

Lima, 15 de Setiembre de 2026

RESOLUCIÓN SBS
N° 02271-2026

El Superintendente de Banca, Seguros y
Administradoras Privadas de Fondos de Pensiones

CONSIDERANDO:

Que, la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones es el organismo encargado de regular, supervisar y fiscalizar a las entidades del sistema financiero, del sistema de seguros y del sistema privado de pensiones, así como a otras entidades cuya supervisión le haya sido atribuida por otras leyes especiales, conforme a lo dispuesto en la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, aprobada por la Ley N° 26702 y normas modificatorias (en adelante, la Ley General), la Ley del Sistema Privado de Administración de Fondos de Pensiones, cuyo Texto Único Ordenado fue aprobado por el Decreto Supremo N° 054-97-EF, y otras leyes;

Que, mediante la Trigésima Segunda Disposición Final y Complementaria de la Ley General, se establecen disposiciones aplicables a la publicación de proyectos normativos;

Que, dicha disposición es concordante con el artículo IV del Título Preliminar de la Ley N° 27444, Ley del Procedimiento Administrativo General, que establece el principio de participación de los administrados en el proceso de decisiones públicas, así como con el capítulo IV del "Reglamento que establece disposiciones sobre publicación y difusión de normas jurídicas de carácter general, resoluciones y proyectos normativos", aprobado por el Decreto Supremo N° 009-2024-JUS;

Que, resulta conveniente reemplazar el reporte de eventos de interrupción significativa de operaciones y el reporte de incidentes de ciberseguridad significativos por un reporte de incidentes operacionales a fin de estandarizar la información que se remite a la Superintendencia;

Que, asimismo, resulta necesario establecer lineamientos para el reporte de incidentes operacionales significativos, lo cual incluye, en base a la experiencia de supervisión, contar con reportes iniciales, intermedios y finales de los incidentes que presenten los supervisados;

Que, en cumplimiento del marco normativo antes referido, la Superintendencia dispone aprobar mediante resolución de Superintendencia sus proyectos normativos y publicarlos en su sede digital con el objetivo de asegurar la participación efectiva del público en general;

Con el visto bueno de las Superintendencias Adjuntas de Banca y Microfinanzas, de Seguros, de Pensiones y de Regulación y Jurídica, así como de la Gerencia de Riesgos;



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

RESUELVE:

Artículo Primero. - Autorizar la difusión en consulta pública, en la sede digital de la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (www.sbs.gob.pe), del proyecto normativo que reemplaza el reporte de eventos de interrupción significativa de operaciones y el reporte de incidentes de ciberseguridad significativos por un reporte de incidentes operacionales y establece lineamientos para dicho reporte, lo cual incluye, contar con reportes iniciales, intermedios y finales de los incidentes que presenten los supervisados.

Artículo Segundo. - El plazo para que el público en general pueda remitir a la Superintendencia de Banca, Seguros y AFP sus comentarios y observaciones sobre el proyecto señalado en el artículo anterior es de treinta (30) días calendario, contados desde el día siguiente de la fecha de publicación de la presente resolución en el Diario Oficial El Peruano.

Regístrese, comuníquese y publíquese

SERGIO JAVIER ESPINOSA CHIROQUE
SUPERINTENDENTE DE BANCA, SEGUROS Y AFP

«TipoExpedienteSbs»
Nº «NumExpedienteSbs»
El Superintendente de Banca, Seguros y
Administradoras Privadas de Fondos de Pensiones,

CONSIDERANDO

Que mediante Resolución SBS N° 877-2020 se aprobó el Reglamento para la Gestión de la Continuidad del Negocio, el cual establece disposiciones que las empresas deben cumplir para la adecuada gestión de la continuidad del negocio;

Que el Reglamento para la Gestión de la Continuidad del Negocio establece que las empresas deben reportar a la Superintendencia la ocurrencia de eventos significativos de interrupción de operaciones;

Que mediante Resolución SBS N° 504-2021 se aprobó el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, con la finalidad de fortalecer las capacidades de ciberseguridad y procesos de autenticación de las empresas;

Que el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad establece que las empresas deben reportar a la Superintendencia la ocurrencia de incidentes de ciberseguridad significativos;

Que la Unión Europea aprobó el Reglamento de Resiliencia Operativa Digital (DORA) en 2022, el cual tiene como objetivo garantizar que las entidades financieras puedan mantener la resiliencia operacional frente a los riesgos digitales, como ciberataques, fallas tecnológicas, o cualquier incidente que pueda afectar la continuidad de los servicios financieros;

