NUEVA ESPECIFICACIÓN TÉCNICA DEL CÓDIGO DE CONTROL
Ver.7.0
(10.09.2007)

1. ANTECEDENTES

En el marco del Nuevo Sistema de Facturación implementado por la Administración Tributaria, se tiene prevista la incorporación de nuevos elementos de seguridad en las facturas emitidas por sistemas de facturación computarizada. En este sentido, toda factura emitida por este medio, deberá incorporar un Código de Control generado a partir de información de la misma.

A efectos del Nuevo Sistema de Facturación, solo podrán emitir facturas aquellos sistemas de facturación computarizada que tengan implementado el generador del Código de Control, estén registrados en Impuestos Nacionales, y además pasen por un proceso de certificación que verifique la correcta generación del Código de Control.

2. ¿QUE ES EL CÓDIGO DE CONTROL?

Es un dato alfanumérico generado e impreso por un sistema de facturación computarizada a tiempo de emitir una factura. Constituye una representación única de una factura, que será empleada por el SIN para que junto a otra información permitan determinar la validez o no de la misma.

Este código se genera en base a información de dosificación de la factura, información de la transacción comercial, y un dato alfanumérico denominado *Llave de Dosificación*, que el contribuyente recibirá por Internet cada vez que solicite dosificaciones de facturas para su sistema de facturación computarizada.

3. EMISIÓN DE FACTURAS A TRAVÉS DE SISTEMAS DE FACTURACIÓN COMPUTARIZADA

Todo contribuyente que requiera emitir facturas haciendo uso de un sistema de facturación computarizada, deberá previamente:

- Registrar su sistema de facturación computarizada en el SIN, llevando a cabo el trámite de *Registro de Autoimpresores* en oficinas de Impuestos Nacionales, o a través del Portal Tributario, siempre que el contribuyente sea Newton.

- Certificar la correcta generación del Código de Control, ingresando al Portal Tributario y sometiéndose a una prueba de certificación, la cual verificará que su sistema de facturación genera correctamente el Código de Control.

Una vez que su sistema de facturación esté registrado y certificado por el SIN, el contribuyente podrá:

- Solicitar dosificación de facturas para su sistema de facturación computarizada. Este trámite deberá realizarse a través del Portal Tributario, producto del mismo el contribuyente recibirá un Certificado de Activación de Dosificación, que incluirá información de la dosificación realizada.

- Recabar la *Llave de Dosificación* que el SIN asignó a su dosificación, esto a partir del Portal Tributario. Dada la sensibilidad de este dato, su conocimiento y divulgación serán de entera y absoluta responsabilidad del contribuyente.

- Configurar su sistema de facturación computarizada, ingresando información de dosificación contenida en el Certificado de Activación de Dosificación de Facturas, además de la *Llave de Dosificación* recibida.

- Finalmente, el sistema de facturación computarizada estará en condiciones de emitir las facturas dosificadas por el SIN, generando e imprimiendo en cada una el Código de Control correspondiente.

4. GENERADOR DEL CÓDIGO DE CONTROL

4.1. Algoritmos Utilizados:

Para generar un Código de Control, se hace uso de los siguientes algoritmos informáticos:

Alleged RC4	Un algoritmo de criptografía simétrica, basado en cifrado de flujo (stream cipher), muy utilizado por su rendimiento y simplicidad.
Verhoeff	Algoritmo de dígito verificador que trabaja con cadenas de dígitos decimales de cualquier tamaño. Además de detectar una amplia gama de errores en datos numéricos, este algoritmo también detecta casos de transposición de dígitos adyacentes.

Base 64	Algoritmo que convierte cifras en base 10 a base 64, utilizando divisiones sucesivas además de un diccionario de 64 caracteres. El diccionario a utilizarse para efectos del Código de Control es:
	`0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, G, H, I, J, K, L, M, N, O,`
	`P, Q, R, S, T, U, V, W, X, Y, Z, a, b, c, d, e, f, g, h, i, j, k, l, m, n,`
	`o, p, q, r, s, t, u, v, w, x, y, z, +, /`

4.2. Insumos Requeridos

Para generar un Código de Control, se requiere de la siguiente información:

Datos de dosificación	- **Número de autorización:** Dato numérico de máximo 15 dígitos. - **Número de factura:** Dato numérico de máximo 12 dígitos.
Datos de la transacción comercial	- **CI o NIT del cliente:** Dato numérico de máximo 12 dígitos. - **Fecha de la transacción:** Dato numérico de 8 dígitos, en el formato AAAAMMDD. - **Monto de la transacción:** Importe de la factura *sujeto a débito fiscal*. Solo para efectos del Código de Control, este monto deberá expresarse sin centavos, redondeado al inmediato superior a partir de los 50 centavos (Según Art. 11 de la RA Nº 05-0048-99). En el caso de Notas de Crédito – Débito, el monto a utilizarse será el de Monto Efectivo del Crédito – Débito.

Llave de Dosificación	- Llave asignada por el SIN a la dosificación solicitada por el contribuyente. Constituye la llave privada utilizada por el algoritmo de criptografía. Dato alfanumérico de hasta 256 caracteres generado a partir del siguiente diccionario:
	`A, B, C, D, E, F, G, H, I, J, K, L, M, N, P, Q, R, S, T, U, V, W, X, Y, Z,`
	`a, b, c, d, e, f, g, h, i, j, k, m, n, p, q, r, s, t, u, v, w, x, y, z, 2,`
	`3, 4, 5, 6, 7, 8, 9, =, #, (, ), *, +, -, _, \, @, [, ], {, }, %, $`

El Código de Control generado a partir de los algoritmos mencionados, será un dato alfanumérico de hasta 10 caracteres, representado en grupos de 2 separados por el caracter "-".

4.3. Proceso de generación del Código de Control

A continuación se explican en detalle los pasos a seguir para obtener el Código de Control:

Datos de Insumo

Número de Autorización:	**29040011007**
Número de Factura:	**1503**
NIT / CI del Cliente:	**4189179011**
Fecha de la Transacción:	**20070702**
Monto de la Transacción:	**2500**
Llave de Dosificación:	**9rCB7Sv4X29d)5k7N%3ab89p-3(5[A**

Paso 1

Obtener y concatenar consecutivamente 2 dígitos Verhoeff al final de los siguientes datos: Número Factura, NIT / CI del Cliente, Fecha de la Transacción y Monto de la Transacción. Posteriormente hallar la sumatoria de los datos obtenidos y sobre este resultado generar consecutivamente 5 dígitos Verhoeff. Para efectos de Verhoeff, tomar en cuenta el 0 (cero) como cualquier otro número, aún cuando este se encuentre a la izquierda de la cifra.

```
      Número de Factura:                 150312
   NIT / CI del Cliente:            418917901158
Fecha de la Transacción:              2007070201
Monto de la Transacción:                250031
                                  ---------------
                                  420925371702

     5 dígitos Verhoeff:      420925371702 71621 -> 71621
```

Paso 2

Tomando cada uno de los 5 dígitos Verhoeff obtenidos, recuperar de la Llave de Dosificación 5 cadenas adyacentes, cada una con un largo definido por el dígito Verhoeff correspondiente más 1. Concatenar la primera cadena obtenida al final del dato relacionado al Número de Autorización; la segunda al Número de factura; la tercera al NIT / CI del Cliente; la cuarta a la Fecha de la Transacción y la quinta al Monto de la Transacción.

```
  Llave de dosificación: 9rCB7Sv4X29d)5k7N%3ab89p-3(5[A
     5 Dígitos Verhoeff: 71621
   Largo de las cadenas: 8-2-7-3-2 (Suma 1 a cada dígito Verhoeff)

              Cadena 1: 9rCB7Sv4   (8 caracteres de largo)
              Cadena 2: X2         (2 caracteres de largo)
              Cadena 3: 9d)5k7N    (7 caracteres de largo)
              Cadena 4: %3a        (3 caracteres de largo)
              Cadena 5: b8         (2 caracteres de largo)

 Número de Autorización:  29040011007 → 29040011007 9rCB7Sv4
      Número de Factura:       150312 → 150312 X2
   NIT / CI del Cliente: 418917901158 → 418917901158 9d)5k7N
Fecha de la Transacción:   2007070201 → 2007070201 %3a
Monto de la Transacción:       250031 → 250031 b8
```

Paso 3

Aplicar el AllegedRC4 a la cadena conformada por la concatenación de todos los datos anteriores, utilizando como llave la concatenación de la Llave de Dosificación y los 5 dígitos Verhoeff generados previamente.

5 Dígitos Verhoeff: **71621**

Cadena concatenada: **290400110079rCB7Sv4150312X24189179011589d)5k7N2007070201%3a250031b8**
<----------*Cad 1*---------><--*Cad-2*-><----------*Cad 3*----------><-------*Cad 4*-----><--*Cad 5*->

Llave para cifrado: **9rCB7Sv4X29d)5k7N%3ab89p-3(5[A71621**
<----------*Llave Dosificación*----------><--DV->

AllegedRC4(290400110079rCB7Sv4150312X24189179011589d)5k7N2007070201%3a250031b8, 9rCB7Sv4X29d)5k7N%3ab89p-3(5[A71621) = **69DD0A42536C9900C4AE6484726C122ABDBF95D80A4BA403FB7834B3EC2A88595E 2149A3D965923BA4547B42B9528AAE7B8CFB9996BA2B58516913057C9D791B 6B748A**

Paso 4

Obtener la sumatoria total de los valores ASCII de todos los caracteres de la cadena resultante del paso anterior, además, calcular 5 sumatorias parciales de los ASCII de ciertos caracteres de la misma cadena, de acuerdo al siguiente criterio: La primera sumatoria parcial tomará las posiciones 1, 6, 11, 16, 21, etc.; la segunda 2, 7, 12, 17, 22, etc.; la tercera 3, 8, 13, 18, 23, etc.; la cuarta 4, 9, 14, 19, 24,etc. y la quinta 5, 10, 15, 20, 25, etc.

Sumatoria Total: **ST = 7720**
Sumatoria Parcial 1 (Posiciones 1-6-11-16-21...): **SP1 = 1548**
Sumatoria Parcial 2 (Posiciones 2-7-12-17-22...): **SP2 = 1537**
Sumatoria Parcial 3 (Posiciones 3-8-13-18-23...): **SP3 = 1540**
Sumatoria Parcial 4 (Posiciones 4-9-14-19-24...): **SP4 = 1565**
Sumatoria Parcial 5 (Posiciones 5-10-15-20-25..): **SP5 = 1530**

Paso 5

Obtener las multiplicaciones entre la sumatoria total y cada una de las sumatorias parciales. Dividir cada uno de los resultados obtenidos entre el dígito Verhoeff correspondiente más 1, el resultado deberá ser truncado. Finalmente obtener la sumatoria de todos los resultados y aplicar Base64.

5 Dígitos Verhoeff: **71621**

Dividendos: **8-2-7-3-2** (Suma 1 a cada dígito Verhoeff)

ST * SP1 = 7720 * 1548 = **11950560** -> Truncar(11950560 **/ 8**) = **1493820**
ST * SP2 = 7720 * 1537 = **11865640** → Truncar(11865640 **/ 2**) = **5932820**
ST * SP3 = 7720 * 1540 = **11888800** → Truncar(11888800 **/ 7**) = **1698400**
ST * SP4 = 7720 * 1565 = **12081800** → Truncar(12081800 **/ 3**) = **4027266**
ST * SP5 = 7720 * 1530 = **11811600** → Truncar(11811600 **/ 2**) = **5905800**

19058106

Base64(19058106) = **18isw**

Paso 6

Aplicar el AllegedRC4 a la anterior expresión obtenida, utilizando como llave la concatenación de la Llave de Dosificación y los 5 dígitos Verhoeff generados anteriormente.

5 Dígitos Verhoeff: **71621**

Llave para cifrado: **9rCB7Sv4X29d)5k7N%3ab89p-3(5[A71621**
<----------*Llave Dosificación*----------><--*DV*->

AllegedRC4(18isw, 9rCB7Sv4X29d)5k7N%3ab89p-3(5[A71621) = **6ADC530514**

Código de Control

La información resultante del proceso de cifrado, expresada en formato hexadecimal separada en pares por guiones (-), se denominará Código de Control y deberá ser impresa en cada factura emitida.

Código de Control: 6A-DC-53-05-14

5. EJEMPLOS DE GENERACIÓN DEL CÓDIGO DE CONTROL

Los siguientes son ejemplos de Códigos de Control generados a partir de los datos propuestos:

Ej.1

Número de Autorización: **79040011859**
Número de Factura: **152**
NIT / CI del Cliente: **1026469026**
Fecha de la Transacción: **20070728**
Monto de la Transacción: **135**

Llave de Dosificación: **A3Fs4s$)2cvD(eY667A5C4A2rsdf53kw9654E2B23s24df35F5**

Paso 1

Número de Factura: 152**72**
NIT / CI del Cliente: 1026469026**92**
Fecha de la Transacción: 20070728**68**
Monto de la Transacción: 135**41**

104654004373

5 dígitos Verhoeff: 104654004373**42765** -> **42765**

Paso 2

Llave de dosificación: **A3Fs4s$)2cvD(eY667A5C4A2rsdf53kw9654E2B23 s24df35F5**

5 dígitos Verhoeff: **42765**

Largo de las cadenas: **5-3-8-7-6** (Suma 1 a cada dígito Verhoeff)

