limitar el número de usuarios y ejercer un estricto control de las actividades que realizan.

Determinar si el departamento usuario valida periódicamente los permisos, alcance y estratificación de las claves de acceso asignadas a cada uno de sus miembros.

Comprobar que durante el proceso de información crítica se efectúan comprobaciones periódicas que permitan certificar la identidad y permanencia del usuario, mediante información que solo él conozca. Por ejemplo:

- Dirección anterior
- Fecha y/o lugar de nacimiento de algún miembro de la familia
- Color de ojos de alguien de su familia

### Acceso a la información

Asegurar que el acceso a la información está restringido con la adecuada estratificación de niveles de acceso. Determinar si los procedimientos prevén que las claves asignadas a los usuarios consideren el nivel de acceso para:

- Equipos
- Archivos
- Programas de las aplicaciones
- Comandos del sistema operativo, etcétera

Verificar la existencia de la documentación mediante la cual se justificaron las asignaciones de claves de acceso a los equipos e información.

Verificar que existan procedimientos para la asignación de claves de acceso temporal o de emergencia. Determinar si es necesario obtener una autorización especial para este tipo de accesos y si este tipo de autorizaciones se limitan a un periodo dado y si se informa de ello a la administración. Verificar que estos accesos temporales se concedan con poca frecuencia.

Verificar que los procedimientos de autorización para la ejecución de procesos cubren los siguientes elementos:

- Recursos o protección de objetos
  - Implementar autorizaciones a diferentes niveles con la finalidad de proteger adecuadamente la integridad y confidencialidad de datos y programas, por ejemplo:
    - \_ Archivos, base de datos o programas
    - \_ Un grupo particular de registros en base de datos
    - \_ Un registro en particular o categorías de registros en base de datos o archivo
    - \_ Un campo particular o categorías de campos en base de datos o archivo
    - \_ Diferentes tipos de procesos, etcétera
- Perfiles
  - Verificar que existan procedimientos para la asignación de perfiles de acceso a los sistemas

- Verificar que exista una bitácora automatizada, en la que se registren:

- \_ Todos los intentos de acceso al sistema, válidos e inválidos
- \_ Todos los requerimientos hechos al sistema para respaldar programas, datos, o transacciones
- \_ Todas las modificaciones de datos críticos o programas

- Verificar que:

- \_ Existan procedimientos para detectar las posibles violaciones
- \_ La seguridad de la bitácora está protegida
- \_ Periódicamente se revise la bitácora por el supervisor indicado

Dentro de este tipo de auditoría, se pueden considerar los siguientes tipos de análisis, los cuales realizan diferentes empresas en el mercado, entre las que destacan:

### Diagnósticos

Análisis completo de los sistemas desde internet (o test de intrusión) identificando las vulnerabilidades críticas y no críticas, así como recomendaciones de seguridad, instrucciones para arreglar las vulnerabilidades adjuntando parches de seguridad necesarios, o recomendando versiones apropiadas del software que usa el cliente.

### Monitoreo en línea

Instalación en los sistemas del cliente de un software propio para el seguimiento remoto diario de las posibles incidencias de seguridad, así como la propuesta de planes de acción de emergencia.

### Forenses

Análisis de la superficie del disco duro programados, aleatorios o puntuales (bajo sospecha de anomalía), con el fin de asegurar la integridad de los registros y de que éstos no han sido manipulados por un intruso; es decir, rastrear el uso autorizado de los datos almacenados en diferentes tipos de dispositivos.

### Sistemas de alertas y vigilancia tecnológica

Si vigilan las vulnerabilidades que afecten sistemas en operación y en caso de algún acceso no autorizado, se generan reportes de alertas a diferentes niveles descriptivos.

### Conclusión

Para lograr determinar una evaluación adecuada con respecto a los controles en tecnologías de información y en particular lo relacionado con la seguridad, de manera sustancial, los auditores han tenido que tomar el liderazgo en estos esfuerzos, ya que se enfrentan cotidianamente a la necesidad de soportar y sustentar sus opiniones frente a la administración, acerca de los controles internos que garantizan razonablemente la confiabilidad de la información que en ellos se genera y por ende el cumplimiento de sus metas y objetivos. 

1 Lista de verificación elaborada por el Área de Auditoría Interna del Órgano Interno de Control de PEMEX.



C.P.C. y C.I.A. Beatriz Castelán G.

*Directora General de Auditoría de la Contraloría General del Gobierno del D.F.*



Ing. Edmundo Rodríguez Valenzuela

*Director de Auditoría Especializada de la Contraloría General del Gobierno del D.F.*

# La seguridad informática en el Banco de México

**Entrevista con Jesús Vázquez Gómez  
Dr. en Seguridad Computacional  
Jefe de la Oficina de Seguridad Informática del  
Banco de México**

*¿Cuál es papel de la función de seguridad informática en el Banco de México?*

R. Las funciones de la Oficina de Seguridad Informática del Banco de México son variadas, éstas pueden dividirse en 4 grandes grupos: operación, monitoreo, administración y capacitación.

Estas funciones se orientan a proteger la información manejada en la infraestructura informática y a coadyuvar a la continuidad de la operación de esta infraestructura, que sustenta los procesos fundamentales del Banco.

En lo que se refiere a la operación, se administran los sistemas de seguridad que han sido implantados para proteger la infraestructura de TI, esto incluye soporte a casos específicos de los usuarios y configuraciones de nuevos requerimientos de protección.

El monitoreo consiste en verificar de forma continua el estado de seguridad en actualizaciones y configuraciones en los sistemas operativos y servicios que componen la infraestructura de TI del Banco.

Incluida en el monitoreo, y como uno de los aspectos más importantes de la función de seguridad, la detección o descubrimiento oportuno de nuevas amenazas, como pueden ser los códigos maliciosos o estrategias de ataque que se están gestando en internet. Esta actividad puede marcar la diferencia entre un día normal de operación y un día de pesadilla en el que se deben aplicar los procedimientos de recuperación. En la actualidad para atacar este problema, considerando que los nuevos ataques informáticos toman unos cuantos minutos para afectar a toda una organización, no existen estrategias precisas definidas, y por ello cada organización hace



su mejor esfuerzo revisando tanto los avisos que se presentan en internet, como revisando las alertas generadas por sus detectores de intrusión; también, pueden apoyarse en servicios de terceros (normalmente internacionales), donde los precios de alerta oportuna varían entre unos cuantos miles y hasta varios cientos de miles de dólares. El propósito final es contrarrestar en lo posible un ataque fulminante de los que ya estamos acostumbrados a escuchar cotidianamente en internet.

En lo que se refiere a la administración, las actividades se orientan a la identificación de riesgos sobre la infraestructura de TI, el análisis de los mismos y el estudio de los controles que pueden ayudar a mitigarlos. Entre estos controles, además de los controles tecnológicos (por ejemplo, *firewalls*, antivirus, detectores de intrusos y de vulnerabilidades, etc.) se considera muy necesario contar con planes de contingencia. Adicionalmente, en la administración de la seguridad, se actualiza y propone normatividad referente al buen uso de los recursos informáticos, así como a las responsabilidades que adquieren en este uso los empleados, dependiendo de su función.

La capacitación quizás sea una de las actividades donde se presenta una mayor oportunidad de mejora; actualmente se limita a difusión de artículos en la revista interna del Banco, se tiene planeado generar un manual sencillo donde se instruya a los usuarios a conocer algunas (digamos 10) medidas básicas de manejo adecuado de la información del Banco. Asimismo, habrá situaciones en que la capacitación cubra aspectos más especializados, como son: la firma electrónica, clasificación de la información, etc.

*P. ¿Desde cuándo existe la función de Seguridad Informática en Banxico?*

R. La Seguridad Informática no es un aspecto nuevo en el Banco, en el sentido de que siempre ha existido una gran preocupación en la protección a la información que se genera en las áreas de la Institución. Se puede mencionar que se han aplicado mejores prácticas y controles al respecto, desde la década de los ochenta, por ejemplo, el apego a normas internacionales del medio financiero, protección a las comunicaciones con la Banca Nacional e Internacional, respaldos y redundancia en la infraestructura informática, por mencionar algunas prácticas de antaño en Banxico.

