2.3.4.4. Receptores de dinero en efectivo

Los dispositivos que permitan la recepción de dinero en efectivo deben cumplir, como mínimo, con los siguientes requerimientos:

2.3.4.4.1. Contar con mecanismos que verifiquen la autenticidad y denominación de los billetes.

2.3.4.4.2. Totalizar el monto de la operación con los billetes aceptados y permitir que el cliente o usuario confirme o no su realización. En este último caso se debe devolver la totalidad de los billetes entregados, generando el respectivo registro.

2.3.4.4.3. Las operaciones en efectivo deben realizarse en línea, afectando el saldo de la respectiva cuenta. La operación no debe quedar sujeta a verificación.

2.3.4.4.4. Los billetes no aceptados no pueden ser retenidos y deben ser retornados inmediatamente al cliente o usuario.

2.3.4.5. POS (incluye PIN Pad)

Deben cumplir, como mínimo, con los siguientes requerimientos:

2.3.4.5.1. La lectura de tarjetas solo debe hacerse a través de la lectora de los datáfonos y los PIN Pad.

2.3.4.5.2. Cumplir el estándar EMV (Europay MasterCard VISA).

2.3.4.5.3. Los administradores de las redes de este canal deben validar automáticamente la autenticidad del datáfono que se intenta conectar a ellas, así como el medio de comunicación a través del cual operará.

2.3.4.5.4. Establecer procedimientos que le permitan a los responsables de los datáfonos en los establecimientos comerciales, confirmar la identidad de los funcionarios autorizados para retirar o hacerle mantenimiento a los dispositivos.

2.3.4.5.5. Velar porque la información confidencial de los clientes y usuarios no sea almacenada o retenida en el lugar en donde los POS estén siendo utilizados.

2.3.4.5.6. Contar con mecanismos que reduzcan la posibilidad de que terceros puedan ver la clave digitada por el cliente o usuario.

2.3.4.6. Sistemas de audio respuesta (IVR)

Los sistemas de audio respuesta deben cumplir, como mínimo, con los siguientes requerimientos:

2.3.4.6.1. Permitir al cliente confirmar la información suministrada en la realización de la operación monetaria.

2.3.4.6.2. Permitir transferir la llamada a un operador, al menos en los horarios hábiles de atención al público.

2.3.4.6.3. Las entidades que permitan realizar operaciones monetarias por este canal, deben ofrecer a sus clientes mecanismos fuertes de autenticación**.**

2.3.4.7. Centro de atención telefónica (Call Center, Contact Center)

Los centros de atención telefónica deben cumplir, como mínimo, con los siguientes requerimientos:

2.3.4.7.1. Destinar un área dedicada exclusivamente para la operación de los recursos necesarios en la prestación del servicio, la cual debe contar con los controles físicos y lógicos que impidan el ingreso de personas no autorizadas, así como la extracción de la información manejada.

2.3.4.7.2. Impedir el ingreso de dispositivos que permitan almacenar o copiar cualquier tipo de información, o medios de comunicación, que no sean suministrados por la entidad.

2.3.4.7.3. Dotar a los equiposde cómputo que operan en el centro de atención telefónica de los elementos necesarios que impidan el uso de dispositivos de almacenamiento no autorizados por la entidad. Igualmente, se debe bloquear cualquier tipo de conexión a red distinta a la usada para la prestación del servicio.

2.3.4.7.4. Garantizar que los equipos de cómputo destinados a los centros de atención telefónica solo sean utilizados en la prestación de servicios por ese canal.

2.3.4.7.5. En los equipos de cómputo usados en los centros de atención telefónica no se debe permitir la navegación por internet, el envío o recepción de correo electrónico, la mensajería instantánea, ni ningún otro servicio que permita el intercambio de información, a menos que se cuente con un sistema de registro de la información enviada y recibida. Estos registros deben ser conservados por lo menos 6 meses o en el caso en que la información respectiva sea objeto o soporte de una reclamación, queja, o cualquier proceso de tipo judicial, hasta el momento en que sea resuelto.

**2.3.4.7.6. Las entidades podrán contar con los servicios del Centro de atención telefónica (Call Center, Contact Center) en áreas no exclusivas para su operación, siempre que los servicios se presten a través de personas vinculadas de forma directa, es decir, a través de un contrato de trabajo en los términos de la legislación vigente y previo el análisis de riesgo e implementación de las medidas de control para:**

1. **Preservar la confidencialidad, integridad y disponibilidad de la información.**
2. **Impedir i) la extracción, almacenamiento o copia de la información manejada, ii) el uso de dispositivos o medios de comunicación que no sean suministrados o autorizados por la entidad para la prestación del servicio, iii) el uso de redes o conexiones a redes distintas a las autorizadas para la prestación del servicio y iv) la destinación de los dispositivos y medios de comunicación para actividades distintas a la prestación de los servicios por este canal.**
3. **Fortalecer el monitoreo sobre las operaciones realizadas con productos cuya información haya sido gestionada en estos centros de atención telefónica.**

**En aquellos eventos en que los equipos de cómputo permitan el envío o recepción de correo electrónico, mensajería instantánea, o cualquier otro servicio que permita el intercambio de información, las entidades deben contar con un**

**sistema de registro de la información enviada y recibida y conservar los mismos por un periodo mínimo de 6 meses. En el caso en que la información respectiva sea objeto o soporte de una reclamación, queja o forme parte de proceso de judicial, se deberá conservar hasta el momento en que la reclamación o queja se resuelva, o el proceso finalice.**

2.3.4.8. Sistemas de acceso remoto para clientes (RAS)

Entendido como el acceso brindado por las entidades vigiladas a sus clientes para la realización de operaciones mediante el uso de aplicaciones personalizadas, utilizando generalmente enlaces dedicados

Las entidades que ofrezcan servicio de acceso remoto para la realización de operaciones monetariasdeben contar con un módulo de seguridad de hardware para el sistema, que cumpla al menos con el estándar de seguridad FIPS-140-2 (Federal Information Processing Standard), el cual debe ser de propósito específico (appliance) totalmente separado e independiente de cualquier otro dispositivo o elemento de procesamiento de información, de seguridad informática, de transmisión y/o recepción de datos, de comunicaciones, de conmutación, de enrutamiento, de gateways, de servidores de acceso remoto (RAS) y/o de concentradores.

2.3.4.9. Internet

Las entidades que ofrezcan la realización de operaciones por Internet deben cumplir con los siguientes requerimientos: