

Factura Electrónica

Entendiendo el Sello Digital

Plan

- Comentarios y Novedades
 - Posible reducción a límite de ingresos
 - Decreto del 30 de Marzo
 - Fechas a recordar
- Entendiendo el Sello Digital
 - Suma de Números
 - Suma y Control
 - Funciones de Hash
 - Ejemplos de Hash
 - XML y Cadena Original
 - Hash SHA1 y Sello digital
 - Validación
 - Alteración y Validación
 - Componentes del Certificado de Sello Digital
 - Valores dentro de archivo KEY
 - Cambio de MD5 a SHA1

Comentarios y Novedades

Posible reducción a límite de ingresos

- <http://www.eluniversal.com.mx/finanzas/94056.html>

Podrán las pymes dar facturación electrónica

Jueves 29 de marzo de 2012

El Servicio de Administración Tributaria analiza la posibilidad de que micros, medianas y pequeñas empresas pudieran emitir facturas electrónicas.

Francisco Martínez Coss, administrador central del Servicio de Administración Tributaria (SAT), informó que **la autoridad evalúa reducir el mínimo de ingresos obligatorio para que empresas puedan emitir una factura electrónica, la cual es de 4 millones de pesos al año.**

Sin embargo, aclaró que se analizan todos los panoramas para no afectar a los contribuyentes. “Estamos revisando todas las vertientes, tipo de contribuyente, vertiente, capacidad tecnológica, de manera que como avanzamos de manera paulatina, no vamos a tomar una decisión sin antes cuidar de que quien vayamos a incluir, pueda cumplir con esto”, dijo el funcionario.

Martínez Coss dijo que debajo de los 4 millones de pesos anuales se encuentran micros, medianos y pequeños empresarios.

“Lo que estamos siendo muy cuidadosos es que bajando de este nivel podemos involucrar a sectores que no necesariamente tengan la capacidad tecnológica de atender temas de este tipo”, dijo.

El funcionario del SAT puntualizó que en el primer semestre del año se tendrá una determinación, la cual se publicaría en una miscelánea fiscal.

Posible reducción a límite de ingresos

4 millones al año equivale aproximadamente a \$11,000 pesos diarios.

2 millones al año equivale aproximadamente a \$5,500 pesos diarios.

Decreto del 30 de Marzo

- http://dof.gob.mx/nota_detalle.php?codigo=5241653&fecha=30/03/2012

(Primera Sección)

DIARIO OFICIAL

Viernes 30 de marzo de 2012

Artículo 1.17. Las personas morales obligadas a efectuar la retención del impuesto sobre la renta y del impuesto al valor agregado en los términos de los artículos 127, último párrafo y 143, penúltimo párrafo de la Ley del Impuesto sobre la Renta y 1o.-A, fracción II, inciso a) y 32, fracción V de la Ley del Impuesto al Valor Agregado, **podrán optar por no proporcionar la constancia de retención** a que se refieren dichos preceptos, siempre que la persona física que preste los servicios profesionales o haya otorgado el uso o goce temporal de bienes, **le expida un Comprobante Fiscal Digital por Internet** que cumpla con los requisitos a que se refieren los artículos 29 y 29-A del Código Fiscal de la Federación y en el comprobante se señale expresamente el monto del impuesto retenido.

Las personas físicas que expidan el comprobante fiscal digital a que se refiere el párrafo anterior, **podrán considerarlo como constancia de retención** de los impuestos sobre la renta y al valor agregado y efectuar el acreditamiento de los mismos en los términos de las disposiciones fiscales.

Lo dispuesto en este artículo **en ningún caso libera a las personas morales de efectuar**, en tiempo y forma, **la retención y entero del impuesto** de que se trate **y la presentación de las declaraciones informativas** correspondientes, en los términos de las disposiciones fiscales respecto de las personas a las que les hubieran efectuado dichas retenciones.