A pesar de esta conciencia que se ha dejado sentir en la Institución por años, y del hecho de que la función de la

seguridad informática sigue estando distribuida en varias áreas, es en el año 2003 que se crea de manera formal la función de Seguridad Informática en el Banco de México. Para esta formalización, se crea una oficina con analistas especializados y certificados en seguridad informática.

*P. ¿En dónde está ubicada dentro de la organización la seguridad informática y a quién le reporta?*

R. En la jerarquía establecida en Banco de México, partiendo del estrato más alto, existe un Comité de Tecnologías de Información, que es la entidad que autoriza toda directriz en Tecnologías de Información y Seguridad Informática.

En el mismo nivel, se cuenta con un Comité de Información, que emite los lineamientos y guías para clasificar la información; asimismo, es el órgano que confirma o revierte cualquier controversia referente a la clasificación de la información de las áreas del Banco.

En este contexto, existen dos ramificaciones de la seguridad en el Banco, Seguridad Física y Seguridad Informática; la primera es responsabilidad de la Dirección de Seguridad, mientras que la segunda es responsabilidad de la Dirección de Sistemas.

En seguida, en orden descendente siguen a la Dirección de Sistemas, la Gerencia de Telecomunicaciones, la Subgerencia de Desarrollo Tecnológico de Seguridad, para llegar finalmente a la Oficina de Seguridad Informática del Banco.

Se reporta, en el orden establecido por la jerarquía, exceptuando situaciones que ameriten notificación directa a los Directores o al Comité de Tecnologías de Información (en casos de emergencia).

*P. ¿Desde su perspectiva, cuáles son los retos que enfrenta la industria en lo que se refiere a seguridad de la información?*

R. Existen diferentes retos en el entorno nacional. Por un lado, en el plano normativo, actualmente enfrentamos, sobre todo en el medio financiero y en sectores comerciales con presencia internacional, una lluvia de regulaciones y estándares producto de acuerdos internacionales, por mencionar algunas: tenemos los acuerdos de Basilea II, Sarbanes-Oxley, ISO 17799, HIPAA, etc. Existe el reto de aplicar los controles conforme a estas regulaciones y el contar con una capacidad real para verificar su implantación.

Por otro lado está la planeación de la seguridad basada en un análisis de impacto al negocio o al menos un análisis de los riesgos a los que está expuesta la organización. La mayor dificultad en general es lograr el apoyo de la alta dirección para proveer los recursos en tiempo y humanos para hacer

**Es en 2003 que se crea de manera formal la función de Seguridad Informática en el Banco de México. Para esta formalización, se crea una oficina con analistas especializados y certificados en seguridad informática**

posible este tipo de análisis, considerando a toda la organización. Con estos análisis se podrían identificar los procesos críticos de la organización, lo que haría más simple la tarea de proteger los elementos de la tecnología de información que permiten la operación de los referidos procesos.

Dado que la velocidad de propagación de códigos maliciosos ya se cuenta en decenas de minutos, y no siempre es oportuna la protección de los sistemas antivirus, de manera personal considero que se debería constituir un Organismo Nacional de Vigilancia Permanente (24x7 los 365 días del año), que alertara a los diferentes sectores del país, tan pronto se tuviera noticias de algún evento de riesgo considerable en internet, particularmente la Banca Nacional sería uno de los grandes beneficiados con este esquema de prevención. Desde luego, este esquema debe ser complementado en las empresas con esquemas y procedimientos locales de reacción inmediata.

Por último, no menos importante es la cultura en seguridad de la información; considero que México debería ya empezar a fortalecer la formación de Ingenieros con especialidad en Seguridad Informática, así como estudios de posgrado en esta área, sin olvidar que también requerimos que los futuros estudiantes de leyes conozcan sobre delitos cibernéticos y se cree una legislación adecuada para sancionarlos.

*P. En su experiencia ¿qué características debe poseer un equipo de seguridad informática?*

R. Aunque definitivamente uno quisiera contratar personal especializado en seguridad informática, que ya tuviese cierta experiencia, certificado, sin antecedentes, etc., la realidad es que en el medio son escasos, sin experiencia, ex-hackers; lo que obliga la mayoría de las veces a formarlos gradualmente dentro de la organización, iniciándolos como apoyo a servicios de seguridad ya administrados y al mismo tiempo programándoles cursos de capacitación, hasta que un tiempo después (poco más de un año) se les asigne la responsabilidad de proyectos que atiendan a nuevas necesidades.

Afortunadamente, el tema de la seguridad para la mayoría resulta apasionante, por lo que este empujón inicial mantiene una inercia que los llevará tarde o temprano a certificarse o a obtener especialidades en la materia (en este punto se constituyen como especialistas), aunado a que Banco de México promueve la capacitación de sus empleados.

*P. De manera breve, ¿cómo es atacado el tema del awareness por el área a su cargo?*

R. Gran parte del esfuerzo de awareness ha sido abordado a diferentes niveles. No podemos considerarlo aún eficiente, hay mucho por trabajar en este sentido.

A nivel institucional, publicamos un artículo mensual en la revista interna referente a la seguridad informática y al uso de las tecnologías de información con que cuenta el Banco.

A nivel de especialistas técnicos, se inició haciéndoles comentarios referentes a las vulnerabilidades y amenazas que pesaban sobre los sistemas administrados por ellos, así como el impacto que se estimaba de las mismas, invitándolos a estar siempre al día en sus actualizaciones de seguridad y en sus configuraciones. Aún sin ser algo perfecto, se han logrado grandes avances en este sentido, y ahora son los administradores quienes parecen ser los predicadores de la seguridad en la Institución.

A nivel de directivos, se les comenta acerca de los problemas que pudieran estar ocurriendo a empre-

sas similares al Banco o de gobierno en ese momento, enviándoles noticias, haciendo referencia a encuestas y reportes internacionales de seguridad. El resultado de esta concientización se ha traducido en una mayor inversión en recursos destinados a la seguridad de la información.

A nivel de analistas de seguridad informática se ha perseguido la obtención de posgrados en seguridad informática, así como certificaciones en esa área. Con el fin de estar actualizados en tecnologías, se fomenta también la especialización en ciertos productos de seguridad y la asistencia a conferencias y diplomados. 



C.P.C. y C.I.A. Beatriz Castelán García

*Directora General de Auditoría  
de la Contraloría General del  
Gobierno del D.F.*

Ing. Edmundo Rodríguez Valenzuela

*Director de Auditoría Especializada  
de la Contraloría General del  
Gobierno del D.F.*

# El reto de la seguridad de la información en México, una estrategia para abordarla

## Entrevista con el Lic. Adrián Palma Castillo Presidente de la ALAPSI

PÚBLICA  
C O N T A D U R I A  
54  
J U L I O 2 0 0 5



*L*ic. Adrián Palma, ¿qué es la ALAPSI?

R. La Asociación Latinoamericana de Profesionales en Seguridad Informática (ALAPSI) surge de la inquietud y preocupación de un grupo de profesionales relacionados con la informática, por reducir los riesgos del uso de la tecnología de la información en las organizaciones tanto públicas como privadas.

Dentro sus objetivos principales está el de promover el conocimiento mediante la capacitación y adiestramiento en seguridad informática, promover la cultura de seguridad informática de prevención y resaltar su importancia a todos los niveles en las organizaciones y en la sociedad en general, proponer políticas, normas y legislación en seguridad, estimular el libre intercambio de información entre los miembros, y ser la instancia de consulta y de referencia en cualquier iniciativa de seguridad informática en los distintos ámbitos organizacionales promoviendo prácticas que aseguren la confidencialidad, integridad y disponibilidad de los recursos informáticos de las organizaciones.

La ALAPSI es una organización relativamente joven, se constituye el 11 de julio de 1995 y es reconocida por la ISSA (International Systems Security Association), se vincula, además, con distintas asociaciones relacionadas con el tema, como son: ISACA, ASIS, FEPACEP, entre otras, con las que realiza sinergias.

La integran profesionales provenientes de distintos sectores y entornos, lo que la enriquece por su diversidad de enfoques. Contamos con personal que proviene del sector financiero (30%), proveedores de tecnología (20%), despachos de consultoría en seguridad (15%), industrias de servicios o productos (10%), instituciones gubernamentales (10%), universidades (10%) y asociaciones civiles (5%).

La asociación cuenta actualmente con 280 miembros activos.

**La ALAPSI está organizada de la siguiente forma**

Presidente	Adrián Palma, CISSP, CISA, CISM
Vicepresidente	Ezequiel Chávez
Administración	Luis Miguel Murguía, CISSP
Secretario	Gonzalo Espinosa, CISSP, CISM
Certificación	Adrián Palma CISSP, CISA, CISM
Membresías	Raúl Aguirre CISSP, CISA, CISM
Difusión	Alejandro Cerezo
Relaciones con Empresas	Clemente Topete
Relaciones con Gobierno	Andrés Velázquez, CISSP
Relaciones con Proveedores	Manuel Rayn
Relaciones con Internacionales	Miguel Ángel Alvarado, CISM
Proyectos Especiales	Antonio Quiñones, CISSP, CISA, CBCP
Transparencia	Armando Mendoza
Eventos	Roberto Gómez

*P. En su opinión, ¿representa la seguridad de la información un nuevo paradigma en las organizaciones? ¿Es un problema meramente tecnológico?*

R. Efectivamente la seguridad de la información representa un cambio en las organizaciones, el problema de la seguridad de la información es un problema de gente, por lo tanto automáticamente se vuelve un problema institucional u organizacional o de negocio, según sea el caso, en primera instancia, recayendo después en la tecnología, un gran problema para desplegar en toda una organización la seguridad es que los usuarios (a todos los niveles de la organización) no conocen su rol y responsabilidad dentro del esquema de la seguridad aunado a que el 80% de las empresas son reactivas y correctivas, en lugar de ser preventivas y proactivas a la hora de hablar de seguridad.

*P. En medio de tantas organizaciones y asociaciones relacionadas con el tema de la seguridad ¿cómo se distingue o diferencia la ALAPSI?*

R. La ALAPSI es la única asociación a nivel nacional y latinoamericano que está directamente enfocada a la seguridad de la información. La ALAPSI se distingue de las organizaciones, primeramente porque es una asociación sin fines de lucro, por ser imparcial y objetiva y no casándose con ningún tipo de empresa, institución, fabricante o proveedor de servicios, cabe señalar que la ALAPSI siempre ha sido autónoma y a diferencia de otras asociaciones donde se manejan por capítulos locales, la ALAPSI hoy día es la matriz de los distintos capítulos a nivel nacional y latinoamericano.

*P. El tema de la seguridad de la información es un tema relativamente novedoso, ¿estamos preparados para enfrentarlo? ¿Existen las normas, el marco legal, los cuadros técnicos, las empresas de seguridad para afrontar el reto que plantea el tema dentro de las organizaciones?*

El gran problema de la seguridad a nivel nacional y Latinoamérica y en algunos casos a nivel internacional es el desconocimiento real de los distintos temas de seguridad, hoy día como comentaba las organizaciones se enfocan a soluciones puntuales y totalmente reactivas y correctivas además de que la mayoría de

las organizaciones se enfocan a la cultura del producto, el problema radica en que las instituciones o empresas no saben realmente cuál es el nivel de seguridad que requiere su organización y esto es porque no se sabe cuáles son realmente los riesgos que pudieran poner en peligro la capacidad de operación, servicio y en algunos casos hasta la supervivencia de la organización.

Aunado a lo anterior, las organizaciones tienen que enfrentar el reto de exigir servicios que realmente cumplan con sus necesidades de seguridad con una alta calidad y a un costo aceptable, la pregunta obligada es: ¿cómo lograrlo?, ya que la seguridad se ve desde un punto de vista meramente tecnológico y difícilmente se involucran a todas las áreas del negocio. Recordemos que hablar de la seguridad de la información es complejo, aparentemente hablamos de intangibles, el retorno de la inversión (ROI) no es fácilmente demostrable, etc.; por eso, uno de los objetivos principales de la ALAPSI es diseminar el conocimiento, la educación, el entrenamiento y las certificaciones en seguridad (CISSP) para que las organizaciones puedan ser más asertivas a la hora de involucrarse en temas de seguridad. La ALAPSI, hoy día ofrece a sus miembros un plan de carrera dentro de la organización donde la idea es que los miembros puedan aprender reforzando y consolidando sus conocimientos en seguridad. Creemos firmemente que con el conocimiento difundido en todos los niveles de una organización podan ser mucho más eficaces y eficientes en las organizaciones a la hora de desarrollar e implementar esquemas y modelos de seguridad.

*P. ¿Cómo participa o participará ALAPSI en el establecimiento de los marcos regulatorios, normativos y legales que demanda el tema?*

R. La ALAPSI hoy día participa en distintos grupos gubernamentales que tienen que ver con el desarrollo y establecimiento de los marcos normativos y regulatorios en la administración pública, de forma consultiva como en el caso de la policía cibernética, la policía federal preventiva el grupo DC México, agencias federales para el apoyo de investigación en materia de delitos informáticos, Secretaría de Economía para la regulación de servicios de certificación, participación en las modificaciones del código de comercio en materia de la firma electrónica, etc.

Por último, me gustaría invitar a toda la gente interesada en el tema de la seguridad de la información a participar de una forma activa y proactiva en los distintos proyectos que tiene la asociación, o en su defecto, si tienen proyectos o inquietudes propias la ALAPSI con gusto los apoyará en su realización, además de que la ALAPSI ofrece beneficios como: Intercomunicación con y entre los miembros, acceso a información actual de seguridad informática, página web exclusiva para socios, capacitación para la certificación CISSP, apoyo para su desarrollo profesional, boletín acceso, bolsa de trabajo, descuentos en eventos nacionales e internacionales, y seguimiento en su desarrollo profesional. Recordemos que una asociación lo que requiere para trascender son manos para poder trabajar y el crecimiento de la asociación se logrará única y exclusivamente con la participación de más miembros.

Gracias por la entrevista. 

Para mayor información visitar la página [www.alapsi.org](http://www.alapsi.org)

Lic. Benjamín Hill Mayoral  
bhill@funcionpublica.gob.mx

*Director General Adjunto de  
Vinculación con Gobierno y  
Sociedad de la Secretaría de la  
Función Pública*

## La alianza con la sociedad, pieza fundamental para prevenir la corrupción

**L**a corrupción es un problema dinámico, que comprende un amplio espectro de causas y manifestaciones y que genera una larga cadena de costos sociales; es difícil de identificar, de explicar y de

medir, se presenta en todos los ámbitos de la sociedad y sus causas responden a problemas culturales, institucionales y económicos.

Durante muchos años, en México y en otros países de América Latina, las estrategias anticorrupción de los gobiernos se centraron en acumular controles y normas, seguidos de mecanismos correctivos y sanciones para inhibir la corrupción. Con el tiempo, la proliferación de controles se convirtió en un obstáculo para la operación eficiente de los gobiernos y, en algunos casos, el exceso de trámites favorecía a la corrupción, en vez de evitarla.

Sin abandonar la aplicación de sanciones, el control y la vigilancia, los nuevos paradigmas en el combate a la corrupción están orientados a la racionalización de esos controles y a privilegiar mecanismos preventivos, ya que es más efectivo y eficiente prevenir la comisión de actos de corrupción que concentrar todos los esfuerzos en investigar, identificar, sancionar y corregir las faltas, una vez que se han presentado.

Combatir la corrupción y promover la transparencia es indispensable para impulsar el desarrollo de un país. Las instituciones financieras internacionales, inversionistas, empresas calificadoras y grandes bancos están concediendo cada vez mayor atención al desempeño de los gobiernos en el combate a la corrupción como un indicador que determina el ambiente para la inversión y la competitivi-

dad. Los gobiernos que no obtengan buenos resultados en la promoción de la transparencia, no tendrán las mismas oportunidades de competir por fuentes de inversión.

El establecimiento de una vinculación cercana y permanente con la sociedad es un elemento fundamental de la estrategia de cualquier gobierno en el combate a la corrupción. En todos los programas anticorrupción que han tenido éxito internacionalmente, la participación de los ciudadanos se revela como un factor clave e indispensable. Un programa anticorrupción no puede funcionar sin involucrar a la ciudadanía y poner en marcha una estrategia de cambio cultural en favor de la transparencia.

De acuerdo con la Organización de las Naciones Unidas<sup>1</sup>, la prevención por medio de la generación de conciencia sobre los costos de la corrupción es una estrategia que debe acompañar a los mecanismos de identificación y sanción para que éstos puedan ser efectivos.

En un sistema democrático de gobierno, la participación de la sociedad es fundamental para prevenir la corrupción y asegurar el funcionamiento de los mecanismos de rendición de cuentas de los gobernantes. Muchos expertos en combate a la corrupción coinciden en que “la rendición de cuentas es una relación de dos vías entre servidores públicos y la sociedad. Si bien existe la obligación constitucional de los servidores públicos de cumplir la ley, los ciudadanos deben asegurarse de que aquellos rindan cuentas.”<sup>2</sup>





Investigadores del Banco Mundial, con base en observaciones hechas en casos exitosos de combate a la corrupción de varios países, concluyen que “involucrar a los ciudadanos en el diseño de políticas públicas puede reducir la corrupción y aumentar la eficiencia, la equidad y la transparencia.”<sup>3</sup>

Experiencias como las de Palermo, Seúl, Nueva York, Bogotá y otros gobiernos locales y nacionales en los que se involucró a los ciudadanos para denunciar los delitos, monitorear los servicios del gobierno y participar en el diseño de estrategias de combate a la corrupción, han fortalecido la evidencia de que existe una relación directa y positiva entre la efectividad de las políticas anti-corrupción y la participación ciudadana.

Cuando los ciudadanos se involucran, ejercitan su voz y demandan rendición de cuentas, se echa a andar una dinámica social en la que el desempeño del gobierno mejora y se previene la corrupción.<sup>4</sup>

Involucrar a la sociedad en el combate a la corrupción y la promoción de la transparencia significa por un lado, hacer conscientes a los ciudadanos del enorme poder que tienen para ayudar a romper un eslabón de la cadena de la corrupción, y por el otro, lograr su participación en la construcción de una cultura de transparencia y cambiar los referentes culturales y sociales que permiten que la corrupción siga siendo parte de la vida cotidiana de los mexicanos.

La conformación de organizaciones de la sociedad como Transparencia Mexicana, CIMTRA, LIMAC, el Colectivo por la Transparencia y el Observatorio para la Transparencia, interesadas en el impulso de la transparencia, junto con otras organizaciones como Alianza Cívica, que han hecho suya esa tarea, son muestra de la profundidad del cambio de actitud de la sociedad mexicana acerca de que el combate a la corrupción no es ya un asunto que incumbe solamente a los gobiernos. La construcción de un México más transparente es ahora una labor que emprenden de forma corresponsable la sociedad y el gobierno.

Coinciden en el tiempo con este cambio de actitud, profundas transformaciones legales impulsadas en esta administración y apoyadas por la sociedad, que trastocan materialmente los puntos de referencia en la relación entre gobierno y ciudadano. La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental aprobada en 2002, representa un salto en la consolidación de los mecanismos democráticos de rendición de cuentas.

Durante los dos primeros años de vigencia de la Ley de Transparencia se recibieron cerca de 70 mil solicitudes de información por parte de la sociedad mexicana, lo que refleja la enorme demanda acumulada por conocer la información que se genera dentro del gobierno, así como el buen recibimiento que ha tenido este mecanismo de transparencia.

La obtención del derecho a preguntar al gobierno cualquier cosa y tener los mecanismos para obtener la respuesta es, después del sufragio efectivo, la reforma democrática más importante de nuestra historia. La información es poder, y si la información del gobierno se hace accesible a los ciudadanos, éstos adquieren necesariamente un mayor control sobre el gobierno; el poder se redistribuye colectivamente y los gobernantes dejan de tener un control monopólico sobre la información.

En sociedades libres con ciudadanos que tienen el poder de llamar a cuentas a sus gobiernos periódicamente en las elecciones y de forma constante mediante mecanismos de acceso a la información, cada una de nuestras acciones a favor de la transparencia cuenta y tiene un impacto real.

Cuando un tema como la transparencia se encuentra tan profundamente integrado en el interés de la sociedad; cuando existen mecanismos institucionales que aseguran al ciudadano el derecho a la información del gobierno; cuando la transparencia forma parte inseparable de la agenda pública, la participación ciudadana en el combate a la corrupción no solamente se vuelve más importante: se convierte en una realidad necesaria.

El derecho a contar con un gobierno que informa y que rinde cuentas es corolario natural del derecho a elegir libremente a los gobernantes. Con la participación ciudadana se cierra el círculo democrático que inicia con las elecciones y se extiende a la celebración de un pacto de honestidad entre el gobierno y los ciudadanos, en el que ambos son protagonistas activos y corresponsables en el combate a la corrupción y en la construcción de una cultura de integridad y transparencia. 

- 1 Global Programme Against Corruption, Anti-Corruption Toolkit.
- 2 Colm Allan, Civil Society and Public Accountability: The need for active monitoring, 9th International Anti-Corruption Conference, 10-15 October 1999, Durban, South Africa.
- 3 González de Asís, María. “México contra la Corrupción: Dejemos de ser Indiferentes”, Ponencia presentada en el panel “Prevención y Combate a la Corrupción a Nivel Local”, Instituto del Banco Mundial, Ciudad de México, 15-19 de abril, 2002.
- 4 “A Framework for Empowerment: Summary, Poverty Reduction Group”, World Bank, May 2002.

# Enfrentemos con éxito el reto de elevar la calidad de nuestros servicios

**U**no de los temas más controvertidos de los últimos años está relacionado con la calidad de los servicios prestados por los auditores externos y con la pérdida de confianza del público en la información financiera dictaminada.

En mayo de 1988 (cuando yo participaba por primera ocasión en esta entrañable Comisión normativa de nuestra profesión), se promulgó el primer boletín mexicano en materia de control de calidad de las firmas de Contadores Públicos, el Boletín B-02 denominado "Control de calidad del trabajo de auditoría de estados financieros". Como su nombre lo señalaba tenía el objetivo central de establecer y explicar los procedimientos para la aplicación práctica de los pronunciamientos relativos al control de calidad del trabajo de auditoría de estados financieros. Años después, se convirtió en el Boletín 3020 (bajo la nueva clasificación decimal), cuya última actualización de su contenido entró en vigor en el año 2002.

Este primer Boletín estuvo inspirado básicamente en la norma internacional de auditoría correspondiente, la ISA 7 "Control of the Quality of Audit Work", emitida por la Federación Internacional de Contadores (IFAC), desde septiembre de 1981 (hoy ISA 220). Reconocía que controlar la calidad de los servicios de auditoría era esencial para mantener los altos estándares de la profesión, distinguiendo los controles sobre los trabajos individuales de los controles generales de calidad adoptados por la firmas de auditoría.

Desde aquel entonces, el control de calidad se consideraba como un concepto amplio que debería incluir políticas y procedimientos sobre la independencia del Contador Público y su personal con respecto a su cliente, los sistemas para reclutamiento y contratación de personal, los planes de educación profesional continua, los sistemas de promoción de personal, los planes de asignación de personal a los trabajos de auditoría, los sistemas de investigación y consulta en casos especiales, los sistemas de planeación, ejecución y supervisión de los trabajos, las reglas para la aceptación y conservación de clientes, así como los sistemas de inspección para comprobar el cumplimiento de los procedimientos establecidos en materia de control de calidad.

Como es sabido por todos, nuestra profesión organizada, tanto a escala internacional como nacional, siempre ha estado consciente de la enorme importancia que tiene el hecho de que sus miembros presten servicios de calidad que fortalezcan la confianza de los usuarios de dichos servicios, por lo cual desde hace muchos años se ha autoimpuesto la obligación, no sólo de emitir una serie de normas que permitan contar con políticas y procedimientos de calidad (sistema integral de control de calidad) para los individuos y firmas prestadoras de servicios de audito-

ría, sino, además, establecer programas de vigilancia que aseguren el adecuado cumplimiento de dichos estándares de calidad.

Lamentablemente, los recientes escándalos financieros ocurridos en Estados Unidos de América y en algunos países europeos, a partir del año 2001 han puesto en entredicho la transparencia de la información financiera de las empresas públicas (cotizadas en bolsa), las medidas de gobierno corporativo adoptadas, la integridad de la alta dirección de dichas empresas y sus analistas, así como el grado de independencia y nivel de calidad de los servicios prestados por los auditores externos.

Esto ha provocado una sobre reacción en muchos países del mundo, ocasionando que las autoridades regulatorias hayan desarrollado una serie de medidas enérgicas, para proteger los intereses del público inversionista y recuperar su confianza en los mercados de dinero y de capitales. Sin lugar a dudas, Estados Unidos es el país en que se han tomado las medidas más drásticas que, de hecho, han servido de modelo y fuente de inspiración para muchos otros países. Dentro de dichas medidas, cabe destacar la promulgación de la nueva Ley Sarbanes-Oxley en julio de 2002 y el establecimiento de un organismo de vigilancia para las empresas públicas y sus auditores externos, denomi-

nado Public Company Accounting Oversight Board (PCAOB).

En mi ya larga trayectoria profesional de más de tres décadas, he tenido la enorme fortuna de estar estrechamente vinculado a cuestiones normativas de nuestra profesión, entre las cuales destaca el estar participando hoy en día como coordinador desde hace más de dos años en un grupo de trabajo plural (llamado Grupo Ad-Hoc), auspiciado por el Instituto Mexicano de Contadores Públicos y apoyado por las autoridades regulatorias de nuestro país (CNBV, CNSF y CONSAR), así como por diferentes agrupaciones empresariales que tiene como propósito central sentar las bases del funcionamiento de un organismo de vigilancia del control de calidad de las firmas de Contadores Públicos, que no sea una réplica de lo que está ocurriendo en el extranjero, sino que esté acorde con las circunstancias y realidad de nuestro país, pero cumpliendo con los estándares internacionales establecidos hasta la fecha.

A continuación haré una breve reseña de los principales avances logrados por este grupo de trabajo hasta la fecha, resaltando que el objetivo final es que este organismo comience a funcionar a partir del presente año de 2005.

Después de varios meses de análisis y amplias deliberaciones, se tomó la decisión fundamental de que la revisión de la calidad de las firmas de auditores en México se llevara a cabo mediante un organismo independiente, en cuyos órganos de gobierno participaran las autoridades regulatorias, los organismos empresariales y representantes del Instituto Mexicano de Contadores Públicos. Además, también se decidió que dicho organismo no emitiría normatividad profesional y regulatoria en materia de control de calidad, principios de contabilidad, normas de auditoría y ética, sino que se aplicaría la que estuviera emitida por el Instituto, el CINIF y por las autoridades antes mencionadas; asimismo, tampoco impondría sanciones en caso de encontrar incumplimiento con disposiciones profesionales y regulatorias, sino que esto sería responsabilidad de las autoridades y de las juntas de honor de los colegios federados de nuestro Instituto que correspondan.

Cabe señalar que, recientemente (en el año 2004), se hicieron algunas modificaciones al contenido de los estatutos y del Código de Ética Profesional del Instituto para contemplar la obligación de sus miembros

**El objetivo final del organismo de vigilancia es que comience a funcionar a partir del presente año de 2005**

de sujetarse a las revisiones de control de calidad que pudiera llevar a cabo el organismo independiente por constituirse o el propio Instituto.

A la fecha ya se tienen preparados los borradores de sus estatutos y de los reglamentos operativos de las comisiones técnicas y administradora, así como de las propias revisiones y el programa de trabajo de las revisiones iniciales, estando en proceso el código de conducta respectivo. Asimismo, existe un folleto descriptivo de la organización, características y funcionamiento del organismo.

Las firmas de Contadores Públicos que decidan sujetarse al programa de revisiones, deberán estar registradas en el organismo, una vez que hayan cumplido con una serie de requisitos establecidos en el instructivo correspondiente.

En relación con las revisiones del organismo, se tiene en consideración que, estarían enfocadas básicamente a verificar que el sistema integral de control de calidad que tengan establecidas las firmas de Contadores Públicos (registradas en el organismo), cumplan con la normatividad correspondiente. Dichas revisiones serían complementadas con revisiones de ciertos trabajos individuales (auditorías) para vigilar el estricto cumplimiento con las disposiciones profesionales y regulatorias aplicables. Dichos trabajos, en principio estarían relacionados con entidades de interés público, es decir, entidades cotizadas en bolsa y entidades del sistema financiero (bancos, casas de bolsa, sofoles, organizaciones auxiliares de crédito, aseguradoras, afores, etcétera). Por otra parte, también se podrán llevar a cabo revisiones de algunos trabajos específicos a solicitud expresa de las autoridades regulatorias. En el primer año de operaciones del organismo, se ha decidido que sus revisiones se limiten al sistema de control de calidad, a las que se les ha llamado genéricamente como revisiones limitadas,

sobre una muestra de firmas grandes y medianas, para las cuales ya se tiene elaborado el programa de trabajo correspondiente.

Las revisiones serán realizadas por personal profesional de alto nivel, que cumpla ampliamente con requisitos personales y profesionales en materia de capacidad técnica y experiencia, independencia mental, confidencialidad y cuidado y diligencia profesionales. De acuerdo con los requerimientos de cada trabajo, el equipo de revisores estará formado básicamente por Contadores Públicos, que pudiera estar apoyado por especialistas de otras disciplinas, como ingenieros en sistemas, actuarios, abogados, entre otros, en caso de ser necesario.

Como resultado de estas revisiones el organismo deberá emitir un informe que podrá ser sin salvedades, con salvedades o con opinión negativa, así como una carta con sugerencias para fortalecer el sistema de control de calidad de la firma de auditoría revisada, o para reforzar el estricto cumplimiento de las disposiciones profesionales y regulatorias aplicables a los trabajos individuales revisados.

Como se puede apreciar, se lleva un avance considerable en el establecimiento de las bases para el funcionamiento del organismo; sin embargo, existen todavía algunas cuestiones críticas que están en proceso de definición, como son: cuáles serán las fuentes de financiamiento del organismo, quiénes ocuparán los puestos principales dentro de la organización (consejo directivo, dirección general, comisiones técnica y administradora, etc.), qué metodología y herramientas tecnológicas se utilizarán para llevar a cabo las revisiones y otras de menor relevancia.

Para concluir, quisiera recalcar el hecho de que es evidente que estamos ante la presencia de uno de los retos más grandes a que se ha enfrentado la profesión independiente mexicana en toda su larga historia, lo cual nos debe llevar al convencimiento de que tenemos que redoblar esfuerzos para elevar la calidad de los trabajos de auditoría y atestiguamiento, no sólo para pasar satisfactoriamente la dura prueba de las revisiones del organismo, cumpliendo cabalmente con el compromiso contraído por las autoridades del país y nuestra profesión con los organismos internacionales, sino también para fortalecer la confianza de los usuarios de nuestros servicios y de paso enaltecer la imagen de la Contaduría Pública. 

