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 en combinación con un segundo factor de autenticación para operaciones no presenciales. En aquellos eventos en que la operación se efectúe de manera presencial no se requerirá el uso de un segundo factor de autenticación.

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. Participante no vigilado: Se refiere a quien haya sido autorizado por una Entidad Administradora de Sistemas de Pago de Bajo Valor (EASPBV) para tramitar órdenes de pago y de transferencia de fondos a través de su sistema y que no sea una entidad vigilada por la SFC, de conformidad con el numeral 16 del artículo 2.17.1.1.1 del Decreto 2555 de 2010).**

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 fácil 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 .

2.2.12. Tokenización: Proceso de remplazar un dato confidencial por otro equivalente que no lo es (no confidencial), el cual garantiza la misma operatividad y no tiene un valor intrínseco.

2.2.13. Característica biométrica: Atributo biológico o comportamental de un individuo del cual se pueden extraer propiedades distintivas y repetibles para su reconocimiento.

2.2.14. Muestra biométrica: Representación que se obtiene de una característica biométrica capturada mediante un dispositivo vinculado a un sistema biométrico, como una imagen facial, una grabación de voz o una imagen de huella digital.

2.2.15. Plantilla biométrica: Representación de una o varias muestras biométricas utilizadas para la comparación, reconocimiento e individualización de una persona, las cuales pueden construirse a través de métodos tales como vectores, datos numéricos y algoritmos criptográficos.

2.2.16. Omnicanalidad: Estrategia que busca mejorar la experiencia del consumidor y la eficiencia operativa, proporcionando la mayor homogeneidad posible en los diferentes canales y el uso de varios de ellos en la ejecución de las operaciones, cuando esto resulte procedente.

2.2.17. Pagos sin contacto (*contactless*): Sistema que permite pagar una compra mediante tecnologías de identificación por radiofrecuencia o lectura electrónica, incorporadas en tarjetas de crédito o débito, llaveros, tarjetas inteligentes, teléfonos móviles u otros dispositivos.

## 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:

2.3.6.2.3. Propiedad de la información.

2.3.6.2.4. Restricciones sobre el software empleado.

2.3.6.2.5. Normas de seguridad informática y física a ser aplicadas.

2.3.6.2.6. Procedimientos a seguir cuando se encuentre evidencia de alteración o manipulación de dispositivos o información.

2.3.6.2.7. Procedimientos y controles para la entrega de la información manejada y la destrucción de la misma por parte del tercero una vez finalizado el servicio.

Las entidades deben contar con los procedimientos necesarios para verificar el cumplimiento de las obligaciones señaladas en el presente subnumeral, los cuales deben ser informados previamente a la auditoría interna o quien ejerza sus funciones.

2.3.6.3. Exigir que los terceros contratados dispongan de planes de contingencia y continuidad debidamente documentados. Las entidades deben verificar que los planes, en lo que corresponde a los servicios convenidos, funcionen en las condiciones pactadas.

2.3.6.4. Establecer procedimientos que permitan identificar físicamente, de manera inequívoca, a los funcionarios de los terceros contratados.

2.3.6.5. Implementar mecanismos de cifrado fuerte para el envío y recepción de información confidencial con los terceros contratados.

2.3.7 Análisis de vulnerabilidades

Las entidades deben implementar un sistema de análisis de vulnerabilidades informáticas que cumpla al menos con los siguientes requisitos:

2.3.7.1. Estar basado en un hardware de propósito específico (appliance) totalmente separado e independiente de cualquier dispositivo de procesamiento de información, de comunicaciones y/o de seguridad informática.

2.3.7.2. Generar de manera automática por lo menos 2 veces al año un informe consolidado de las vulnerabilidades encontradas. Los informes de los últimos 2 años deben estar a disposición de la SFC.

2.3.7.3. Las entidades deben tomar las medidas necesarias para remediar las vulnerabilidades detectadas en sus análisis.

2.3.7.4. Realizar un análisis diferencial de vulnerabilidades, comparando el informe actual con respecto al inmediatamente anterior.

2.3.7.5. Las herramientas usadas en el análisis de vulnerabilidades deben estar homologadas por el CVE (Common Vulnerabilities and Exposures) y actualizadas a la fecha de su utilización.

2.3.7.6. Para la generación de los informes solicitados se debe tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre.

**2.3.8. Vinculación de Participantes a las EASPBV**

**Las EASPBV que vinculen a los Participantes no vigilados a los que se refiere el subnumeral 2.2.10 de este Capítulo, que prestan servicios de aplicación de comercio electrónico para almacenar, procesar y/o transmitir el pago correspondiente a operaciones de venta en línea con tarjetas débito o crédito, deben incluir en los contratos que celebren con estos, la obligación de contar, mantener y entregar la certificación PCI-DSS, emitida por una entidad que ostente la categoría QSA (Qualified Security Assessor), y soportada por el documento AoC (“Attestation of Compliance”) correspondiente. Así mismo, las EASPBV deben verificar que la certificación PCI-DSS a que hace referencia el inciso anterior este vigente. Si el participante obligado a contar con la certificación no la mantiene vigente, no podrá continuar prestando los servicios señalados en el inciso anterior.**

2.3.9 Requerimientos mínimos para la implementación y uso de biometría como factor de autenticación electrónica.

En aquellos eventos en que las entidades usen biometría como factor de autenticación electrónica, deben realizar el proceso de verificación de la identidad del cliente contra las bases de datos de la Registraduría Nacional del Estado Civil, los operadores de servicios ciudadanos digitales o de identidad digital autorizados, o contra sus propias bases de datos.