Decreto del 30 de Marzo

Factura Electrónica (CFDI)		Folio Fiscal: ad862d33-6934-459e-a128-bdf0393e0f44	
RFC: CRAC800914ER9		No de Serie del Certificado del CFD: 30001000000100000995	
Régimen Fiscal: Régimen de las Personas Físicas con Actividades Empresariales y Profesionales		Fecha y hora de emisión: MÉXICO D.F. 2012-01-02T20:20:00	
RFC Receptor:			
CAUR390312587			
Cantidad	Unidad de medida	Descripción del Producto	Honorarios
1	Servicio	Por concepto de: Asesoría Fiscal y Administrativa	\$2,000.00
Total con letra: Dos mil trescientos veinte pesos, 00/100 m. n.			IIVA (16%): \$320.00 Subtotal: \$2,320.00 ISR Retenido: IIVA Retenido:
Condiciones de Pago: UNA SOLA EXHIBICIÓN Forma de Pago: EFECTIVO			Total: \$2,320.00
Sello Digital del CFDI: IDSe=Edwms33YQvfmJw331CzrWbVn6STG9tKdcBdpBu2UGkU7xv70yQqWv7e8S3Smc3DpfPjO90keATffRymcdUgJ AmAKZLSBEEAJWyUUtMktBnpEwETTOH9pKctB90~Ph-C1adbuRUtHe+ Sello del SAT: pb2Qydx3w6-v4Gm3Ceqdyrd#d5907b0akcuTSF+rVCVWgwHr1bvdylitGBndruVgBVUPsdEBnuhTUUYGV1coRDGkvvhvAkx qb2oDxDr3vntufPHVnqh1SCqpd9FD5ASj3uagL5urfgLgDLVok+			
 Cadena Original del complemento de certificación digital del SAT: [1]3e9582d33-6934-459e-a128-bdf0393e0f44[2011-07-02T20:20:00+07:00Yk1N4EPk1rf3b5KYzjd3VwdkLghp oG3Uhp0EOPkSLVbzV2GLZ7X00-KF+yUp-S4p-HpawL1DEES-SvncP8at4as-e1WvcCB3ukdw/gpgph17YokH EDUtmce=ztglilng4WlnfyXOLDOB0LvazicDzTEAw=[12345678901234567890]			
No de Serie del Certificado del SAT: 30001000000100000801			
Fecha y hora de certificación: 2012-01-02T20:20:10			
Este documento es una representación impresa de un CFDI			

CONSTANCIA DE PAGOS Y RETENCIONES DEL ISR, IVA E IEPS					
PERIODO QUE ABARCA LA CONSTANCIA:			MES INICIAL	MES FINAL	EJERCICIO
			04	04	2012
DATOS DE IDENTIFICACIÓN DEL TERCERO					
1. REGISTRO FISCAL DE CONTRIBUYENTES					
CLAVE ÚNICA DE REGISTRO DE FISCACIÓN (7)					
APORTE PATRIMONIAL, RENDIMIENTO Y GANANCIAS DE PARTICIPACIÓN O					
2. DIVIDENDOS O UTILIDADES DISTRIBUIROS					
a. TIPO DE DIVIDENDO O UTILIDAD					
b. MONTO DEL DIVIDENDO O UTILIDAD					
c. MONTO DEL DIVIDENDO O UTILIDAD					
d. MONTO DEL DIVIDENDO O UTILIDAD					
3. REMANENTE DISTRIBUIBLE					
a. PORCENTAJE DE PARTICIPACIÓN					
b. MONTO DEL REMANENTE QUE LE CORRESPONDE					
4. PAGOS Y RETENCIONES					
a. CLAVE DEL PAGO (2)					
b. MONTO DEL PAGO (1)					
c. MONTO DE LA OPERACIÓN O ACTIVIDAD					
d. MONTO DE LA OPERACIÓN O ACTIVIDAD					
e. IMPUESTO RETENIDO					
5. DATOS DEL RETENEDOR					
a. REGISTRO FISCAL DE CONTRIBUYENTES					
b. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN (7)					
c. APELLIDO PATERNO (1)					
d. APELLIDO MATERNO (1)					
e. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
f. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
g. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
h. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
i. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
j. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
k. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
l. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
m. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
n. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
o. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
p. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
q. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
r. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
s. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
t. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
u. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
v. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
w. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
x. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
y. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
z. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
aa. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
ab. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
ac. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
ad. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
ae. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
af. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
ag. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
ah. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
ai. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
aj. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
ak. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
al. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
am. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
an. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
ao. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
ap. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
aq. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
ar. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
as. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
at. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
au. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
av. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
aw. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
ax. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
ay. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
az. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
ba. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bb. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bc. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bd. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
be. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bf. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bg. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bh. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bi. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bj. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bk. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bl. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bm. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bn. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bo. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bp. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bq. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
br. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bs. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bt. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bu. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bv. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bw. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bx. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
by. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
bz. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
ca. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
cb. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
cc. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
cd. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
ce. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
cf. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
cg. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
ch. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
ci. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
cj. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
ck. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
cl. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
cm. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
cn. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
co. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
cp. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
cq. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
cr. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
cs. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
ct. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
cu. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
cv. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
cw. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
cx. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
cy. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
cz. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
da. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
db. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
dc. CLAVE ÚNICA DE REGISTRO DE FISCACIÓN					
dd. CLAVE ÚNICA DE REGISTRO DE FISC					

Decreto del 30 de Marzo

- A partir del 1 de Abril 2012
- Solo CFD-**I** (con PAC)

Fechas a recordar

Décimo Octavo.