# Examen Uniforme de Certificación

## Resumen 1999-2004 de los 10 EUC realizados

### 1. Introducción

**A** lo largo ya de los siete años de iniciado el proceso de certificación (1º de mayo de 1998), es pertinente hacer, de nueva cuenta, un análisis de las estadísticas de los profesionistas certificados, así como de los resultados que arroja el Examen Uniforme de Certificación (EUC), para enterar al público, en general, acerca de los avances en esta materia, con el fin de motivar al interesado en la presentación del examen y proporcionar al estudioso información valiosa para la realización de sus trabajos.

Este artículo presenta los números de los EUC que, a la fecha, se han presentado, con las cifras más relevantes en aspectos tales como: el número de sustentantes y aprobados, las regiones y los colegios a los que están adscritos, las universidades de las cuales han egresado, su sexo y edad, así como el sector laboral al que pertenecen, con su correspondiente relación de aprobados/ sustentantes.

### 2. Exámenes, aplicaciones y sedes, sustentantes

A partir de 1999, el EUC se ha aplicado con toda regularidad. Los dos primeros años con un examen anual, en el mes de julio y, a partir de 2001, con dos exámenes anuales, en julio y diciembre. Lo anterior nos lleva a un total de 10 EUC celebrados a la fecha. Pero estos 10 EUC han ido, generalmente, incrementando sus aplicaciones y sustentantes, como se muestra en la tabla 1.

**T a b l a 1**  
**EUC 1999 - 2004**  
Exámenes, aplicaciones y sustentantes

Núm.	Año	Núm. de exámenes	Aplicaciones (Cd. sede)	Sustentantes
1	1999	1	2	105
2	2000	1	3	172
3	2001	2	15	787
4	2002	2	12	617
5	2003	2	13	621
6	2004	2	18	1,080
	Total	10	63	3,382

La tabla 1 nos indica la secuencia del desarrollo de los 10 exámenes llevados a cabo, y nos muestra que el primer examen se efectuó en dos ciudades simultáneamente (esto es, que hubo dos aplicaciones), en donde hubo un total de 105 sustentantes. En el se-

gundo año, el EUC se aplicó en tres ciudades, con un total de 172 sustentantes, y así sucesivamente, hasta el último año, en el cual se observa que el EUC se aplicó en 18 ciudades, y que tuvo un total de 1,080 sustentantes.

El total indica que los 10 EUC se han aplicado 63 veces y que han reunido a 3,382 sustentantes.

La tabla 2 nos muestra las ciudades que en mayor número de ocasiones han sido sede del EUC, porque los colegios organizadores han reunido en su ciudad a, por lo menos, 30 sustentantes. La Ciudad de México ha sido sede las 10 ocasiones en que se ha realizado el EUC, seguida muy de cerca por Monterrey (ocho veces). Complementan la tabla: Ciudad del Carmen, Hermosillo y Mérida (cuatro ocasiones), y Guadalajara y Veracruz (tres veces).

**T a b l a 2**  
**EUC 1999 - 2004**  
Ciudades con mayor número de aplicaciones

Núm.	Ciudades sede	Número de aplicaciones
1	Ciudad de México	10
2	Monterrey	8
3-5	Ciudad del Carmen	4
3-5	Hermosillo	4
3-5	Mérida	4
6-7	Guadalajara	3
6-7	Veracruz	3

### 3. Sustentantes y aprobados

Se menciona muchas veces que casi nadie aprueba el EUC, sin embargo, las estadísticas nos muestran que año tras año se incrementa el número de aprobados del EUC, como se observa en la tabla 3.

**EUC 1999 - 2004***Sustentantes y aprobados*

Núm.	Año	Sustentantes	Aprobados	Porcentaje de aprobación
1	1999	105	32	30.48 %
2	2000	172	58	33.72 %
3	2001	787	329	41.80 %
4	2002	617	258	41.82 %
5	2003	621	275	44.28 %
6	2004	1,080	504	46.67 %
	Total	3,382	1,456	43.05 %

**4. Aprobados por colegio**

Nos concentraremos, a partir de ahora, en los aprobados y, por tanto, en los Contadores Públicos Certificados mediante el EUC. El siguiente cuadro presenta los 10 colegios con el mayor número de certificados.

**EUC 1999 - 2004***Colegios con mayor número de certificados*

Núm.	Colegio	Total
1	México	501
2	Nuevo León	167
3	Guadalajara	78
4	Yucatán	64
5	Puebla	44
6	Baja California	31
7	Sonora	28
8	León	26

Además de los colegios de la tabla 4, también superan los 20 aprobados los colegios de Michoacán, Mexicali, Ciudad Victoria y Cd. Juárez.

En cuanto al porcentaje de aprobados, por colegio, en relación con los sustentantes que han presentado el examen (sin considerar a los colegios con número menor a 18 sustentantes, por no ser representativos del porcentaje de participación y aprobación), los 10 primeros colegios, que además superan el promedio general de aprobación de 43.05% de los 10 exámenes, se muestran en la tabla 5.

Otros colegios que, dentro del estándar del número de sustentantes establecido para la tabla 5, superan el promedio general de aprobación del EUC, son: Mexicali, Ensenada, Querétaro y Tabasco.

**EUC 1999 - 2004***Colegios con mayor relación aprobados/sustentantes*

Núm.	Colegio	Sustes.	Aprobados	Relación aprobados / Sustes.
1	Cancún	28	18	64.29 %
2	Michoacán	38	23	60.53 %
3	Yucatán	108	64	59.26 %
4	Guadalajara	138	78	56.52 %
5	México	928	501	53.99 %
6	Saltillo	19	10	52.63 %
7	Nuevo León	326	167	51.23 %
8	Ciudad Victoria	42	21	50.00 %
9	Celaya	50	24	48.00 %
10	Ciudad Juárez	44	21	47.73 %

**5. Aprobados por región**

El Instituto Mexicano de Contadores Públicos, A. C. (IMCP) ha dividido a sus 61 colegios afiliados en cinco zonas estratégicas en todo el país. Conforme a esta clasificación, la tabla 6 señala las cinco regiones, clasificadas por número de aprobados en los exámenes, más los no socios del IMCP que también aprobaron el EUC.

**EUC 1999 - 2004***Certificados por región*

Núm.	Región	Total	Porcentaje de certificados
1	Centro	538	36.95 %
2	Noreste	288	19.78 %
3	Centro Occidente	215	14.77 %
4	Centro-Istmo-Peninsular	199	13.67 %
5	Noroeste	131	9.00 %
	Subtotal	1,371	94.16 %
	No socios	85	5.84 %
	Total	1,456	100.00 %

La tabla 6 resalta que más de la tercera parte de los certificados mediante el EUC pertenecen a la Región Centro y que una quinta parte de los aprobados son de la Región Noreste.

El porcentaje de aprobados, en relación con los sustentantes del EUC en la tabla 7, nos muestra el orden en que figuran las regiones, en donde se observa que tres de ellas (Centro, Centro Occidente y Noreste) superan el promedio general de aprobación.

**EUC 1999 - 2004***Relación aprobados / sustentantes por región*

Núm.	Región	Sustes.	Aprobados	Relación aprobados / Sustes.
1	Centro	1071	538	50.23 %
2	Centro Occidente	448	215	47.99 %
3	Noreste	652	288	44.17 %
4	Noroeste	391	131	33.50 %
5	Centro Istmo Peninsular	614	199	32.41 %
	Subtotal	3,176	1,371	43.17 %
	No socios	206	85	41.26 %
	Total	3,382	1,456	43.05 %

Es curioso que la región Centro-Istmo-Peninsular, pese a tener dos colegios en los tres primeros lugares de la tabla 5, colegios con el mayor porcentaje de aprobados, se encuentra en el quinto sitio de las regiones.

