

## Requisitos para la Validación de Cumplimiento de Comercios Afiliados Nivel 4

---

A: Comercios Afiliados Nivel 4  
Gerente General

---

### En Breve

VisaNet Dominicana anuncia la inclusión de medidas complementarias de control en el marco de cumplimiento para los Comercios Afiliados Nivel 4 de acuerdo a la norma PCI-DSS y los programas de cumplimiento de seguridad de datos VISA, con el fin de garantizar aún más la seguridad del sistema de pago electrónico en la República Dominicana. Las mejoras esbozadas en la presente están encaminadas a impulsar una mayor validación de cumplimiento con la Norma de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI-DSS, según sus siglas en inglés), a fin de evitar los compromisos de datos de los tarjetahabientes<sup>1</sup>.

Independientemente al mandato de cumplimiento con las Normas de Seguridad PCI existe además la validación mediante la cual las entidades verifican y demuestran su cumplimiento. Esta importante tarea permite identificar y corregir vulnerabilidades, y proteger a los clientes asegurando que se mantengan niveles apropiados de seguridad.

Visa Inc. ha establecido prioridades y ha definido niveles de validación de cumplimiento basados en el volumen de transacciones, el riesgo potencial y la exposición que los comercios introducen al sistema de pago electrónico. Para leer más acerca de los niveles y requisitos de validación de los comercios visite [http://lac.visa.com/merchant/security\\_3.jsp](http://lac.visa.com/merchant/security_3.jsp).

A partir de estos requisitos fundamentales, VisaNet Dominicana, como miembro adquirente de la marca VISA en República Dominicana, establece procedimientos y requisitos adicionales acordes al escenario local.

Para los comercios afiliados que apliquen, este nuevo marco establece los requisitos mínimos para validar su cumplimiento con la norma PCI DSS. Más adelante se presenta el plazo límite para la corrección de faltas e incumplimientos con la Norma PCI DSS.

---

### Antecedentes

La Norma de Seguridad de Datos de la Industria de Tarjetas de Pagos (PCI DSS) consiste en una serie integral de requisitos de seguridad internacional para salvaguardar los datos de los tarjetahabientes. La norma PCI DSS fue desarrollada por Visa, conjuntamente con las cuatro otras marcas de pago fundadoras del Consejo de Normas de Seguridad PCI (PCI SSC - por sus siglas en inglés), para ayudar a facilitar la amplia adopción de medidas uniformes de seguridad de datos a nivel mundial. Los requisitos de PCI DSS son la base de los programas de cumplimiento de seguridad de datos de Visa Inc., incluyendo el Programa de Seguridad de Información de las Cuentas (AIS) y el Programa de Seguridad de Información de los Tarjetahabientes (CISP).

VisaNet Dominicana está comprometida a proteger el sistema de medios de pagos electrónicos y los datos de tarjetahabientes en sentido general. El cumplimiento con la norma PCI DSS resulta en beneficios más allá que simplemente garantizar la seguridad de los datos de los tarjetahabientes, ya que sólidas prácticas de seguridad, ayudan a proteger a las organizaciones contra consecuencias financieras y/o de reputación adversa, a menudo relacionadas con casos en que los datos de los tarjetahabientes se han visto comprometidos.

En la actualidad, cualquier entidad que almacene, procese o transmita datos de los tarjetahabientes tiene la obligación de cumplir con la norma PCI DSS. Para garantizar el cumplimiento, Visa Inc. ha implementado un marco uniforme para validar el cumplimiento con la norma PCI DSS en cada región. Este marco establece los requisitos de cumplimiento de línea de base para los comercios y proveedores de servicio concentrados en validar y hacer cumplir la norma PCI DSS.

---

<sup>1</sup> Tarjetahabiente - Persona individual que a través del uso de la tarjeta (crédito, débito y prepago), de la cual es legítimo titular, adquiere bienes o servicios en los establecimientos comerciales.

## Marco de Cumplimiento con la Norma PCI DSS para los Comercios Nivel 4

### Comercios de Nivel 4 y Requisitos de Validación

Además de los mandatos para cumplir con la norma PCI DSS, Visa Inc. ha establecido prioridades y ha definido niveles globales de validación de cumplimiento basados en el volumen de transacciones, el riesgo potencial y la exposición que introducen al sistema de medios de pago electrónico, comercios y proveedores de servicios.

VisaNet Dominicana tiene la responsabilidad de identificar el nivel de validación de los comercios. Todos los comercios se identificarán en uno de éstos cuatro niveles basados en el volumen de transacciones Visa durante un periodo de 12 meses.