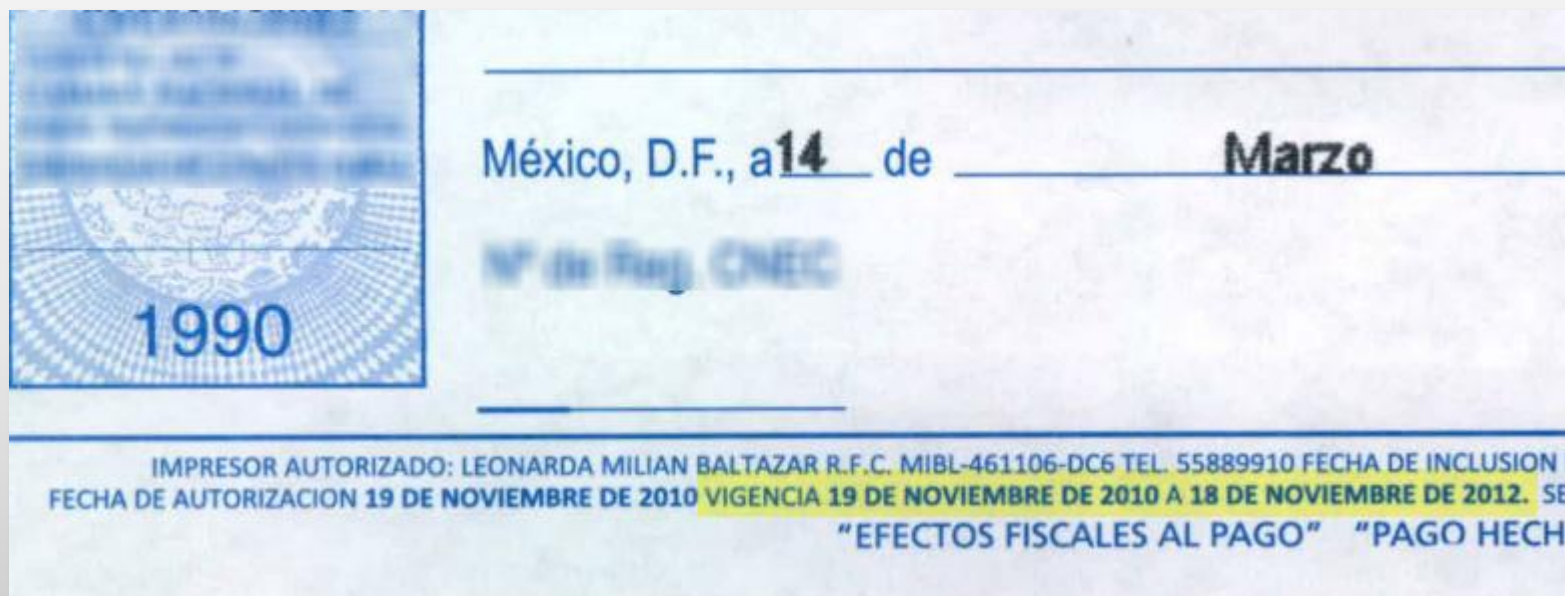
Para los efectos del Artículo Primero Transitorio del "Decreto que reforma, adiciona y deroga diversas disposiciones del Código Fiscal de la Federación", publicado en el DOF el 12 diciembre de 2011, los contribuyentes podrán emitir hasta el 30 de junio de 2012, comprobantes fiscales en los términos de los Capítulos I.2.7., I.2.8., I.2.9., II.2.5., II.2.6. y II. 2.7. de la RMF para 2011, así como sus respectivos anexos 1-A y 20, en lo concerniente a la aplicación de dichos capítulos, salvo los supuestos a que se refieren las reglas I.2.7.1.4., I.2.8.1.5., I.2.8.1.8., I.2.8.3.1., I.2.8.3.2., I.2.8.3.3. y II.2.7.1.8. de la RMF para 2011.

Los contribuyentes que se acojan a la facilidad prevista en el presente artículo deberán aplicar las especificaciones técnicas previstas en el Anexo 20 de la RMF publicado en el DOF del 23 de septiembre de 2010, pudiendo establecer en los campos relativos al nombre, denominación o razón social, domicilio fiscal del emisor y la aduana por la cual se realizó la importación, la expresión "No aplica".

Para los efectos de lo dispuesto en el párrafo anterior, los contribuyentes podrán emitir comprobantes fiscales sin incorporar los siguientes requisitos:

- I. El régimen fiscal en que tributen conforme a la Ley del ISR.
- II. La unidad de medida.
- III. Identificación del vehículo de la persona física, en tratándose de contribuyentes que cumplan sus obligaciones por conducto del coordinado y que hayan optado por pagar el impuesto individualmente.
- IV. La clave vehicular que corresponda a la versión enajenada, en tratándose de contribuyentes dedicados a la fabricación, ensamble o distribución de automóviles nuevos e importados para permanecer en forma definitiva en la franja fronteriza norte del país y en los Estados de Baja California, Baja California Sur y la región parcial del Estado de Sonora.
- V. El número, la fecha y el importe total del comprobante fiscal que se hubiese expedido por el valor total de la operación, en tratándose de pago en parcialidades.
- VI. La forma en que se realizó el pago, así como los últimos cuatro dígitos del número de la cuenta o tarjeta de crédito, de débito, de servicios o de los llamados monederos electrónicos.