**6. Aprobados por sexo**

Aún es considerablemente mayor el número de aprobados del género masculino (que también está relacionado con la cantidad de sustentantes de este género) que el del femenino en el EUC. La tabla 8 nos muestra que más de 76% de los Contadores Públicos Certificados mediante el EUC son varones.

**EUC 1999 - 2004***Certificados por sexo*

Núm.	Sexo	Total	Porcentaje de certificados
1	Masculino	1,117	76.72 %
2	Femenino	339	26.28 %
	Total	1,456	100.00 %

En cuanto al porcentaje de aprobados por sexo, en relación con el número de sustentantes, también es mayor el correspondiente al masculino, como lo indica la tabla 9 (*ver siguiente página*). Asimismo, el género masculino supera el promedio general de aprobación.

**7. Aprobados por edad**

En la tabla 10 se clasifica a los Contadores Públicos Certificados en cinco grupos con-

T a b l a 9

**EUC 1999 - 2004**

*Relación aprobados / sustentantes por sexo*

Núm.	Sexo	Sustes.	Aprobados	Relación aprobados/sustes.
1	Masculino	2,386	1,117	46.81 %
2	Femenino	996	339	34.04 %
	Total	3,382	1,456	43.05 %

forme a su edad. En dicha tabla se observa que el grupo que fluctúa entre los 31 y 40 años es el más numeroso en cuanto a aprobados se refiere. Este grupo representa 50% de todos los aprobados, mientras que el menor, el grupo de más de 60 años, comprende apenas 1% del total, aunque en descargo de esta cifra, diremos que el grupo en cuestión es de sólo 1.5% del total de sustentantes.

T a b l a 10

**EUC 1999 - 2004**

*Certificados por edad*

Núm.	Edad	Total	Porcentaje de aprobados
1	De 30 años o menos	357	24.52 %
2	De 31 a 40 años	736	50.55 %
3	De 41 a 50 años	269	18.48 %
4	De 51 a 60 años	80	5.49 %
5	Más de 60 años	14	0.96 %
	Total	1,456	100.00 %

En cuanto a la relación de aprobados, respecto al número de sustentantes, ésta va desde la aprobación de uno de cada dos sustentantes que se presenta al EUC, en el grupo de 30 años o menores, hasta el de uno de cada cuatro sustentantes en el grupo de más de 60 años, según se aprecia en la tabla 11.

**8. Aprobados por universidad**

En cuanto al número de aprobados por universidad o centro de educación superior, la tabla 12 nos da a conocer las universidades de las cuales han egresado el mayor número de aprobados en los EUC. Destacan considerablemente, en cantidad por sobre los demás, los egresados del Instituto Politécnico Nacional, de la Universidad Nacional Autónoma de México y de la Universidad Autónoma de Nuevo León.

La tabla 13, por su parte, muestra la relación aprobados / sustentantes con respecto

T a b l a 11

**EUC 1999 - 2004**

*Relación aprobados / sustentantes por edad*

Núm.	Edad	Sustes.	Aprobados	Relación aprobados/sustes.
1	De 30 años o menos	674	357	52.97 %
2	De 31 a 40 años	1,718	736	42.84 %
3	De 41 a 50 años	697	269	38.59 %
4	De 51 a 60 años	242	80	33.06 %
5	Más de 60 años	51	14	27.45 %
	Total	3,382	1,456	43.05 %

T a b l a 12

**EUC 1999 - 2004**

*Universidades con mayor número de certificados*

Núm.	Universidad	Total
1	Instituto Politécnico Nacional (IPN)	226
2	Universidad Nacional Autónoma de México (UNAM)	220
3	Universidad Autónoma de Nuevo León (UANL)	117
4	Universidad Autónoma de Yucatán (UAY)	69
5	Universidad Autónoma de Tamaulipas (UAT)	52
6	Instituto Tecnológico de Estudios Superiores de Monterrey (ITESM)	51
7	Escuela Bancaria Comercial (EBC)	49
8	Universidad de Guadalajara (UG)	46
9	Universidad Autónoma de Baja California (UABC)	41
10	Universidad La Salle (ULSA)	26

a las universidades de donde han egresado los Contadores Públicos Certificados. Es de señalarse que, para este efecto, sólo se consideraron las universidades que han tenido, por lo menos, 40 sustentantes. Curiosamente, estos centros de educación superior son los mismos que aparecen en la tabla 12, sólo difieren en el orden.

T a b l a 13

**EUC 1999 - 2004**

*Universidades con mayor relación aprobados/sustentantes*

Núm.	Universidad	Sustes.	Aprobados	Relación aprobados/sustes.
1	ITESM	79	51	64.56 %
2	EBC	76	49	64.47 %
3	UAY	114	69	60.53 %
4	ULSA	45	26	57.78 %
5	UG	86	46	53.49 %
6	UNAM	428	220	51.40 %
7	IPN	469	226	48.19 %
8	UANL	253	117	46.25 %
9	UABC	113	41	36.28 %
10	UAT	147	52	35.37 %

Como se observa, las primeras ocho universidades superan el promedio general de aprobación.

**9. Estadísticas por sector**

En este ámbito, es de destacarse el mayor número de Contadores Públicos Certificados del sector independiente. Los 1,033 contadores de este sector conforman 70.95% del total, lo que hace notar que este sector representa 66% del total de sustentantes.

T a b l a 14

**EUC 1999 - 2004**

*Número de aprobados por sector*

Núm.	Sector	Total	Porcentaje de aprobados
1	Independiente	1,033	70.95 %
2	Empresarial	385	26.44 %
3	Gubernamental	32	2.20 %
4	Docente	6	0.41 %
	Total	1,456	100.00 %

En cuanto al porcentaje de aprobados en relación con el número de sustentantes, el sector independiente también va a la cabeza con 46.24% de aprobación, aunque seguido muy de cerca por el sector empresarial, con 42.49%, según muestra la tabla 15.

**10. Resumen**

Como síntesis, las estadísticas de los EUC de 1999 a 2004 nos muestran lo siguiente:

**EUC 1999 - 2004**

Relación aprobados / sustentantes por sector

Núm.	Sector	Sustes.	Aprobados	Relación aprobados/sustes.
1	Independiente	2,234	1,033	46.24%
2	Empresarial	906	385	42.49%
3	Docente	31	6	19.35%
4	Gubernamental	211	32	15.17%
	Total	3,382	1,456	43.05%