Que el Consejo de Estabilidad Financiera (FSB) ha desarrollado desde 2023 el Formato para el Intercambio de Reporte de Incidentes (FIRE) para reducir la fragmentación en el reporte de incidentes operativos, incluidos los incidentes de ciberseguridad, y mejorar la cooperación transfronteriza;

Que, tanto el DORA como el FIRE establecen que, frente a incidentes operacionales, deben remitirse a las autoridades competentes informes iniciales, intermedios y finales; los cuales deben brindar secuencialmente más información y mayor detalle sobre dichos incidentes;

Que, con el fin de estandarizar la información que se remite a la Superintendencia, resulta conveniente reemplazar el reporte de eventos de interrupción significativa de operaciones y el reporte de incidentes de ciberseguridad significativos por un reporte de incidentes operacionales;

Que, asimismo, resulta necesario establecer lineamientos para el reporte de incidentes operacionales significativos, lo cual incluye, en base a la experiencia de supervisión, contar con reportes iniciales, intermedios y finales de los incidentes que presenten los supervisados;

Que, a efectos de recoger las opiniones del público sobre lo propuesto, se dispone la publicación del proyecto de resolución en la sede digital de la Superintendencia, al amparo de lo dispuesto en la Trigésimo Segunda Disposición Final y Complementaria de la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros - Ley N° 26702 y sus normas modificatorias, en adelante Ley General, así como del Decreto Supremo N° 009-2024- JUS;

Contando con el visto bueno de las Superintendencias Adjuntas de Banca y Microfinanzas, de Seguros, de Administradoras Privadas de Fondos de Pensiones, de Regulación y Jurídica, y de la Gerencia de Riesgos;

En uso de las atribuciones conferidas por los numerales 7 y 9 del artículo 349 de la Ley General,

RESUELVE:

Artículo Primero. Aprobar el Procedimiento para el Reporte de Incidentes Operacionales Significativos, de acuerdo con lo siguiente:

PROCEDIMIENTO PARA EL REPORTE DE INCIDENTES OPERACIONALES SIGNIFICATIVOS

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1. Alcance

- 1.1 El presente Procedimiento es de aplicación a las empresas comprendidas en los literales A y D del artículo 16, y en los numerales 2 y 4 del artículo 17 de la Ley General, así como a las Administradoras Privadas de Fondos de Pensiones (AFP) y al Banco de la Nación, en adelante empresas.
- 1.2 En el caso de las empresas de crédito a las que se refiere el numeral 5 del literal A del artículo 16 de la Ley General, el presente Procedimiento es de aplicación únicamente si cuentan con autorización para operar con dinero electrónico o tarjetas de crédito, o si brindan servicios de pagos interoperables.

Artículo 2. Definiciones

Para la aplicación del presente Procedimiento deben considerarse las siguientes definiciones:

- a) **Empresas con concentración de mercado:** Empresas sujetas al requerimiento de patrimonio efectivo por riesgo por concentración de mercado, de acuerdo con lo señalado en el Reglamento para el Requerimiento de Colchones de Conservación, por Ciclo Económico y por Riesgo por Concentración de Mercado, aprobado por la Resolución SBS N° 3954-2022 y sus modificatorias, o norma que lo sustituya. Para efecto del presente Procedimiento, en el caso de empresas sujetas al requerimiento antes mencionado que pertenezcan a un mismo grupo económico, de acuerdo con la definición contemplada en las Normas Especiales sobre Vinculación y Grupo Económico aprobadas por la Resolución SBS N° 5780-2015 o norma que las sustituya, sólo se



considera como empresa con concentración de mercado a aquella empresa del grupo económico que tenga el mayor nivel de activos.

- b) **Evento:** Un suceso o serie de sucesos que pueden ser internos o externos a la empresa, originados por la misma causa, que ocurren durante el mismo periodo de tiempo.
- c) **Evento de interrupción significativa de operaciones:** Evento que comprende la suspensión en la entrega de los productos y servicios priorizados, la activación del plan de gestión de crisis o la interrupción de los canales de atención, cuando cumple con los supuestos establecidos en los párrafos 15.1, 15.2 o 15.3 del artículo 15 del Reglamento para la Gestión de la Continuidad del Negocio.
- d) **Incidente:** Evento que se ha determinado que tiene o podría tener un impacto adverso sobre la empresa y que requiere de acciones de respuesta y recuperación.
- e) **Incidente de seguridad significativo:** Para efectos del presente procedimiento, comprende los incidentes de ciberseguridad que presentan un impacto adverso significativo, verificado o presumible, incluyendo la pérdida o hurto de información de la empresa o de clientes, el fraude interno o externo, el impacto negativo en la imagen y reputación de la empresa o la interrupción de operaciones, conforme al artículo 15 del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad; así como otros incidentes que presentan un impacto adverso significativo sobre la confidencialidad, integridad o disponibilidad de la información de la empresa o de sus clientes.
- f) **Incidente operacional:** Incidente cuyo origen corresponde a factores relacionados con personas, procesos, tecnología, instalaciones, terceros o eventos externos, y que genera o podría generar impactos financieros; legales o regulatorios; en la continuidad operativa; en clientes, usuarios u otros grupos de interés; o en la reputación de la empresa.
- g) **Reclasificación de incidentes:** Modificación de la clasificación inicial de un incidente operacional como significativo o no significativo, como resultado de la evaluación de nueva información o de la reevaluación de la información disponible.
- h) **Reglamento para la Gestión de la Continuidad del Negocio:** Reglamento para la Gestión de la Continuidad del Negocio, aprobado por la Resolución SBS N° 877-2020 y sus modificatorias, o norma que lo sustituya.
- i) **Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad:** Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado por la Resolución SBS N° 504-2021 y sus modificatorias, o norma que lo sustituya.
- j) **Tiempo de detección:** Momento en el cual la empresa identifica por primera vez la ocurrencia de un incidente a partir de una alerta, indicio o cualquier medio de detección, independientemente de su confirmación posterior o de su registro formal como incidente.
- k) **Tiempo de resolución:** Momento en el cual el incidente ha sido contenido, sus impactos inmediatos han sido mitigados o eliminados, y el servicio, proceso o función afectada ha sido restablecido a un estado operativo aceptable, el cual debe ser definido por la empresa considerando, según corresponda, el objetivo de recuperación del negocio definido conforme al Reglamento para la Gestión de la Continuidad del Negocio.
- l) **Tiempo de cierre:** Momento en el cual se concluye la revisión formal posterior al incidente, tras lo cual el incidente se considera formalmente cerrado desde el punto de vista de gestión.

Artículo 3. Tipología de incidentes operacionales

3.1 Los incidentes operacionales se clasifican en las siguientes categorías:



- a) **Interrupción del negocio, falla de sistema o de ejecución:** Incidente operacional que afecta o puede afectar la provisión de servicios, actividades o funciones de la empresa.
 - b) **Compromiso no disruptivo:** Violación de la seguridad de un sistema de información que no interrumpe la provisión de servicios de la empresa.
 - c) **Vulneración de datos:** Acceso, divulgación, alteración, pérdida o destrucción no autorizada de datos.
 - d) **Fraude financiero:** Actos deliberados orientados a la obtención de un beneficio financiero no autorizado, incluyendo el robo.
 - e) **Desorden informativo:** Difusión de información falsa, manipulada o malintencionada que pueda afectar a la entidad o sus grupos de interés.
- 3.2 Las categorías mencionadas en el párrafo anterior no tienen carácter excluyente, por lo que un incidente operacional puede corresponder a más de una categoría de manera simultánea.
- 3.3 La clasificación de un incidente operacional en una o más categorías no condiciona su calificación como significativo, la cual debe evaluarse de manera integral conforme al artículo 4.