Fechas a recordar



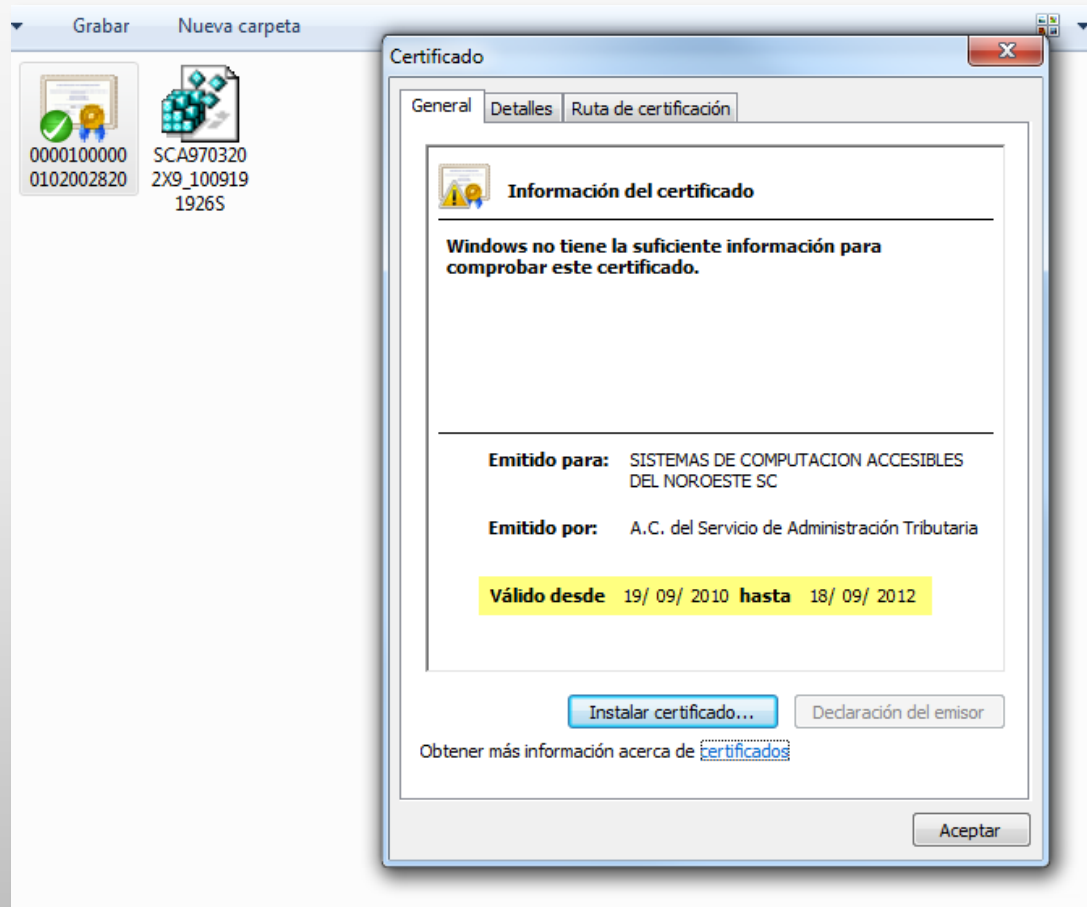
México, D.F., a **14** de **Marzo**

Nº de Reg. CNEC

1990

IMPRESOR AUTORIZADO: LEONARDA MILIAN BALTAZAR R.F.C. MIBL-461106-DC6 TEL. 55889910 FECHA DE INCLUSION E
FECHA DE AUTORIZACION 19 DE NOVIEMBRE DE 2010 VIGENCIA 19 DE NOVIEMBRE DE 2010 A 18 DE NOVIEMBRE DE 2012. SE
"EFECTOS FISCALES AL PAGO" "PAGO HECHO"