	Cadena 1: **A3Fs4** (**5** caracteres de largo) Cadena 2: **s$)** (**3** caracteres de largo) Cadena 3: **2cvD(eY6** (**8** caracteres de largo) Cadena 4: **67A5C4A** (**7** caracteres de largo) Cadena 5: **2rsdf5** (**6** caracteres de largo) Número de Autorización: 79040011859 → 79040011859**A3Fs4** Número de Factura: 15272 → 15272**s$)** NIT / CI del Cliente: 102646902692 → 102646902692**2cvD(eY6** Fecha de la Transacción: 2007072868 → 20070728**67A5C4A** Monto de la Transacción: 13541 → 13541**2rsdf5**
Paso 3	5 dígitos Verhoeff: **42765** Cadena concatenada: **79040011859A3Fs415272s$)1026469026922cvD(eY6200707286867A5C4A135412rsdf5** Llave para cifrado: **A3Fs4s$)2cvD(eY667A5C4A2rsdf53kw9654E2B23s24df35F542765** AllegedRC4(79040011859A3Fs415272s$)1026469026922cvD(eY6200707286867A5C4A135412rsdf5, A3Fs4s$)2cvD(eY667A5C4A2rsdf53kw9654E2B23s24df35F542765) = **BEE6B80BB6F414D9AE3031EFA37C272B9B6CB87EFE32C4407296FA4CA7825E85ADDA18CA746CA83A6ABC6E8527B6C487CB9BBCF9A6AF59F22FB6A0934C5ED94301A02C5484E48BBD**
Paso 4	Sumatoria Total: **ST** = **8523** Sumatoria Parcial 1 (Posiciones 1-6-11-16-21...): **SP1** = **1739** Sumatoria Parcial 2 (Posiciones 2-7-12-17-22...): **SP2** = **1755** Sumatoria Parcial 3 (Posiciones 3-8-13-18-23...): **SP3** = **1720** Sumatoria Parcial 4 (Posiciones 4-9-14-19-24...): **SP4** = **1679** Sumatoria Parcial 5 (Posiciones 5-10-15-20-25..): **SP5** = **1630**
Paso 5	5 dígitos Verhoeff: **42765** Dividendos: **5-3-8-7-6** (Suma 1 a cada dígito Verhoeff) ST * SP1 → 8523 * 1739 = **14821497** → Truncar(14821497 **/ 5**) = **2964299** ST * SP2 → 8523 * 1755 = **14957865** → Truncar(14957865 **/ 3**) = **4985955** ST * SP3 → 8523 * 1720 = **14659560** → Truncar(14659560 **/ 8**) = **1832445** ST * SP4 → 8523 * 1679 = **14310117** → Truncar(14310117 **/ 7**) = **2044302** ST * SP5 → 8523 * 1630 = **13892490** → Truncar(13892490 **/ 6**) = **2315415** **14142416** Base64(14142416) = **rylG**

Paso 6

5 dígitos Verhoeff: **42765**

Llave para cifrado: **A3Fs4s$)2cvD(eY667A5C4A2rsdf53kw9654E2B23s24df35F542765**

AllegedRC4(rylG, A3Fs4s$)2cvD(eY667A5C4A2rsdf53kw9654E2B23s24df35F542765) = **FBA6E478**

Código de Control: FB-A6-E4-78

Ej.2

Número de Autorización: **20040010113**
Número de Factura: **665**
NIT / CI del Cliente: **1004141023**
Fecha de la Transacción: **20070108**
Monto de la Transacción: **905.23**

Llave de Dosificación: **442F3w5AggG7644D737asd4BH5677sasdL4%44643(3C3674F4**

Paso 1

Número de Factura: 665**04**
NIT / CI del Cliente: 1004141023**00**
Fecha de la Transacción: 20070108**47**
Monto de la Transacción: 905**57**

102421270208

Dígitos Verhoeff: 102421270208**45644** -> **45644**

Paso 2

Llave de dosificación: **442F3w5AggG7644D737asd4BH5677sasdL4%44643(3C3674F4**

5 dígitos Verhoeff: **45644**

Largo de las cadenas: **5-6-7-5-5** (Suma 1 a cada dígito Verhoeff)

Cadena 1: **442F3** (**5** caracteres de largo)
Cadena 2: **w5AggG** (**6** caracteres de largo)
Cadena 3: **7644D73** (**7** caracteres de largo)
Cadena 4: **7asd4** (**5** caracteres de largo)
Cadena 5: **BH567** (**5** caracteres de largo)

Número de Autorización: 20040010113 → 20040010113**442F3**
Número de Factura: 66504 → 66504**w5AggG**
NIT / CI del Cliente: 100414102300 → 100414102300**7644D73**
Fecha de la Transacción: 2007010847 → 2007010847**7asd4**
Monto de la Transacción: 90557 → 90557**BH567**

