2.2.2. Cifrado fuerte:Técnicas de codificación para protección de la información que utilizan algoritmos reconocidos internacionalmente, brindando al menos los niveles de seguridad ofrecidos por 3DES o AES.

2.2.3. Operaciones no monetarias: Son las acciones a través de las cuales se desarrollan, ejecutan o materializan los productos o servicios que prestan las entidades a sus clientes o usuarios y que no conllevan movimiento, manejo o transferencia de dinero.

2.2.4. Operaciones monetarias: Son las acciones que implican o conllevan movimiento, manejo o transferencia de dinero.

2.2.5. Autenticación: Conjunto de técnicas y procedimientos utilizados para verificar la identidad de un cliente, entidad o usuario. Los factores de autenticación son: algo que se sabe, algo que se tiene, algo que se es.

2.2.6. Mecanismos fuertes de autenticación: Se entienden como mecanismos fuertes de autenticación los siguientes:

2.2.6.1. Biometría.

2.2.6.2. Certificados de firma digital de acuerdo a lo establecido en la Ley 527 de 1999 y sus decretos reglamentarios.

2.2.6.3. OTP (One Time Password), en combinación con un segundo factor de autenticación.

2.2.6.4. Tarjetas que cumplan el estándar EMV, en combinación con un segundo factor de autenticación.

2.2.6.5. Registro y validación de algunas características de los computadores o equipos móviles desde los cuales se realizarán las operaciones, en combinación con un segundo factor de autenticación.

2.2.7. Proveedores de redes y servicios de telecomunicaciones: Son las empresas reguladas por la Comisión de Regulación de Comunicaciones y debidamente habilitadas por el Ministerio de Tecnologías de la Información y las Comunicaciones, responsables de la operación de redes y/o de la provisión de servicios de telecomunicaciones a terceros, de acuerdo a lo establecido en el art 1. de la Resolución 202 de 2010.

2.2.8 Ambiente de venta presente: transacciones en las cuales el instrumento de pago interactúa con el dispositivo de captura de información.

2.2.9 Ambiente de venta no presente: transacciones en las cuales el instrumento de pago no interactúa con el dispositivo de captura de información.

2.2.10. Entidades administradoras de pasarelas de pago: entidades que prestan servicios de aplicación de comercio electrónico para almacenar, procesar y/o transmitir el pago correspondiente a operaciones de venta en línea.

**2.2.11 Código QR (Quick Response Code): Es un código de respuesta rápida, bidimensional, con estructura cuadrada. Tiene la capacidad de almacenar datos codificados, es de** f**ácil lectura y tiene mayor capacidad de almacenamiento que los códigos universales de productos (UPC por sus siglas en inglés) o códigos de barras. Puede ser estático (su contenido no cambia, generalmente impreso) o dinámico (cambia su contenido para cada compra, generado por software en tiempo real).**

**Los códigos QR pueden ser adaptados para transacciones tales como pagos, transferencias P2P o P2B .**

## 2.3. Criterios

2.3.1. Respecto de la seguridad de la información

2.3.1.1. Confidencialidad: Hace referencia a la protección de información cuya divulgación no está autorizada.

2.3.1.2. Integridad: La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.

2.3.1.3. Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

2.3.2. Respecto de la calidad de la información

2.3.2.1. Efectividad: La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.

2.3.2.2. Eficiencia: El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.

2.3.2.3. Confiabilidad: La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones

2.3.3 Requerimientos generales

2.3.3.1. En materia de seguridad y calidad de la información

A fin de dar debida aplicación a los criterios antes indicados las entidades deben adoptar, al menos, las medidas que se relacionan a continuación:

2.3.3.1.1. Disponer de hardware, software y equipos de telecomunicaciones, así como de los procedimientos y controles necesarios, que permitan prestar los servicios y manejar la información en condiciones de seguridad y calidad.

2.3.3.1.2. Gestionar la seguridad de la información, para lo cual pueden tener como referencia el estándar ISO 27000, o el que lo sustituya.