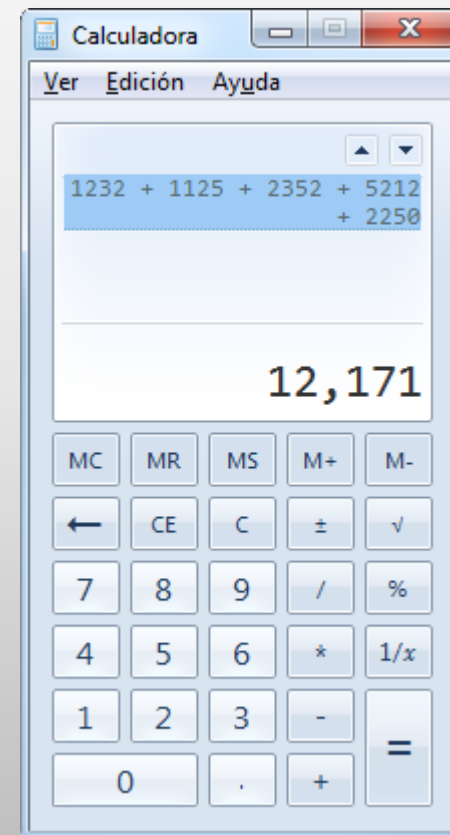
Fechas a recordar



Entendiendo el Sello Digital

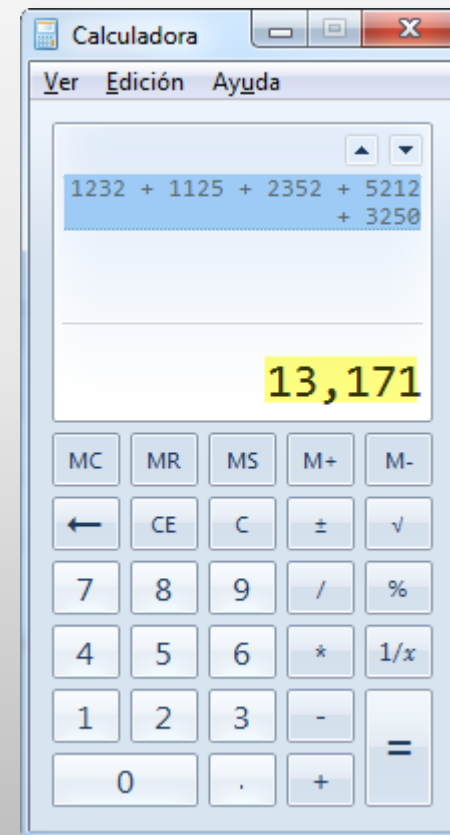
Suma de Números

Recibo 1	1,232
Recibo 2	1,125
Recibo 3	2,352
Recibo 4	5,212
Recibo 5	2,250
Suma	12,171



Suma de Números

Recibo 1	1,232
Recibo 2	1,125
Recibo 3	2,352
Recibo 4	5,212
Recibo 5	3,250
Suma	12,171



Suma y Control

Recibo 1	1,232	
Recibo 2	1,125	
Recibo 3	2,352	
Recibo 4	5,212	
Recibo 5	2,250	
Suma	12,171	
Número Secreto	823	
División	14	
Residuo	649	
$823 \times 14 + 649 = 12,170$		

Suma y Control

Recibo 1	1,232	
Recibo 2	1,125	
Recibo 3	2,352	
Recibo 4	5,212	
Recibo 5	2,250	
Suma	12,171	
Control	649	

Suma y Control

Recibo 1	1,232
Recibo 2	1,125
Recibo 3	2,352
Recibo 4	5,212
Recibo 5	3,250
Suma	13,171
Control	649

Suma	13,171
Número Secreto	823
División	16
Residuo	3
Suma	13,171
Control	3

Funciones de Hash

- “Hash” en inglés significa “chop and mix”, “picar y mezclar”
- Es un proceso que toma una lista de tamaño variable de valores y genera un nuevo valor de longitud fija.

Ejemplos de Hash con SHA1

<http://www.functions-online.com/sha1.html>

1	356a192b7913b04c54574d18c28d46e6395428ab
2	da4b9237bacccdf19c0760cab7aec4a8359010b0
AEIOU	6dc0ef3746f96a31e4353494f0d789e230992331
AEIOU	5daecd889486e7d84abc0c1622135e67e7ac6e0a
Carlos Gutiérrez	dcbdb857d9ed1bb1545d019580f509e371cb62ed
En un lugar de la Mancha, de cuyo nombre no quiero acordarme, no ha mucho tiempo que vivía un hidalgo de los de lanza en astillero, adarga antigua, rocín flaco y galgo corredor.	de185782e0813e3ae8be152ad75e2a7be28192bc

XML y Cadena Original

```
▼<Comprobante version="2.0" folio="1" fecha="2011-05-27T22:14:26" noAprobacion="14751"
anoAprobacion="2009" formaDePago="Pago en una sola exhibición"
noCertificado="300010000000100000800" subTotal="200.00" total="232.00"
tipoDeComprobante="ingreso">
  ▼<Emisor rfc="AAA010101AAA" nombre="EJEMPLO SA">
    <DomicilioFiscal calle="CALLE JUAREZ" municipio="HERMOSILLO" estado="SONORA"
    pais="MEXICO" codigoPostal="83249"/>
  </Emisor>
  ▼<Receptor rfc="XAXX010101001" nombre="PUBLICO EN GENERAL">
    <Domicilio pais="MEXICO"/>
  </Receptor>
  ▼<Conceptos>
    <Concepto cantidad="1" unidad="SERVICIO" descripcion="ASESORIA"
    valorUnitario="200.00" importe="200.00"/>
  </Conceptos>
  ▼<Impuestos totalImpuestosTrasladados="32.00">
    ▼<Traslados>
      <Traslado impuesto="IVA" tasa="16.00" importe="32.00"/>
    </Traslados>
  </Impuestos>
</Comprobante>
```

```
||2.0|1|2011-05-27T22:14:26|14751|2009|ingreso|Pago en una sola exhibición|200.00|232.00|AAA010101AAA|EJEMPLO
SA|CALLE JUAREZ|HERMOSILLO|SONORA|MEXICO|83249|XAXX010101001|PUBLICO EN
GENERAL|MEXICO|1|SERVICIO|ASESORIA|200.00|200.00|IVA|16.00|32.00|32.00||
```

Hash SHA1 y Sello Digital

||2.0|1|2011-05-27T22:14:26|14751|2009|ingreso|Pago en una sola exhibición|200.00|232.00|AAA010101AAA|EJEMPLO
SA|CALLE JUAREZ|HERMOSILLO|SONORA|MEXICO|83249|XAXX010101001|PUBLICO EN
GENERAL|MEXICO|1|SERVICIO|ASESORIA|200.00|200.00|IVA|16.00|32.00|32.00||

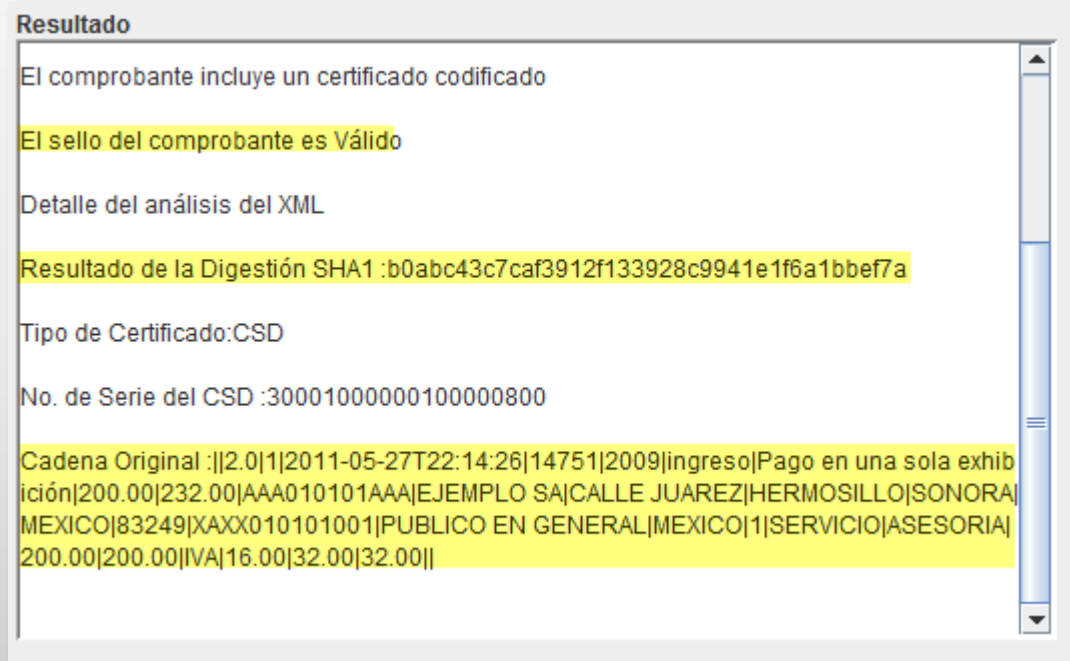
b0abc43c7caf3912f133928c9941e1f6a1bbef7a

Suma

1nAb1Bov8sHFpledw4GSxKcbEGcnd4M085hQjEhDUmx dQpX0ln4PTYW2TpxGMVCtOnxg5L6LWsiUvWTmoEWy
wnlrdznVg8mTlt3sM0wNE8yWK2l7psN4b4b49oil15xfQ0s=

