Box 3

Payment systems of *Banco de la República*: availability and technological events that occurred in 2017

One of the main functions of *Banco de la República* is to further the safe and efficient functioning of the payment systems, a job it carries out by providing banking services to financial institutions. These include access to payment systems and to trading, clearing, and custody of government bonds. These services are a central axis of the Colombian financial infrastructure and their development has contributed significantly to the effectiveness of the transmission of monetary policy, the deepening of financial markets, and the modernization of payments in the economy.

In addition, the Bank has headed up and supported initiatives that ensure that the improvement and development of the payment system infrastructure and the provision of electronic services that are focused on facilitating and making the transactions carried out by financial intermediaries and the capital market safer, more efficient and economical. These initiatives have had a profound impact on the high and low value electronic payments[1] and have contributed to the solid and safe performance of the payment systems.

Banco de la República manages seven payment systems: 1) The Electronic Check Clearing System (CEDEC in Spanish); 2) the National Interbank Electronic Clearing System (Cenit in Spanish); 3) the Deposit Account and High Value Payment Settlement System (CUD in Spanish); 4) the System of Settlement, Custody, and Central Securities Depository (DCV in Spanish); 5) the Computer System for the management of Treasury Transactions (Master); 6) Electronic Trading System (SEN), and 7) the Auction System which sells the government's public debt securities (Auctions) on the market.

An efficient and safe operation of the Payment Systems that it manages is a priority for *Banco de la República*. The availability of the systems was higher than 99.9% in 2017 and thus complied with the optimal standard in the industry of technology service[2] which has established that these must be available at least 99.9% of the time set out in the service agreements. The operation of the systems also satisfied the principles of information security.[3] This result is the product of the continuing effort to strengthen the diagnostic tools in order to decrease the probability that incidents could occur that will affect the external and internal users of the services provided.

The availability of the payment systems that the Bank manages and the technological events that materialized in 2017 are presented below.

1. Availability of Payment Systems

Estimating the availability of payment systems makes is possible to: 1) know how much internal and external users are affected; 2) analyze the causes of the events that have materialized, and 3) decrease the probability that the events will occur or reduce their impact.

The estimate of availability considers the hours that the systems must be available each year and how heavily the service delivery schedules will be used as follows: 1) *high* level, if it refers to a heavily used time period, with a high impact or volume in the operation; 2) *moderate*, if the time period is moderately heavy where the flow of operations is lower; 3) *low*, if it is at a time when the flow of operations or the impact is not significant.[4]

The availability of these systems in 2017 was above the 99.9% standard and during some timeframes, the availability of service was 100% (Graph B3.1).

The lack of availability based on time period (low, medium, and high) is presented in Graph B3.2. In general terms,

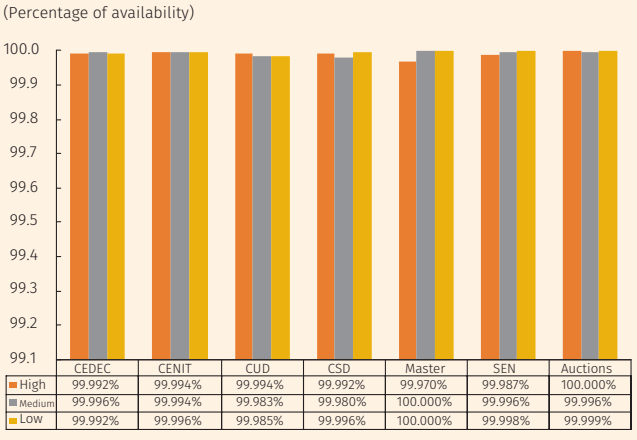
1 The Bank for International Settlements (BIS) refers to high value payments such as those that generally involve a significant amount and in which prompt payment is critically important. These are primarily exchanged by banks or financial intermediaries. The low value payments, in turn, are those that are made between consumers, companies, and the government, generally for small quantities.

2 StandardusedbyDisasterRecoveryInstituteInternational DRI

3 Best practices in information security such as the ISO 27002 standard states that this can be described on the basis of three principles: 1) the preservation of confidentiality, which ensures that access to information is properly authorized; 2) the integrity, which safeguards the precision and completeness of the information and its processing methods, and 3) the availability, which ensures that the authorized users may access the information when they need it.

4 $\%\ Availability_i = \left[\left(\frac{Annual\ hours\ not\ available}{Annual\ hours}\right)_i\right] \times 100\%,\ where\ i = \{high, Medium, low\}$

Graph B3.1
Percentage of Time Available based on Payment System in 2017



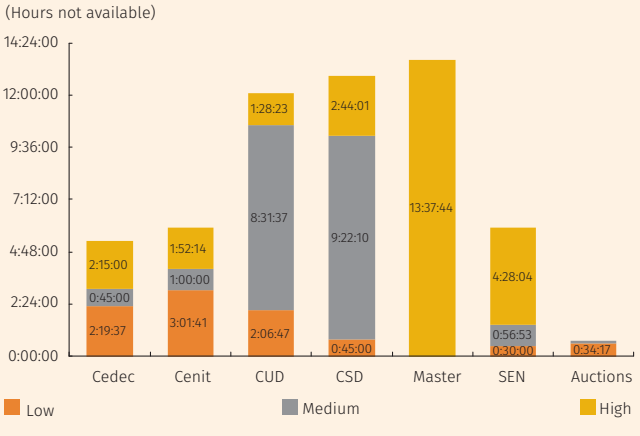
	CEDEC	CENIT	CUD	CSD	Master	SEN	Auctions
High	99.992%	99.994%	99.994%	99.992%	99.970%	99.987%	100.000%
Medium	99.996%	99.994%	99.983%	99.980%	100.000%	99.996%	99.996%
Low	99.992%	99.996%	99.985%	99.996%	100.000%	99.998%	99.999%

Source: *Banco de la República.*

such eventualities were seen to occur during periods of low or medium use. In the case of Master, this situation occurred during a period of heavy usage (13 hours and 37 minutes in the year) while this service was available 100% of the rest of the schedule (as is shown in Graph B3.1).

When 2017 is compared to 2016, a reduction in the lack of availability of the service during hours of high impact (0.010%) was registered which meant an increase of 3 hours and 17 minutes in the availability.

Graph B3.2
No Availability by Critical Information System in 2017



Source: *Banco de la República.*

2. Technological events that affected the availability of payment systems

Analyzing the technological events that affected the payment systems makes it possible to identify root causes and establish proper treatment and controls so that the systems function in accordance with what has been established in the service agreements. Guaranteeing that their workability is supported within an effective information system that maintains the confidentiality, integrity, and availability of information is also sought.

Graph B3.3 shows the root causes of the technological events that occurred in 2017. It highlights the following:

a. The *failure of software* represented 35.6% of the events that occurred (sixteen); of these, twelve correspond to the *failure of application software*[5] and two to the *failure of base software*.[6] This category includes damage to the service components that are related to the business application, security components, or elements of the base functionality layer or operating system.
b. The *change in production (implementation)* represented 20.0% of the events that have materialized (nine). This category includes events in which an error occurs in the execution of a procedure on the part of the operator or technician.[7]
c. The *saturation of resources* represented 15.6% of the events that occurred (seven). This category refers to reaching the maximum use limits of any of the resources of the service components in terms of *hardware* (memory, processor, space on the drive) or *software* (business application, security *software*, base *software* or operating system).

In the aggregate, these three root causes accounted for 71.1% of the technological events that occurred in 2017 (32 out of 45 cases).

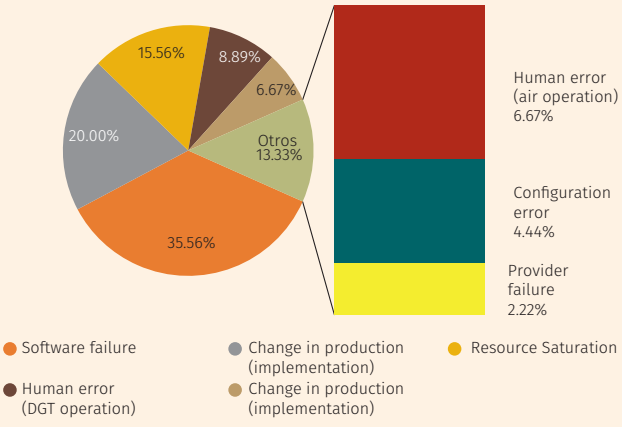
To stabilize the provision of service, the corresponding corrective actions will be carried out. Moreover, the platform for monitoring the technological risk events has been reinforced with optimization tools. This has made it possible to make diagnoses with greater timeliness and precision and take proactive actions before the moment the provision of services is started. In addition, attention protocols and warning controls have been defined that make it possible to deal with or escalate the situations that occur and resolve them expeditiously.

5 This refers to errors in the source code of a business application.

6 This refers to developer errors in some element in the software that is necessary for a business application to operate.

7 Best international practices as defined in the ITIL Standard, version 3.

Graph B3.3
Root Cause of the Technological Events in 2017



Source: *Banco de la República.*