2.3.3.1.3. Disponer que el envío de información confidencial y de los instrumentos para la realización de operaciones a sus clientes, se haga en condiciones de seguridad. Cuando dicha información se envíe como parte de, o adjunta a un correo electrónico, mensajería instantánea o cualquier otra modalidad de comunicación electrónica, ésta debe estar cifrada.

2.3.3.1.4. Dotar de seguridad la información confidencial de los clientes que se maneja en los equipos y redes de la entidad.

2.3.3.1.5. Velar porque la información enviada a los clientes esté libre de software malicioso.

2.3.3.1.6. Proteger las claves de acceso a los sistemas de información. En desarrollo de esta obligación, las entidades deben evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en los dispositivos y sistemas de cómputo de las entidades debe ser única y personalizada.

2.3.3.1.7. Dotar a sus terminales, equipos de cómputo y redes locales de los elementos necesarios que eviten la instalación de programas o dispositivos que capturen la información de sus clientes y de sus operaciones.

2.3.4.12.2. Cifrar la información de los clientes que sea remitida a los proveedores y fabricantes de tarjetas, para mantener la confidencialidad de la misma.

2.3.4.12.3. Velar porque los centros de operación en donde se realizan procesos tales como: realce, estampado, grabado y magnetización de las tarjetas, entre otros, así como de la impresión del sobreflex, mantengan procedimientos, controles y medidas de seguridad orientadas a evitar que la información relacionada pueda ser copiada, modificada o utilizada con fines diferentes a los de la fabricación de la misma.

2.3.4.12.4. Velar porque en los centros donde se realicen los procesos citados en el subnumeral anterior, apliquen procedimientos y controles que garanticen la destrucción de aquellas tarjetas que no superen las pruebas de calidad establecidas para su elaboración, así como la información de los clientes utilizada durante el proceso. Iguales medidas se deben aplicar a los sobreflex.

2.3.4.12.5. Establecer los procedimientos, controles y medidas de seguridad necesarias para la creación, asignación y entrega de las claves a los clientes.

2.3.4.12.6. Cuando la clave (PIN) asociada a una tarjeta débito haya sido asignada por la entidad vigilada, esta debe ser cambiada por el cliente antes de realizar su primera operación.

2.3.4.12.7. Ofrecer a sus clientes mecanismos que brinden la posibilidad inmediata de cambiar la clave de la tarjeta débito en el momento que éstos lo consideren necesario.

2.3.4.12.8. Establecer en los convenios que se suscriben con los establecimientos de comercio la obligación de verificar la firma y exigir la presentación del documento de identidad del cliente para las operaciones monetarias que se realicen con tarjeta de crédito.

2.3.4.12.9. Emitir tarjetas personalizadas que contengan al menos la siguiente información: nombre del cliente, indicación de si es crédito o débito, nombre de la entidad emisora, fecha de expiración, espacio para la firma del cliente y número telefónico de atención al cliente.

2.3.4.12.10. Al momento de la entrega de la tarjeta a los clientes, ésta debe estar inactiva. Las entidades deben definir un procedimiento para su respectiva activación, el cual contemple, al menos, dos de tres factores de autenticación. En cualquier caso, se deben entregar las tarjetas exclusivamente al cliente o a quien este autorice.

2.3.4.12.11. Entregar a sus clientes tarjetas débito y/o crédito que manejen internamente mecanismos fuertes de autenticación, siempre que los cupos aprobados superen 2 SMMLV. Dichas tarjetas deben servir indistintamente para realizar operaciones en cajeros automáticos (ATM) y en puntos de pago (POS).

Sin perjuicio de otras medidas de seguridad, los mecanismos fuertes de autenticación no son obligatorios en tarjetas débito asociadas a productos utilizados para canalizar recursos provenientes de programas de ayuda y/o subsidios otorgados por el Estado Colombiano siempre que estos no superen 2 SMMLV.

Lo dispuesto en los numerales 2.3.4.12.1., 2.3.4.12.2., 2.3.4.12.3., 2.3.4.12.4. y 2.3.4.12.8. de este Capítulo no debe ser cumplido cuando se trate de tarjetas virtuales.

**2.3.4.13. Operaciones por medio de códigos QR**

**Las entidades que ofrezcan la realización de pagos utilizando códigos QR deben tener como referencia** **el estándar internacional para aceptar pagos EMVCo LLC, versión 1.0 EMV® QR Code Specification for Payment Systems (EMV QRCPS) Merchant-Presented Mode, emitido en julio de 2017, o aquellos que lo modifiquen, sustituyan o adicionen y deben cumplir con los siguientes requerimientos:**

**2.3.4.13.1. Proporcionar al consumidor financiero, directamente o a través de terceros, aplicaciones de software que permitan leer el código QR y enrutar la operación.**

**2.3.4.13.2. Facilitar que los datos que no puedan ser obtenidos con la lectura del código QR estático y sean necesarios para la transacción (p.ej. monto), sean capturados por la aplicación del consumidor financiero que realiza la operación.**

**2.3.4.13.3. Cumplir con los requerimientos establecidos en los sub numerales 2.3.4.9, 2.3.4.11 y 2.3.5 del presente capítulo para la implementación del software para realizar pagos o generar los códigos QR dinámicos.**

**2.3.4.13.4. Gestionar los riesgos que se puedan derivar de la realización de este tipo de operaciones.**

**2.3.4.13.5 Con el propósito de promover la interoperabilidad, las entidades administradoras de los sistemas de Pago de Bajo Valor (SPBV) deben concertar y definir de manera conjunta la estructura de los campos donde debe enviarse la información, adicional al estándar, que resulte necesaria para la realización de las operaciones (p.ej. el código identificador del comercio y la discriminación de los impuestos). Cualquier modificación a la estructura definida debe ser informada y socializada a los participantes del sistema de pagos 3 meses antes de su implementación.**

**La información de los campos definidos debe estar a disposición de la SFC y ser publicada en el sitio web de la entidad administradora para consulta de todos los interesados.**

2.3.5 Requerimientos en materia de actualización de Software

Con el propósito de mantener un adecuado control sobre el software, las entidades deben cumplir, como mínimo, con las siguientes medidas:

2.3.5.1. Mantener tres ambientes independientes: uno para el desarrollo de software, otro para la realización de pruebas y un tercer ambiente para los sistemas en producción. En todo caso, el desempeño y la seguridad de un ambiente no pueden influir en los demás.

2.3.5.2. Implementar procedimientos que permitan verificar que las versiones de los programas del ambiente de producción corresponden a las versiones de programas fuentes catalogadas.

2.3.5.3. Cuando las entidades necesiten tomar copias de la información de sus clientes para la realización de pruebas, se deben establecer los controles necesarios para garantizar su destrucción, una vez concluidas las mismas.

2.3.5.4. Contar con procedimientos y controles para el paso de programas a producción. El software en operación debe estar catalogado.

2.3.5.5. Contar con interfaces para los clientes o usuarios que cumplan con los criterios de seguridad y calidad, de tal manera que puedan hacer uso de ellas de una forma simple e intuitiva.

2.3.5.6. Mantener documentada y actualizada, al menos, la siguiente información: parámetros de los sistemas donde operan las aplicaciones en producción, incluido el ambiente de comunicaciones; versión de los programas y aplicativos en uso; soportes de las pruebas realizadas a los sistemas de información; y procedimientos de instalación del software.

2.3.6. Tercerización – Outsourcing

Las entidades que contraten bajo la modalidad de outsourcing o tercerización, a personas naturales o jurídicas, para la atención parcial o total de los distintos canales o de los dispositivos usados en ellos, o que en desarrollo de su actividad tengan acceso a información confidencial de la entidad o de sus clientes, deben cumplir, como mínimo, con los siguientes requerimientos:

2.3.6.1. Definir los criterios y procedimientos a partir de los cuales se seleccionarán los terceros y los servicios que serán atendidos por ellos.

2.3.6.2. Incluir en los contratos que se celebren con terceros, por lo menos, los siguientes aspectos:

2.3.6.2.1. Niveles de servicio y operación.

2.3.6.2.2. Acuerdos de confidencialidad sobre la información manejada y sobre las actividades desarrolladas.