Paso 3

5 dígitos Verhoeff: **45644**

Cadena concatenada: **20040010113442F366504w5AggG1004141023007644D7320070108477asd490557BH567**

Llave para cifrado: **442F3w5AggG7644D737asd4BH5677sasdL4%44643(3C3674F445644**

AllegedRC4(20040010113442F366504w5AggG1004141023007644D7320070108477asd490557BH567, 442F3w5AggG7644D737asd4BH5677sasdL4%44643(3C3674F445644) = **289301C4A332536E7894E1381D04F469C7EF7CD18BAE92827A29BEFCF6D6EBDDA84798C984482D1717855953DF8965B6316DFBDFB3750265D276E5ACF70252EF535120391CEC8A**

Paso 4

Sumatoria Total: **ST = 8219**
Sumatoria Parcial 1 (Posiciones 1-6-11-16-21...): **SP1 = 1682**
Sumatoria Parcial 2 (Posiciones 2-7-12-17-22...): **SP2 = 1657**
Sumatoria Parcial 3 (Posiciones 3-8-13-18-23...): **SP3 = 1624**
Sumatoria Parcial 4 (Posiciones 4-9-14-19-24...): **SP4 = 1641**
Sumatoria Parcial 5 (Posiciones 5-10-15-20-25..): **SP5 = 1615**

Paso 5

5 dígitos Verhoeff: **45644**

Dividendos: **5-6-7-5-5** (Suma 1 a cada dígito Verhoeff)

ST * SP1 → 8219 * 1682 = **13824358** → Truncar(13824358 **/ 5**) = **2764871**
ST * SP2 → 8219 * 1657 = **13618883** → Truncar(13618883 **/ 6**) = **2269813**
ST * SP3 → 8219 * 1624 = **13347656** → Truncar(13347656 **/ 7**) = **1906808**
ST * SP4 → 8219 * 1641 = **13487379** → Truncar(13487379 **/ 5**) = **2697475**
ST * SP5 → 8219 * 1615 = **13273685** → Truncar(13273685 **/ 5**) = **2654737**

12293704

Base64(12293704) = **kvP8**

Paso 6

5 dígitos Verhoeff: **45644**

Llave para cifrado: **442F3w5AggG7644D737asd4BH5677sasdL4%44643(3C3674F445644**

AllegedRC4(kvP8, 442F3w5AggG7644D737asd4BH5677sasdL4%44643(3C3674F445644) = **71D561C8**

Código de Control: 71-D5-61-C8

Ej.3

Número de Autorización: **1904008691195**
Número de Factura: **978256**
NIT / CI del Cliente: **0**
Fecha de la Transacción: **20080201**
Monto de la Transacción: **26006**

Llave de Dosificación: **pPgiFS%)v}@N4W3aQqqXCEHVS2[aDw_n%3)pFyU%bEB9)YXt%xNBub4@PZ4S9)ct**

Paso 1

Número de Factura: 978256**22**
NIT / CI del Cliente: 0**47**
Fecha de la Transacción: 20080201**23**
Monto de la Transacción: 26006**27**

2108446419

Dígitos Verhoeff: 2108446419**21885** -> **21885**

Paso 2

Llave de dosificación: **pPgiFS%)v}@N4W3aQqqXCEHVS2[aDw_n%3)pFyU%bEB9)YXt%xNBub4@PZ4S9)ct**

5 dígitos Verhoeff: **21885**

Largo de las cadenas: **3-2-9-9-6** (Suma 1 a cada dígito Verhoeff)

Cadena 1: **pPg** (**3** caracteres de largo)
Cadena 2: **iF** (**2** caracteres de largo)
Cadena 3: **S%)v}@N4W** (**9** caracteres de largo)
Cadena 4: **3aQqqXCEH** (**9** caracteres de largo)
Cadena 5: **VS2[aD** (**6** caracteres de largo)

Número de Autorización: 1904008691195 → 1904008691195**pPg**
Número de Factura: 97825622 → 97825622**iF**
NIT / CI del Cliente: 047 → 047**S%)v}@N4W**
Fecha de la Transacción: 2008020123 → 2008020123**3aQqqXCEH**
Monto de la Transacción: 2600627 → 2600627**VS2[aD**

Paso 3

5 dígitos Verhoeff: **21885**

Cadena concatenada: **1904008691195pPg97825622iF047S%)v}@N4W20080201233aQqqXCEH2600627VS2[aD**

Llave para cifrado: **pPgiFS%)v}@N4W3aQqqXCEHVS2[aDw_n%3)pFyU%bEB9)YXt%xNBub4@PZ4S9)ct21885**

AllegedRC4(1904008691195pPg97825622iF047S%)v}@N4W20080201233aQqqXCEH2600627VS2[aD, pPgiFS%)v}@N4W3aQqqXCEHVS2[aDw_n%3)pFyU%bEB9)YXt%xNBub4@PZ4S9)ct21885) = **2A60AA64B6624D1F2E2BC3C9295433C52402348DFBB019D7AFC5279E1E9C046841B7E8EB1BD400EF6B0DC84B8580AEAA1C7EB3C7C41A6593C1751DE44A9C8318D32853E94BA2**

Paso 4

Sumatoria Total: **ST = 8107**
Sumatoria Parcial 1 (Posiciones 1-6-11-16-21...): **SP1 = 1630**
Sumatoria Parcial 2 (Posiciones 2-7-12-17-22...): **SP2 = 1532**
Sumatoria Parcial 3 (Posiciones 3-8-13-18-23...): **SP3 = 1639**
Sumatoria Parcial 4 (Posiciones 4-9-14-19-24...): **SP4 = 1659**
Sumatoria Parcial 5 (Posiciones 5-10-15-20-25..): **SP5 = 1647**

Paso 5

5 dígitos Verhoeff: **21885**

Dividendos: **3-2-9-9-6** (Suma 1 a cada dígito Verhoeff)

ST * SP1 → 8107 * 1630 = **13214410** → Truncar(13214410 **/ 3**) = **4404803**
ST * SP2 → 8107 * 1532 = **12419924** → Truncar(12419924 **/ 2**) = **6209962**
ST * SP3 → 8107 * 1639 = **13287373** → Truncar(13287373 **/ 9**) = **1476374**
ST * SP4 → 8107 * 1659 = **13449513** → Truncar(13449513 **/ 9**) = **1494390**
ST * SP5 → 8107 * 1647 = **13352229** → Truncar(13352229 **/ 6**) = **2225371**

15810900

Base64(15810900) = **yK5K**

Paso 6

5 dígitos Verhoeff: **21885**

Llave para cifrado: **pPgiFS%)v}@N4W3aQqqXCEHVS2[aDw_n%3)pFyU%bEB9)YXt%xNBub4@PZ4S9)ct21885**

AllegedRC4(yK5K, pPgiFS%)v}@N4W3aQqqXCEHVS2[aDw_n%3)pFyU%bEB9)YXt%xNBub4@PZ4S9)ct21885) = **6212AF1B**

Código de Control: 62-12-AF-1B

Ej.4

Número de Autorización: **10040010640**
Número de Factura: **9901**
NIT / CI del Cliente: **1035012010**
Fecha de la Transacción: **20070813**
Monto de la Transacción: **451,49**

Llave de Dosificación: **DSrCB7Ssdfv4X29d)5k7N%3ab8p3S(asFG5YU8477SWW)FDAQA**

Paso 1

Número de Factura: 9901**74**
NIT / CI del Cliente: 1035012010**18**
Fecha de la Transacción: 2007081**372**
Monto de la Transacción: 451**45**

105509317709

Dígitos Verhoeff: 105509317709**70510** -> **70510**

Paso 2

Llave de dosificación: **DSrCB7Ssdfv4X29d)5k7N%3ab8p3S(asFG5YU8477 SWW)FDAQA**

5 dígitos Verhoeff: **70510**

Largo de las cadenas: **8-1-6-2-1** (Suma 1 a cada dígito Verhoeff)

Cadena 1: **DSrCB7Ss** (**8** caracteres de largo)
Cadena 2: **d** (**1** caracteres de largo)
Cadena 3: **fv4X29** (**6** caracteres de largo)
Cadena 4: **d)** (**2** caracteres de largo)
Cadena 5: **5** (**1** caracteres de largo)

Número de Autorización: 10040010640 → 10040010640**DSrCB7Ss**
Número de Factura: 990174 → 990174**d**
NIT / CI del Cliente: 103501201018 → 103501201018**fv4X29**
Fecha de la Transacción: 2007081372 → 2007081372**d)**
Monto de la Transacción: 45145 → 45145**5**

Paso 3

5 dígitos Verhoeff: **70510**

Cadena concatenada: **10040010640DSrCB7Ss990174d103501201018fv4X292007081372d)451455**