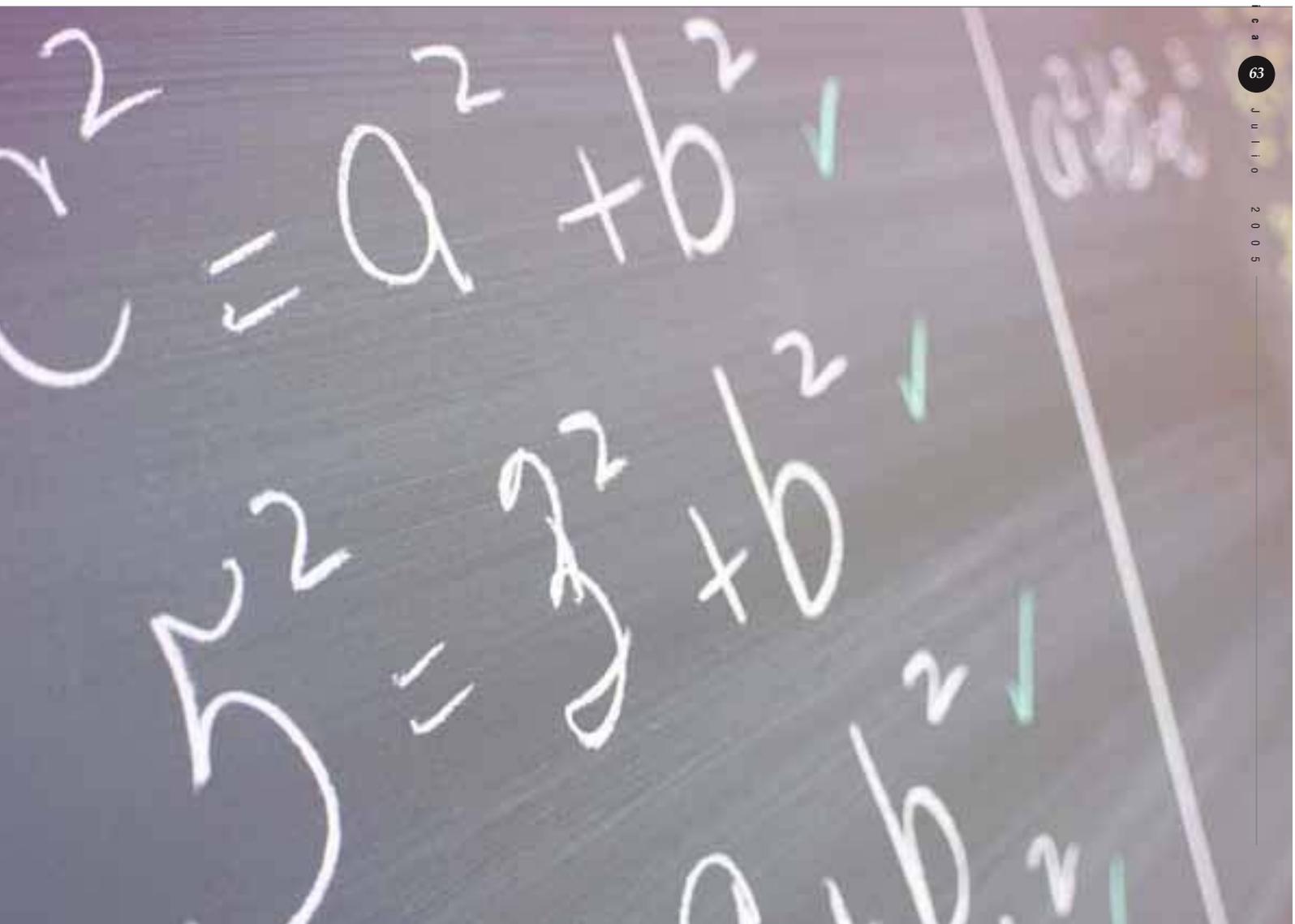
1. Se han llevado a cabo 10 EUC —con 63 aplicaciones en todo el país— en donde se han presentado 3,382 sustentantes, de los cuales aprobaron 1,456. Esto representa 43.05% de aprobación.
2. Anualmente se ha incrementado el número de sustentantes y el de aprobados del EUC. El primer examen (julio

- de 1999) fue presentado por 105 sustentantes, de los cuales aprobaron 32 (30.48%), mientras que el décimo examen (diciembre de 2004) lo presentaron 1080, y aprobaron 504 (46.67%).
3. Los colegios más grandes tienen, en general, el mayor número de certificados. Sin embargo, en cuanto al promedio de aprobación, no necesariamente cuentan con el más alto, aunque se conservan entre los primeros.
  4. El EUC es presentado tanto por socios como por no socios. De los profesionistas que han aprobado el EUC, 94.16% son socios de algún colegio federado al IMCP. El resto de los aprobados no son socios (5.84%).
  5. En cuanto a edad, el porcentaje de aprobación del EUC es inversamente proporcional a ésta: mientras que en los menores de 30 años aprueba uno de cada dos, en los mayores de 60 aprueba uno de cada cuatro.

6. Coincide que los 10 centros de educación superior con mayor número de egresados que han aprobado el EUC, sean los mismos, aunque en distinto orden, que los que tienen la mayor relación aprobados/sustentantes por universidad.
7. Del total de los Contadores Públicos que han aprobado el EUC, 70% pertenece al sector independiente, y este sector, así como el empresarial, superan por mucho —en la relación aprobados/sustentantes— a los sectores docente y gubernamental.

**Colofón**

Te invitamos a presentar el EUC y convertirte en Contador Público Certificado. El próximo EUC se llevará a cabo los días 23 y 24 de septiembre de 2005. Las ciudades sedes están por definirse. Pregunta en tu colegio o en el IMCP, al teléfono (55) 52 67 64 23 o al correo electrónico: [certificacion@imcp.org.mx](mailto:certificacion@imcp.org.mx) 



# Los abusos cibernéticos y algunas medidas preventivas

C.P.C. y C.I.A. Beatriz Castelán García

Directora General de Auditoría de la Contraloría General del Gobierno del D.F.

**L**os problemas de virus, gusanos, pérdidas de archivos, reformato total del disco duro e inclusive abuso en operaciones de e-Commerce y bancarias

son experiencias que vivimos a diario directa e indirectamente dentro de los ambientes en que nos desenvolvemos que van desde lo laboral, lo académico, lo personal, lo bancario, o cualquier otro. Lo que pocas veces nos preguntamos es si deberíamos ser más cuidadosos en el manejo de nuestros intercambios de archivos electrónicos, en la descarga de programas no oficiales, en el manejo de la internet y, desde luego, en la utilización de un antivirus actualizado para disminuir nuestra exposición a estos riesgos. Es decir, repensar y replantear el cuidado en el manejo cibernético de nuestra información.

En este sentido, a continuación se proponen algunas prácticas preventivas:

- Frente al deseo de disfrutar de los mensajes de los amigos con música, imágenes y movimiento se sugiere reflexionar en su apertura indiscriminada, pues pueden venir acompañados de virus indeseables. En general, no caiga en tentaciones a menos que conozca con seguridad la fuente.
- Ante la posibilidad de hacernos llegar sin pago o inversión algún programa, juego o software pirata hay que meditar si acaso puede venir acompañado de software espía que informe sobre: hábitos, amigos y sus direcciones, lugares electrónicos de visita y/o sobre nuestro equipo; todo ello, para cualquier efecto y fines ajenos a nuestros deseos o intereses que pueden incluir los propósitos ilícitos. Lo barato sale caro, su información es muy valiosa, no la arriesgue.
- A partir de estos contactos podremos estar sujetos al arribo de correos electrónicos basura (*spam*) que saturan nuestra máquina al recibir mensajes no deseados y, por tanto, sin nuestra autorización, lo que daña la infraestructura

de comunicación del servicio de internet y, desde luego, afectan la comunicación. Es de tal importancia el problema que, se estima, actualmente más de 60% del correo electrónico que circula por el mundo corresponde a mensajes no solicitados ni deseados. No abra estos correos, deséchelos de inmediato.

- Si usted piensa que sus operaciones de e-Commerce y las bancarias puede hacerlas sin riesgos adicionales desde su trabajo, probablemente está siendo demasiado optimista y el riesgo de que un tercero de la red donde usted labora intercepte sus mensajes, conozca datos confidenciales y los use mal, no es imaginario. Hay muchas experiencias al respecto. No incremente riesgos, haga sus operaciones de este tipo desde su máquina personal.
- Con esta orientación, evite mandar datos personales por correo electrónico. Si están solicitando datos personales, claves o números de tarjeta por correo que aparentan ser oficiales, probablemente está frente a las nuevas modalidades de fraude cibernético:
  - *Phishing*
  - *Fishing*
  - *Pharming*

Éstos persiguen direccionar al usuario a un web falso. No dé información personal, claves, ni ningún dato confidencial por correo electrónico.

- Algunas direcciones electrónicas de utilidad frente a estos problemas son:
  - [www.fraudeliminator.com](http://www.fraudeliminator.com)
  - [www.spamhaus.com](http://www.spamhaus.com)
  - [www.ashampoo.com](http://www.ashampoo.com)
  - [www.pctools.com](http://www.pctools.com)
  - [www.safer-networking.org](http://www.safer-networking.org) 