Control

Validación



Alteración y Validación

```
▼<Comprobante version="2.0" folio="1" fecha="2011-05-27T22:14:26" noAprobacion="14751"
anoAprobacion="2009" formaDePago="Pago en una sola exhibición"
noCertificado="30001000000100000800" subTotal="200.00" total="232.00"
tipoDeComprobante="ingreso">
  ▼<Emisor rfc="AAA010101AAA" nombre="EJEMPLO SA">
    <DomicilioFiscal calle="CALLE JUAREZ" municipio="HERMOSILLO" estado="SONORA"
    pais="MEXICO" codigoPostal="83249"/>
  </Emisor>
  ▼<Receptor rfc="XAXX010101001" nombre="PUBLICO EN GENERAL">
    <Domicilio pais="MEXICO"/>
  </Receptor>
  ▼<Conceptos>
    <Concepto cantidad="1" unidad="SERVICIO" descripcion="ASE"
    valorUnitario="2000.00" importe="2000.00"/>
  </Conceptos>
  ▼<Impuestos totalImpuestosTrasladados="320.00">
    ▼<Traslados>
      <Traslado impuesto="IVA" tasa="16.00" importe="320.00"/>
    </Traslados>
  </Impuestos>
</Comprobante>
```

Resultado

El comprobante incluye un certificado codificado

El sello del comprobante es **Inválido**

Detalle del análisis del XML

Resultado de la Digestión SHA1 :f7684db5a54f2debf72ef11e3dbc3083ab5512a7

Tipo de Certificado:CSD

No. de Serie del CSD :30001000000100000800

Cadena Original :||2.0|1|2011-05-27T22:14:26|14751|2009|ingreso|Pago en una sola exhibición|200.00|232.00|AAA010101AAA|EJEMPLO SA|CALLE JUAREZ|HERMOSILLO|SONORA|MEXICO|83249|XAXX010101001|PUBLICO EN GENERAL|MEXICO|1|SERVICIO|ASESORIA|2000.00|2000.00|IVA|16.00|320.00|320.00||

Componentes Certificado de Sello Digital

Nombre	Fecha de modifica...	Tipo	Tamaño
00001000000101141640	29/01/2010 03:21 ...	Certificado de seguridad	2 KB
SCA9703202X9_1001291513S	29/01/2010 03:15 ...	Entradas de registro	1 KB

Propiedades: SCA9703202X9_1001291513S

General Seguridad Detalles Acronis Recovery Versiones anteriores

SCA9703202X9_1001291513S

Tipo de archivo: Entradas de registro (.key)

Se abre con: Editor del Registro

Propiedades: 00001000000101141640

General Seguridad Detalles Acronis Recovery Versiones anteriores

00001000000101141640

Tipo de archivo: Certificado de seguridad (.cer)

Se abre con: Extensiones Crypto She

Componentes Certificado de Sello Digital

Nombre	Fecha de modifica...	Tipo	Tamaño
00001000000101141640	29/01/2010 03:21 ...	Certificado de seguridad	2 KB
SCA9703202X9_1001291513S	29/01/2010 03:15 ...	Entradas de registro	1 KB

Propiedades: SCA9703202X9_1001291513S

General Seguridad Detalles Acronis Recovery Versiones anteriores

SCA9703202X9_1001291513S

Tipo de archivo: Entradas de registro (.key)

Se abre con: Editor del Registro Cambiar...

Propiedades: 00001000000101141640

General Seguridad Detalles Acronis Recovery Versiones anteriores

00001000000101141640

Tipo de archivo: Certificado de seguridad (.cer)

Se abre con: Extensiones Crypto She Cambiar...

Valores dentro de archivo KEY

Número primo 1 (P):

131441318342695122192609419937146696050066257431720060305295046455278009
515236976201499030556632518542200670205037835247855236758191588365477347
70656069477

(155 dígitos decimales)

Número primo 2 (Q):

122885062860918041082626454076587099628033581863163098712057697033712331
158567726582368246310927404030571272719288203639838195442929501955859053
03695015971

(155 dígitos decimales)

Número Público (Modulus):

161521746670640296426473658228859984306663144318152681524054709078245736
590366297248377298082656939330673286493230336261991466938596691073112968
626710792148904239628873374506302653492009810626437582587089465395941375
496004739918498276676334238241465498030036586063929902368192004233172032
080188726965600617167

(309 dígitos decimales)

Exponente:

65537

Cambio de MD5 a SHA1

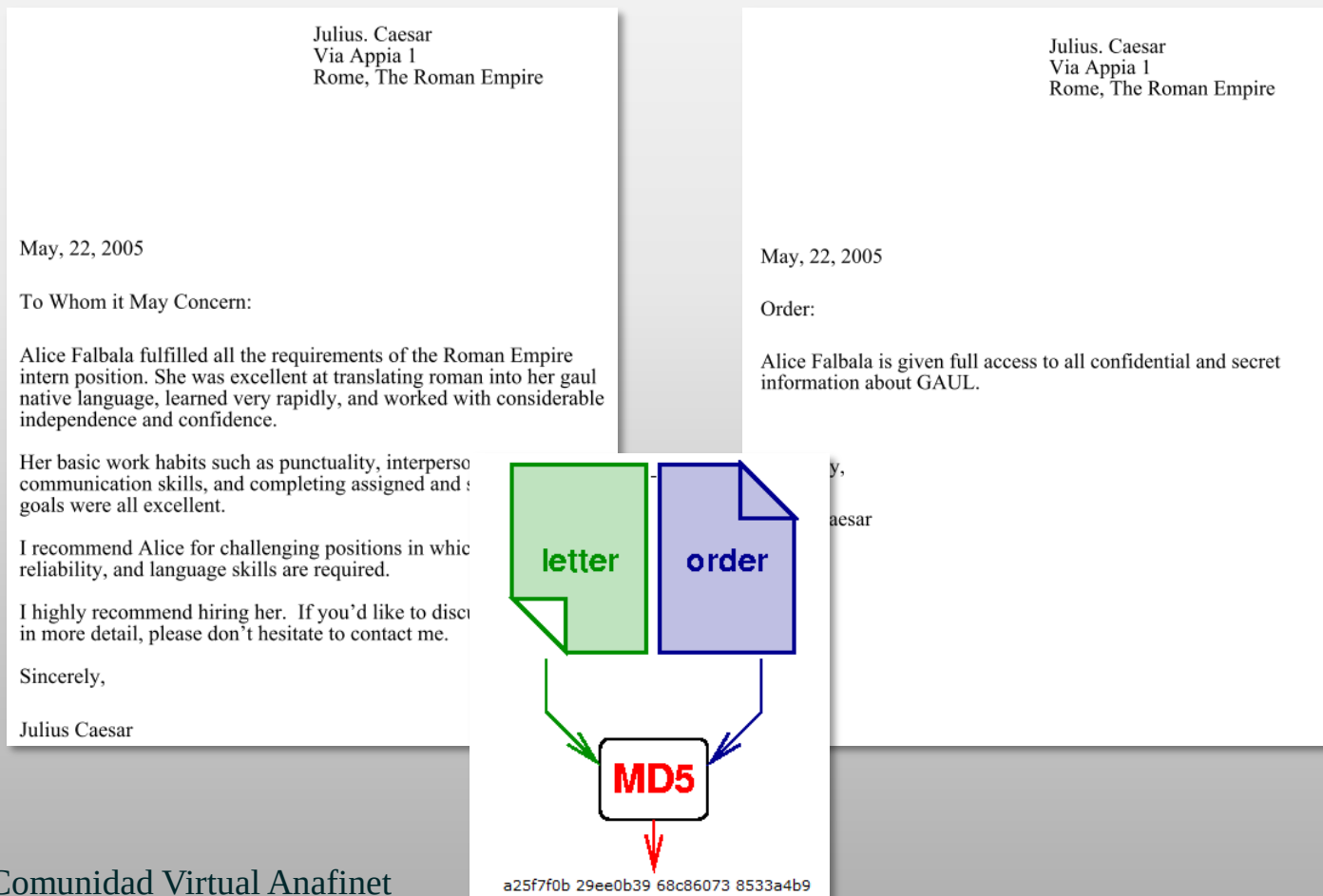
<http://www.kb.cert.org/vuls/id/836068>



The screenshot shows the US-CERT website header with the Department of Homeland Security logo and the text "US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM". Below the header is a navigation bar with links: DATABASE HOME, SEARCH, REPORT A VULNERABILITY, and HELP. The main content area features the title "Vulnerability Note VU#836068" in red, followed by the subtitle "MD5 vulnerable to collision attacks". Below this, it states "Original Release date: 31 dic 2008 | Last revised: 21 ene 2009". There are four social sharing buttons: Print, Tweet, Send (Facebook), and Share (Google+). The "Overview" section explains that weaknesses in the MD5 algorithm allow for collisions in output, enabling attackers to generate cryptographic tokens or other data that illegitimately appear to be authentic. The "Description" section begins by defining a secure cryptographic hash algorithm as one that generates a unique identifier of a fixed size (known as a "digest" or simply "hash") for a block of data of arbitrary size. It notes that the MD5 algorithm is a standard, widely used example of such an algorithm and is defined in IETF RFC 1321. It further states that one of the requirements of secure cryptographic hash algorithms is that it be extremely unlikely for two different inputs to the algorithm to generate the same digest. This property is generally referred to as *collision resistance* and cases where an algorithm generates the same digest for two different blocks of

Cambio de MD5 a SHA1

En 2005 investigadores alemanes crearon dos documentos en formato postscript totalmente diferentes que generan el mismo hash con MD5



Próxima: 23 de Abril de 2012, posible tema:
Modificaciones Abril 2012

Conversaciones sobre Factura Electrónica



Francisco Landa

<http://www.landeber.com.mx>

<http://twitter.com/landeber>



Carlos Gutiérrez

<http://carlosgutierrez.mx>

<http://twitter.com/CarlosGtrz>