Llave para cifrado: **DSrCB7Ssdfv4X29d)5k7N%3ab8p3S(asFG5YU8477 SWW)FDAQA70510**

AllegedRC4(10040010640DSrCB7Ss990174d103501201018fv4X292007081372d)451455, DSrCB7Ssdfv4X29d)5k7N%3ab8p3S(asFG5YU8477SWW)FDAQA70510) = **A0D5B01584CEAED79FF6A08D69406DC2227D2D3D11E9B7455F167BB169A0FE2FFD06A4B9F6F4586584763F5D266C2D23EE3C8C9D98AAB6EA058A18CF0A1**

Paso 4

Sumatoria Total: **ST = 7270**
Sumatoria Parcial 1 (Posiciones 1-6-11-16-21...): **SP1 = 1493**
Sumatoria Parcial 2 (Posiciones 2-7-12-17-22...): **SP2 = 1475**
Sumatoria Parcial 3 (Posiciones 3-8-13-18-23...): **SP3 = 1411**
Sumatoria Parcial 4 (Posiciones 4-9-14-19-24...): **SP4 = 1459**
Sumatoria Parcial 5 (Posiciones 5-10-15-20-25..): **SP5 = 1432**

Paso 5

5 dígitos Verhoeff: **70510**

Dividendos: **8-1-6-2-1** (Suma 1 a cada dígito Verhoeff)

ST * SP1 → 7270 * 1493 = **10854110** → Truncar(10854110 **/ 8**) = **1356763**
ST * SP2 → 7270 * 1475 = **10723250** → Truncar(10723250 **/ 1**) = **10723250**
ST * SP3 → 7270 * 1411 = **10257970** → Truncar(10257970 **/ 6**) = **1709661**
ST * SP4 → 7270 * 1459 = **10606930** → Truncar(10606930 **/ 2**) = **5303465**
ST * SP5 → 7270 * 1432 = **10410640** → Truncar(10410640 **/ 1**) = **10410640**

29503779

Base64(29503779) = **1mZ4Z**

Paso 6

5 dígitos Verhoeff: **70510**

Llave para cifrado: **DSrCB7Ssdfv4X29d)5k7N%3ab8p3S(asFG5YU8477 SWW)FDAQA70510**

AllegedRC4(1mZ4Z, DSrCB7Ssdfv4X29d)5k7N%3ab8p3S(asFG5YU8477SWW)FDAQA70510) = **6A50310132**

Código de Control: 6A-50-31-01-32

Ej.5

Número de Autorización: **30040010595**
Número de Factura: **10015**
NIT / CI del Cliente: **953387014**
Fecha de la Transacción: **20070825**
Monto de la Transacción: **5725,90**

Llave de Dosificación: **33E265B43C4435sdTuyBVssD355FC4A6F46sdQWasdA)d56666fDsmp9846636B3**

Paso 1

Número de Factura: 10015**40**
NIT / CI del cliente: 95338701**474**
Fecha de la Transacción: 2007082**516**
Monto de la Transacción: 572**667**

97347358197

Dígitos Verhoeff: 97347358197**91803** -> **91803**

Paso 2

Llave de dosificación: **33E265B43C4435sdTuyBVssD355FC4A6F46sdQWasdA)d56666fDsmp9846636B3**

5 dígitos Verhoeff: **91803**

Largo de las cadenas: **10-2-9-1-4** (Suma 1 a cada dígito Verhoeff)

Cadena 1: **33E265B43C** (**10** caracteres de largo)
Cadena 2: **44** (**2** caracteres de largo)
Cadena 3: **35sdTuyBV** (**9** caracteres de largo)
Cadena 4: **s** (**1** caracteres de largo)
Cadena 5: **sD35** (**4** caracteres de largo)

Número de Autorización: 30040010595 → 30040010595**33E265B43C**
Número de Factura: 1001540 → 100154**044**
NIT / CI del Cliente: 95338701474 → 95338701474**35sdTuyBV**
Fecha de la Transacción: 2007082516 → 2007082516**s**
Monto de la Transacción: 572667 → 572667**sD35**

Paso 3

5 dígitos Verhoeff: **91803**

Cadena concatenada: **3004001059533E265B43C1001540449533870147435sdTuyBV2007082516s572667sD35**

Llave para cifrado: **33E265B43C4435sdTuyBVssD355FC4A6F46sdQWasdA)d56666fDsmp9846636B391803**

AllegedRC4(3004001059533E265B43C1001540449533870147435sdTuyBV2007082516s572667sD35, 33E265B43C4435sdTuyBVssD355FC4A6F46sdQWasdA)d56666fDsmp9846636B391803) = **AA0197F70906902CC56017591FB1329BB60ABF2FF0CBF26ADFF39B2CCF481AA83CB53BEBB022586CF8484A0C618389F8A3AC33B4F11476D127F8E09DDA386C6C6106F34AEE4F71**

Paso 4

Sumatoria Total: **ST = 8269**
Sumatoria Parcial 1 (Posiciones 1-6-11-16-21...): **SP1 = 1742**
Sumatoria Parcial 2 (Posiciones 2-7-12-17-22...): **SP2 = 1708**
Sumatoria Parcial 3 (Posiciones 3-8-13-18-23...): **SP3 = 1649**
Sumatoria Parcial 4 (Posiciones 4-9-14-19-24...): **SP4 = 1536**
Sumatoria Parcial 5 (Posiciones 5-10-15-20-25..): **SP5 = 1634**

Paso 5

5 dígitos Verhoeff: **91803**

Dividendos: **10-2-9-1-4** (Suma 1 a cada dígito Verhoeff)

ST * SP1 → 8269 * 1742 = **14404598** → Truncar(14404598 **/ 10**) = **1440459**
ST * SP2 → 8269 * 1708 = **14123452** → Truncar(14123452 **/ 2**) = **7061726**
ST * SP3 → 8269 * 1649 = **13635581** → Truncar(13635581 **/ 9**) = **1515064**
ST * SP4 → 8269 * 1536 = **12701184** → Truncar(12701184 **/ 1**) = **12701184**
ST * SP5 → 8269 * 1634 = **13511546** → Truncar(13511546 **/ 4**) = **3377886**

26096319

Base64(26096319) = **1ZZA/**

Paso 6

5 dígitos Verhoeff: **91803**

Llave para cifrado: **33E265B43C4435sdTuyBVssD355FC4A6F46sdQWasdA)d56666fDsmp9846636B391803**

AllegedRC4(1ZZA/, 33E265B43C4435sdTuyBVssD355FC4A6F46sdQWasdA)d56666fDsmp9846636B391803) = **A86BFD8216**

Código de Control: A8-6B-FD-82-16

6. OTRAS IMPLEMENTACIONES

Además del Código de Control, los Sistemas de Facturación Computarizada también deberán contemplar las siguientes implementaciones:

6.1. Incorporación y tratamiento de todos los datos que conforman las facturas o notas fiscales, esto de acuerdo a lo establecido en la RND Nº 10-0016-07.

6.2. Tratamiento de los nuevos formatos, tamaños, colores y materiales para las facturas, establecidos en la RND Nº 10-0016-07.

6.3. Aplicación de los nuevos formatos para el Libro de Compras y Ventas IVA, detallados en la RND Nº 10-0016-07.

6.4. Control de la Fecha Límite de Emisión para la dosificación de las facturas o notas fiscales, de manera que a partir de las dos semanas previas a esta fecha, alerte a los usuarios sobre la necesidad de solicitar una nueva dosificación.

6.5. Pasado el plazo señalado por la Fecha Límite de Emisión, el Sistema de Facturación Computarizada no deberá permitir la emisión de facturas.

6.6. Considerando la importancia y sensibilidad del proceso de configuración de la dosificación en el Sistema de Facturación Computarizada, este deberá contemplar la doble captura de los siguientes datos:

- Número de autorización.
- Número inicial de la factura.
- Fecha límite de emisión.
- Llave de dosificación.

7. REFERENCIAS

Alleged RC4:

- **Pseudocódigo Alleged RC4** - http://www.impuestos.gov.bo/Facturacion/EspAllegedRC4.pdf
- **RC4 Encryption** - http://www.4guysfromrolla.com/webtech/010100-1.shtml
- **RC4 Test** - http://www.4guysfromrolla.com/demos/rc4test.htm
- **Alleged RC4** - http://www.criptored.upm.es/software/sw_m117a.htm

Verhoeff:

- **Pseudocódigo Verhoeff** - http://www.impuestos.gov.bo/Facturacion/EspVERHOEFF.pdf
- **Check Digits** - http://www.augustana.ab.ca/~mohrj/algorithms/checkdigit.html
- **Verhoeff algorithm** - http://en.wikipedia.org/wiki/Verhoeff_algorithm

Base 64:

- **Pseudocódigo Base 64** - http://www.impuestos.gov.bo/Facturacion/EspBASE64.pdf
- **Conversión de números a palabras -** http://mundocripto.com/mambo//content/view/78/43/

Casos de Prueba:

- http://www.impuestos.gov.bo/Facturacion/5000CasosPruebaCCVer7.pdf
- http://www.impuestos.gov.bo/Facturacion/5000CasosPruebaCCVer7.xsl
- http://www.impuestos.gov.bo/Facturacion/5000CasosPruebaCCVer7.txt