#### Consideraciones acerca de la identificación de los Comercios

*El volumen de transacciones es el resultado del total de transacciones (incluyendo crédito, débito y prepago) de un comercio que opera bajo el mismo nombre comercial (DBA<sup>2</sup>).*

*Si un comercio corporativo tiene más de un nombre comercial, debe considerarse el número total agregado de transacciones Visa que almacena, procesa ó transmite la empresa para determinar el nivel de validación.*

*Para empresas con franquicias, el nivel de validación se determina en base al número total de transacciones de la corporación, incluyendo el volumen acumulado de todas las localidades propiedad de la compañía.*

*El volumen de los comercios de propiedad y operación independiente (por ej.: franquicia, concesionario) puede ser excluido si el mismo no es manejado por la entidad corporativa.*

*Para leer más acerca de los niveles y requisitos de validación anual para comercios en general, visite [http://lac.visa.com/merchant/security\\_3.jsp](http://lac.visa.com/merchant/security_3.jsp).*

En adición al marco establecido por Visa Inc., VisaNet Dominicana divide a sus comercios afiliados nivel 4, en dos escalas: los comercios niveles 4.1 y 4.2 respectivamente.

A continuación presentamos la tabla que contiene los requerimientos de validación, establecidos por VisaNet Dominicana, para estos comercios de acuerdo a sus criterios y su capacidad para almacenar información de tarjetahabiente:

Nivel*	Criterios de Comercios	Condición	Requerimientos de Validación						
			SAQ	TRDP	SCAN TRI PCI	SCAN DIA	ADDENDUM	CHARLA PCI-DSS	SCAN INTERNO
4.1	Comercios de Internet (E-commerce) con un volumen de transacciones** entre 10,000 y 20,000 anual.	Con capacidad de almacenamiento	x	x	x	x	x	x	
	Comercios con [Conexión Directa]***, con volumen de transacciones** entre 100,000 y 1MM anual.		x	x	x		x	x	A discreción de VisaNet Dominicana
	Otros comercios con volumen de transacciones entre 200,000 y 1MM.	Sin capacidad de almacenamiento		x			A discreción de VisaNet Dominicana		
4.2	Comercios de Internet (E-commerce) con volumen de transacciones menor a 10,000 anual.	Con capacidad de almacenamiento	x	x	x		x		
	Comercios con [Conexión Directa]***, con volumen de transacciones** menor a 100,000 anual.		x	x			x		A discreción de VisaNet Dominicana
	Otros comercios con volumen de transacciones** hasta 200,000 anual.	Sin capacidad de almacenamiento							

Requerido  Sugerencia

\* Cualquier comercio que sufra un ataque que resulte en compromiso de cuentas puede ser escalado a un nivel más alto de validación.

\*\* Se refiere a transacciones Visa, adquiridas por VisaNet Dominicana.

\*\*\* Comercializado por VisaNet Dominicana como "Conectividad Virtual" (ATM). Usualmente utilizado para los sistemas de cajas registradoras para procesar las transacciones con tarjetas.

<sup>2</sup> DBA - "Doing Business As" término en inglés utilizado para expresar "corporación" o cadena de tiendas.

La información en ésta comunicación sólo aplica a los comercios afiliados a VisaNet Dominicana, R. D.

