

# BANCO CENTRAL DE RESERVA DEL PERÚ

## GUÍA PARA EL REPORTE DE INCIDENTES

### I. OBJETIVO

Establecer los criterios, alcances, responsabilidades, plazos, canales y formatos para el reporte de incidentes operativos de las Entidades Reguladas en el Sistema Nacional de Pagos.

### II. ALCANCE

Se define un incidente como la materialización de un riesgo operativo que afecta la continuidad, integridad y disponibilidad de los servicios ofrecidos por una Entidad Regulada. La lista de códigos de las entidades se encuentra en el Portal Web del BCRP.

La presente disposición tiene cobertura dentro del ámbito del Reglamento General, excluyendo el reporte de incidentes regulado en el Reglamento de los niveles de calidad de los Servicios de Pago Interoperables provistos por los Proveedores, Acuerdos, Sistemas de Pagos y Proveedores Tecnológicos, bajo la Circular N.º 0009-2024-BCRP.

### III. ÁMBITO DE APLICACIÓN

Las disposiciones aquí contenidas resultan aplicables a los incidentes relacionados al riesgo operacional y que se registren en:

- a) Infraestructuras de Pagos: Sistemas de Pagos y Acuerdos de Pago.
- b) Administradores y participantes en dichas Infraestructuras.
- c) Proveedores de Servicios de Pago.

### IV. CATEGORIZACIÓN DEL INCIDENTE

Se considera incidente a la materialización de un riesgo operativo que cumpla al menos uno de los siguientes criterios:

1. **Continuidad del servicio:** Todo evento que interrumpa o afecte la continuidad del servicio por un período superior a treinta (30) minutos consecutivos, impidiendo la ejecución normal de las operaciones. Se considera interrupciones totales o parciales del servicio que impacten las operaciones, cuyo origen pueda ser la propia entidad o un tercero.
2. **Integridad:** Pérdida, alteración o corrupción de datos que comprometa la exactitud, consistencia, confiabilidad o trazabilidad de las operaciones de pago, aun cuando el servicio se mantenga disponible, afectando la calidad de la información procesada o almacenada. Se incluyen en esta categoría los incidentes de ciberseguridad y fraude que comprometan la seguridad de la información, independientemente de si generan o no una interrupción del servicio.
3. **Disponibilidad de la información:** Todo evento que limite o impida el acceso oportuno a la información o a los sistemas por parte de los clientes o usuarios autorizados, afectando la ejecución normal de los procesos, aun cuando no se materialice una interrupción total del servicio.

# BANCO CENTRAL DE RESERVA DEL PERÚ

## V. RESPONSABILIDAD DEL REPORTE

El reporte de incidentes debe ser entregado bajo el formato del Anexo I:

1. En el caso de una Infraestructura de Pagos, los incidentes deberán ser reportados por los Administradores, quienes recopilarán la información que les remitan sus Participantes, Proveedores Tecnológicos y Agentes Terceros.
2. Los Proveedores de Servicios de Pago que operan fuera de una infraestructura.

Cada entidad deberá designar a dos funcionarios responsables (titular y suplente) ante el Banco Central, así como sus datos de contacto (nombres, cargo, correo electrónico institucional y teléfono).

El funcionario responsable consolidará la información y enviará el reporte mediante el canal oficial (SIBFTP) u otro que indique el BCRP. Para ello, los funcionarios responsables deberán contar con un acceso al canal SIBFTP, para carga y envío de reportes (ver Guía de Acceso al canal SIBFTP en el Portal Web del BCRP).

En caso de contingencia (SIBFTP no disponible), el reporte debe ser enviado al correo electrónico [Dpto.AnalisisSistPagos@bcrp.gob.pe](mailto:Dpto.AnalisisSistPagos@bcrp.gob.pe).

El BCRP puede solicitar información adicional a la Entidad Regulada con la finalidad de conocer la naturaleza e impacto del incidente; así como las medidas que se adopten para su resolución y evitar que se repita en el futuro

## VI. PLAZO PARA EL ENVÍO

El plazo para el envío del reporte es al día siguiente hábil de la fecha de inicio del incidente<sup>1</sup>.

## VII. FLUJO DE REPORTE

1. Detección del incidente por la entidad responsable del reporte.
2. Identificación del servicio afectado y de las entidades participantes involucradas.
3. Registro interno y notificación al funcionario responsable.
4. Consolidación de la información en el formato del **Anexo 01 adjunto**.
5. Envío al BCRP mediante SIBFTP u otro canal que se indique.
6. Revisión del BCRP y programación de reuniones de seguimiento, si corresponde.

---

<sup>1</sup> El envío del reporte indicado no exime la obligación de remitir los demás informes requeridos, incluidos aquellos que contengan consolidados de incidentes, conforme a lo dispuesto en el Reglamento General y en las demás normas aplicables.

# BANCO CENTRAL DE RESERVA DEL PERÚ

## ANEXO 01: FORMATO DE REPORTE<sup>2</sup>

### NOMBRE DEL ARCHIVO

| Longitud | Posición |    | Detalle                                                                                                      |
|----------|----------|----|--------------------------------------------------------------------------------------------------------------|
| 4        | 1        | 4  | Código BCRP de la Entidad Regulada que reporta (ver lista de códigos de entidades en el Portal Web del BCRP) |
| 12       | 5        | 16 | Fecha y hora de inicio del incidente (DDMM AAAAHHMM)                                                         |
| 2        | 17       | 18 | Número secuencial diario del incidente. <sup>3</sup>                                                         |

### CABECERA DEL ARCHIVO (Primera línea del reporte)

| Longitud | Posición |    | Detalle <sup>4</sup>                                                                                         |
|----------|----------|----|--------------------------------------------------------------------------------------------------------------|
| 4        | 1        | 4  | Código BCRP de la Entidad Regulada que reporta (ver lista de códigos de entidades en el Portal Web del BCRP) |
| 12       | 5        | 16 | Fecha y Hora de inicio del incidente (DDMM AAAAHHMM)                                                         |
| 12       | 17       | 28 | Fecha y Hora de finalización del incidente (DDMM AAAAHHMM) <sup>5</sup>                                      |
| 3        | 29       | 31 | Código de entidad origen del incidente (Catálogo 1)                                                          |
| 3        | 32       | 34 | Código de fuente del incidente (Catálogo 2)                                                                  |
| 30       | 35       | 64 | Nombre del funcionario responsable                                                                           |
| 20       | 65       | 84 | Correo del funcionario responsable                                                                           |
| 1        | 85       | 85 | Continuidad (Catálogo 3)                                                                                     |
| 1        | 86       | 86 | Integridad (Catálogo 3)                                                                                      |
| 1        | 87       | 87 | Disponibilidad (Catálogo 3)                                                                                  |

### DATA (Segunda línea del reporte)

| Longitud | Posición |      | Detalle                                                                        |
|----------|----------|------|--------------------------------------------------------------------------------|
| 500      | 1        | 500  | Descripción del Incidente                                                      |
| 200      | 501      | 700  | Identificación del Servicio Afectado y de entidades participantes involucradas |
| 300      | 701      | 1000 | Descripción de Acciones Tomadas                                                |
| 500      | 1001     | 1500 | Descripción de la Solución Final                                               |

### CATÁLOGOS:

#### CATÁLOGO 1. ENTIDAD ORIGEN DEL INCIDENTE

| Código | Nombre        |
|--------|---------------|
| S01    | Administrador |
| S02    | Participante  |

<sup>2</sup> El formato del archivo debe ser TXT.

<sup>3</sup> Corresponde al orden en que se registran los incidentes en una misma fecha (ejemplo: 01, 02, 03, ...). Se reinicia cada día. Por cada servicio afectado se debe remitir un reporte de incidente distinto.

<sup>4</sup> En caso de que el nombre o correo del funcionario responsable tenga menos caracteres que la cantidad establecida, el campo deberá completarse con ceros (0) a la izquierda hasta alcanzar la longitud indicada.

<sup>5</sup> Este campo deberá completarse con doce ceros (000000000000) si el incidente no ha sido finalizado. En caso contrario, deberá consignarse la fecha de término correspondiente en el formato indicado.

# BANCO CENTRAL DE RESERVA DEL PERÚ

|     |                                     |
|-----|-------------------------------------|
| S03 | Entidad de Servicios de Pago        |
| S04 | Proveedor de Servicios Tecnológicos |
| S05 | Entidad Tercera                     |

## CATÁLOGO 2. FUENTE DEL INCIDENTE OPERATIVO

| Código de la fuente del incidente | Nombre           | Descripción                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| I01                               | Acción maliciosa | Incidentes operacionales originados por acciones deliberadas de carácter malicioso, tales como código malicioso, intrusiones, ataques distribuidos o de denegación de servicio (DDoS), acciones internas intencionales, daños físicos deliberados, compromisos de seguridad de la información, fraude u otras acciones similares que afecten la operación. |
| I02                               | Falla interna    | Incidentes operacionales causados por errores involuntarios de personas, fallas de sistemas, aplicaciones, infraestructura tecnológica o deficiencias en procesos internos que impacten la continuidad o calidad de la operación.                                                                                                                          |
| I03                               | Evento externo   | Incidentes operacionales cuya causa se origina en eventos fuera del control directo de la organización, como desastres naturales, fallas de proveedores de servicios tecnológicos, interrupciones de servicios públicos u otros eventos externos que afecten la operación.                                                                                 |
| I04                               | No determinado   | Incidentes operacionales cuya fuente no ha podido ser determinada al momento del envío del reporte, quedando sujeta a análisis posterior.                                                                                                                                                                                                                  |

## CATÁLOGO 3. CLASIFICACIÓN DEL INCIDENTE

En la cabecera del archivo, se deberá marcar con '1' el criterio o los criterios afectados (Continuidad del servicio, Integridad y Disponibilidad de la información) y con '0' los que no apliquen.

| Valor | Descripción |
|-------|-------------|
| 1     | Aplica      |
| 0     | No aplica   |