**Definición de Requerimientos de Validación**

<p><b>SAQ</b></p>	<p>Cuestionario de Auto-evaluación (SAQ), el comercio sólo llenará las páginas 1 a 4 del formulario.</p> <p>El cuestionario de auto-evaluación del PCI-DSS es una herramienta elaborada con la intención de asistir a los comercios y proveedores de servicios en autoevaluar su cumplimiento con las Normas de Seguridad de la Información de la Industria de Tarjetas de Pago.</p> <p>Existen múltiples versiones del PCI DSS SAQ, cada una destinada a un escenario específico. El cuestionario que aparece a continuación es el que mejor aplica a la organización a que hacemos referencia en esta comunicación, en este caso, comercios. Descárguelo en <a href="http://www.visanet.com.do/app/public_docs/saq_d_la-es.doc">http://www.visanet.com.do/app/public_docs/saq_d_la-es.doc</a> ó <a href="https://www.pcisecuritystandards.org/saq/docs/saq_d_la-es.doc">https://www.pcisecuritystandards.org/saq/docs/saq_d_la-es.doc</a></p> <p>Para más información acerca del SAQ favor viste <a href="https://www.pcisecuritystandards.org/saq/index.shtml">https://www.pcisecuritystandards.org/saq/index.shtml</a>. Ver instrucciones y directrices en <a href="https://www.pcisecuritystandards.org/saq/docs/saq_inst_guidelines_la-es.pdf">https://www.pcisecuritystandards.org/saq/docs/saq_inst_guidelines_la-es.pdf</a></p>
<p><b>TRDP</b></p>	<p>Testimonio de Retención de Data Prohibida. Documento dónde el comercio confirma si retiene o no data de banda magnética (ej.: track) data, CVV2<sup>3</sup> data, o data de PIN<sup>4</sup> en sistemas luego de la autorización de la transacción.</p> <p>VisaNet Dominicana informará al comercio el nivel a que pertenece y el comercio entregará el documento firmado para su evaluación. En caso de que el comercio esté almacenando información sensible sin truncar o sin que cumpla con los requisitos PCI, VisaNet Dominicana exigirá al comercio la asistencia de un QSA<sup>5</sup> y la entrega del AOC<sup>6</sup>, además debe incluir el plan de remediación o los controles de compensación a tomar.</p> <p>Descárguelo en <a href="http://www.visanet.com.do/app/public_docs/TEC09_INF_FORM_20091019_Testimonio_Retencion_de_Data_Prohibida.doc">http://www.visanet.com.do/app/public_docs/TEC09_INF_FORM_20091019_Testimonio_Retencion_de_Data_Prohibida.doc</a></p>
<p><b>SCAN TRI PCI</b></p>	<p>Escaneo que realiza un (ASV<sup>7</sup>) trimestralmente. Revisa por la presencia de vulnerabilidades de acuerdo a estrictos parámetros de la norma PCI DSS.</p> <p>El escaneo trimestral de seguridad de red es una herramienta automatizada que revisa los sistemas por vulnerabilidades. Conduce un escaneo sin intrusión que revisa remotamente a redes y aplicaciones web cuyo acceso se logra a través de direcciones IP públicas provistas por el comercio que dan frente hacia el internet. Los comercios son responsables por asegurar que los escaneos trimestrales de seguridad de red requeridos sean ejecutados por el ASV.</p> <p>Un servicio popularmente utilizado en el mercado lo es mcafeesecure.com que provee el nivel más alto en seguridad para sitios web; adicionalmente dispone de un nivel aún mayor de inspección para el cumplimiento de las normas PCI DSS. Para mayor información acerca de los servicios que ofrece mcafeesecure.com, favor llenar el formulario en línea disponible en <a href="http://www.mcafeesecure.com/us/merchants-moreinfo.jsp">http://www.mcafeesecure.com/us/merchants-moreinfo.jsp</a></p> <p>Para más información, descargue el Procedimiento PCI para Escaneo de Seguridad (en inglés) <a href="https://www.pcisecuritystandards.org/pdfs/pci_scanning_procedures_v1-1.pdf">https://www.pcisecuritystandards.org/pdfs/pci_scanning_procedures_v1-1.pdf</a>.</p>
<p><b>SCAN DIA</b></p>	<p>Escaneo que realiza un (ASV) diariamente, no necesariamente contempla los parámetros requeridos por PCI DSS. Revisa por la presencia de vulnerabilidades conforme a parámetros considerados de "mejores prácticas" en los sistemas.</p>
<p><b>ADDENDUM A CONTRATO DE AFILIACION</b></p>	<p>Compromiso de cumplimiento y descargo de indemnización a VisaNet Dominicana. El comercio afiliado se compromete a cumplir con las modificaciones que debe realizar a sus sistemas de información para realizar transacciones con tarjetas de Crédito/Débito y que se detallan en los documentos que el comercio adjunta al TRDP.</p> <p>El comercio debe firmar el addendum al contrato de afiliación como muestra de que está de acuerdo en seguir los lineamientos planteados en la norma PCI-DSS.</p>
<p><b>CHARLA PCI-DSS</b></p>	<p>Presentación PCI DSS a gerentes y administradores de las áreas de operaciones, sistemas y redes impartido por personal de VisaNet Dominicana.</p>
<p><b>SCAN INTERNO</b></p>	<p>Escaneo que puede realizarse con herramientas como <a href="#">Nessus</a> o <a href="#">GFI Languard</a> en un período determinado por el comercio o el agente. Verifica por la presencia de vulnerabilidades de red. Presenta un informe sobre los puertos o servicios encontrados (únicamente deben estar habilitados aquellos requeridos para la operación) y la correcta aplicación de parchos en los sistemas.</p>

<sup>3</sup> CVV2 – Valor de 3 dígitos impreso en el panel de firma de una tarjeta de pago cuya finalidad es verificar transacciones de tarjeta-no-presente.

<sup>4</sup> PIN - Número Personal de Identificación que es introducido por el tarjetahabiente durante una transacción tarjeta-presente y/o al envío cifrado de PIN Block presente dentro de un mensaje de transacción.

<sup>5</sup> QSA - asesor calificado de seguridad.

<sup>6</sup> AOC – Attestation of Compliance, prueba de cumplimiento.

<sup>7</sup> ASV - Approved Scanning Vendor. Proveedor de servicio externo al comercio y certificado para conducir inspección por vulnerabilidad de red, inspección de puertos, aplicación web y remediación.

La información en ésta comunicación sólo aplica a los comercios afiliados a VisaNet Dominicana, R. D.

### Principios de VisaNet Dominicana que sirven de guía para el cumplimiento con la norma PCI DSS:

- **Protección de la Información:** El comercio deberá mantener su red segura con acceso limitado al personal autorizado, todos los materiales o registros en cualquier forma que contengan información de cuentas o transacciones de tarjetas de pago electrónico de acuerdo a las normas de seguridad establecidas por el PCI Data Security Standard (PCI DSS). La pérdida o robo de información de cuentas como resultado del incumplimiento de las normas de seguridad de la información podrían resultar en cargos indemnizatorios al comercio parte de VisaNet Dominicana.
- **Validación del Cumplimiento:** El comercio debe leer las normas PCI Data Security Standard (PCI DSS). Éste estándar busca asistir a las organizaciones e instituciones en la protección de toda data relacionada con la información de las cuentas de los tarjetahabientes. En ese sentido, el comercio se debe comprometer a cumplir con las modificaciones necesarias a sus sistemas de información para que las transacciones con tarjetas de Crédito/Débito se realicen de forma segura.
- En todo caso y para toda modalidad de comercio, el almacenamiento de la Banda Magnética<sup>8</sup> (track data) luego del proceso de autorización está prohibido. Para mayor información acerca de la aplicabilidad del estándar de seguridad de datos PCI DSS favor descargue la siguiente tabla: [http://www.visanet.com.do/app/public\\_docs/Aplicabilidad\\_DSS\\_PCI.pdf](http://www.visanet.com.do/app/public_docs/Aplicabilidad_DSS_PCI.pdf).
- Para todo comercio afiliado con capacidad de almacenamiento de datos de tarjetahabientes cuyos procesos operativos requieran del almacenamiento del PAN<sup>9</sup>, Fecha de Vencimiento y/o el CVV2 luego de efectuarse la autorización de la transacción, VisaNet Dominicana exigirá como mínimo el cumplimiento con lo establecido en los acápites 3 y 4 de la norma PCI DSS (v1.2, octubre 2008) para lo cual se requerirá de la participación de un Asesor Calificado de Seguridad (QSA), cuyos gastos serán cubiertos por el comercio. El asesor realizará un Informe Anual de Cumplimiento (ROC<sup>10</sup>); en dicho caso, sólo se requiere que el comercio presente el Formulario de Certificación de Cumplimiento con la norma PCI DSS (AOC). Para una lista de los QSA reconocidos por el Consejo de Estándares de Seguridad PCI visite [https://www.pcisecuritystandards.org/pdfs/pci\\_qsa\\_list.pdf](https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf).
- Para la modalidad de comercio electrónico (nivel 4.1 y 4.2) y/o conectividad directa (nivel 4.1), deben cumplir adicionalmente con los requerimientos establecidos en el acápite 11.2 de la norma. PCI DSS requiere que todos los comercios con direcciones IP externas ó públicas (que dan frente hacia el internet) deben efectuar por lo menos, escaneos por vulnerabilidades trimestrales acompañado de un proceso de remediación correspondiente.
- Los comercios nuevos afiliados que usan software de aplicaciones de pago deben usar aplicaciones de que cumplan con los requisitos de la norma PA-DSS o tienen que cumplir con la norma PCI DSS. Para más información acerca de las Aplicaciones de pago aprobadas, visite [https://www.pcisecuritystandards.org/security\\_standards/vpa/vpa\\_approval\\_list.html](https://www.pcisecuritystandards.org/security_standards/vpa/vpa_approval_list.html).

VisaNet Dominicana comunicará oportunamente a cada comercio su correspondiente nivel de validación. Es obligación del comercio presentar la documentación correspondiente según la escala a que pertenece, a los 30 días desde el momento en que fue informado. Dicha documentación será proporcionada por el comercio al menos (1) una vez por año.

A partir del mes de noviembre del 2009, todo nuevo afiliado que utilice el servicio de comercio electrónico o conectividad directa se le hará entrega de ésta comunicación y los requerimientos establecidos para el nivel 4.2. Al año siguiente se procederá a reevaluar considerando los puntos antes mencionados para verificar si aplica movilización de escala o nivel. Para todos los comercios que aplique el prerrequisito del SCAN Trimestral, VisaNet realizará un scan de direcciones IP públicas de cortesía para conocer su estado actual y entregar los resultados al comercio.

VisaNet Dominicana se reserva el derecho de exigir al comercio la evaluación de cumplimiento por parte de un asesor calificado de seguridad (QSA, por sus siglas en inglés).

<sup>8</sup> Banda Magnética (track data) – data codificada en la franja magnética utilizada para la autorización durante una transacción de tarjeta-presente.

<sup>9</sup> PAN - número de cuenta de tarjetahabiente.

<sup>10</sup> ROC - reporte de cumplimiento.

---

*La información en ésta comunicación sólo aplica a los comercios afiliados a VisaNet Dominicana, R. D.*

## **Plazo Límite para la corrección de faltas e incumplimientos con la Norma PCI DSS para los Comercios del Nivel 4 – 30 de Agosto del 2010**

VisaNet Dominicana exigirá que los comercios proporcionen toda la información requerida para su evaluación. Cada uno de los comercios deberá mostrar al personal correspondiente de VisaNet que ha validado el cumplimiento con la norma PCI DSS antes del 30 de agosto del 2010. Posterior a esta fecha, VisaNet impondrá controles de riesgo adecuados, hasta e incluyendo, sustitución de todo servicio de comercio electrónico o conectividad directa por Puntos de Ventas Dial-up<sup>11</sup> o GPRS<sup>12</sup>, retención de fondos y/o desafiliación.

---

### **Envío de la Documentación**

Toda la documentación debe ser enviada de manera segura, mediante encriptación PGP<sup>13</sup> al departamento de Seguridad de la Información de VisaNet Dominicana a la dirección: [pcidss@visanet.com.do](mailto:pcidss@visanet.com.do).

PGP v6.5.8 (gratis) está disponible en: <http://www.pgpi.org/cgi/download.cgi?filename=PGPFW658Win32.zip>

Puede descargar la llave pública de VisaNet Dominicana en: [http://www.visanet.com.do/app/public\\_docs/pcidss\\_visanet\\_dominicana.asc](http://www.visanet.com.do/app/public_docs/pcidss_visanet_dominicana.asc)

El uso de PGP es sencillo..., descargue e instale la aplicación y llave pública de VisaNet. Sobre el archivo deseado, presione el botón derecho de su puntero → PGP → Encrypt; seleccione la llave de VisaNet y continúe. El archivo resultante estará cifrado y listo para enviar.

---

Glosario de términos: [https://www.pcisecuritystandards.org/security\\_standards/docs/glossary\\_la-es.pdf](https://www.pcisecuritystandards.org/security_standards/docs/glossary_la-es.pdf)

### **Para más información**

Favor comuníquese con el departamento de Seguridad de la Información de VisaNet Dominicana llamando al +1(809) 947 5582 o al correo electrónico a [pcidss@visanet.com.do](mailto:pcidss@visanet.com.do)

Cordialmente,

Pedro Fernández  
Sub-Gerente de Seguridad de la Información  
VisaNet Dominicana

Joan Febles  
Gerente de Tecnología y Operaciones  
VisaNet Dominicana

---

<sup>11</sup> Una conexión Dial Up es una forma barata de acceso a Internet en la que el cliente utiliza un módem para llamar a través de la Red Telefónica Conmutada (RTC) al nodo del ISP, un servidor de acceso (por ejemplo PPP).

<sup>12</sup> General Packet Radio Service (GPRS) o servicio general de paquetes vía radio es una extensión del Sistema Global para Comunicaciones Móviles (Global System for Mobile Communications o GSM) para la transmisión de datos no conmutada (o por paquetes).

<sup>13</sup> Pretty Good Privacy o PGP (privacidad bastante buena) es un programa cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

---

*La información en ésta comunicación sólo aplica a los comercios afiliados a VisaNet Dominicana, R. D.*