Artículo 4. Incidentes operacionales significativos

- 4.1 Son incidentes operacionales significativos aquellos que representan un impacto adverso significativo, verificado o presumible, a nivel financiero, legal o regulatorio; en la continuidad operativa; en clientes, usuarios u otros grupos de interés; en la reputación de la empresa; o en la estabilidad del sistema financiero, de seguros, previsional o cooperativo.
- 4.2 Asimismo, se consideran incidentes operacionales significativos los eventos de interrupción significativa de operaciones y los incidentes de seguridad significativos, los cuales son significativos en virtud de las disposiciones del Reglamento para la Gestión de la Continuidad del Negocio y del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, respectivamente.
- 4.3 La empresa debe establecer e implementar políticas, procedimientos y controles para la gestión integral de los incidentes operacionales, que comprendan su identificación, evaluación, clasificación y, cuando corresponda, reclasificación; así como su respuesta, contención, recuperación, seguimiento y cierre. Estos procedimientos deben asegurar el cumplimiento de las obligaciones de reporte previstas en el presente Procedimiento.
- 4.4 Los procedimientos a los que se refiere el párrafo 4.3 deben permitir estimar, monitorear y actualizar la magnitud de los impactos adversos asociados a los incidentes operacionales, conforme se disponga de nueva información. Dicha estimación constituye la base para la clasificación y reclasificación previstas en los párrafos 4.5 y 4.7.
- 4.5 La clasificación y reclasificación de un incidente operacional como significativo o no significativo se efectúa en función de la magnitud de sus impactos adversos, conforme a criterios que deben considerar, entre otros, los siguientes:
- a) la magnitud del impacto financiero potencial, incluyendo pérdidas directas o indirectas;
 - b) la existencia de potenciales incumplimientos normativos, sanciones o contingencias legales;
 - c) la duración o recurrencia del incidente;
 - d) la criticidad de los procesos, servicios o funciones afectados;



- e) el alcance en términos de clientes, afiliados o usuarios potencialmente afectados;
 - f) la afectación potencial de los derechos de los clientes o afiliados;
 - g) la afectación en la percepción, confianza o imagen de la empresa;
 - h) la afectación a la confidencialidad, integridad o disponibilidad de la información;
 - i) la afectación o alteración de activos críticos de tecnología de la información y las comunicaciones (TIC); o
 - j) el potencial impacto en el sistema financiero, de seguros, previsional, cooperativo, incluyendo efectos en la estabilidad o continuidad de los servicios prestados a otras entidades o sistemas.
- 4.6 La empresa debe definir, en su procedimiento, los umbrales a partir de los cuales el impacto asociado a los criterios del párrafo 4.5 se considera significativo. Estos umbrales, así como sus modificaciones, deben ser aprobados por el Directorio. Asimismo, deben revisarse periódicamente y actualizarse cuando las circunstancias lo justifiquen.
- 4.7 La reclasificación de un incidente operacional de significativo a no significativo solo procede cuando se determine que la clasificación inicial se sustentó en un error en la evaluación o en la información disponible en ese momento. La atenuación, mitigación o reversión posterior de los impactos no constituye fundamento para dicha reclasificación, dado que el carácter significativo se determina por los impactos adversos materializados, los cuales no se desvirtúan por su evolución posterior. Toda reclasificación a no significativo debe quedar registrada y justificada.
- 4.8 El procedimiento a que se refiere el párrafo 4.3 debe asegurar la aplicación continua de los criterios y umbrales previstos en los párrafos 4.5 y 4.6, e incorporar reglas y controles que permitan identificar de forma temprana cuándo corresponde clasificar o reclasificar un incidente operacional como significativo.

Artículo 5. Estado de los incidentes operacionales significativos

- 5.1 El estado de los incidentes operacionales significativos puede ser Abierto, Resuelto o Cerrado, de acuerdo con lo siguiente:
- a) **Abierto:** estado comprendido entre el tiempo de detección y el tiempo de resolución, durante el cual la empresa gestiona activamente el incidente, ejecuta acciones de respuesta y contención, controla los impactos y trabaja en la restauración del servicio o proceso afectado, sin que aún se haya logrado una solución definitiva.
 - b) **Resuelto:** estado comprendido entre el tiempo de resolución y el tiempo de cierre, en el cual el incidente ha sido contenido y los efectos negativos inmediatos han sido mitigados o eliminados, mediante la implementación de soluciones temporales o definitivas, permitiendo el restablecimiento a un estado operativo aceptable. Durante este periodo se debe llevar a cabo la revisión formal posterior al incidente, incluyendo el análisis de causa raíz y la definición de acciones correctivas y preventivas.
 - c) **Cerrado:** estado posterior a la revisión formal del incidente, en el cual las causas han sido identificadas, las lecciones aprendidas documentadas y las acciones correctivas y preventivas definidas, aprobadas y asignadas para su ejecución. El incidente se considera formalmente finalizado desde el punto de vista de gestión y control.
- 5.2 La empresa debe identificar el estado del incidente antes del envío de cada reporte a la Superintendencia, reflejando la situación del incidente a dicho momento.



Artículo 6. Registro de incidentes operacionales

- 6.1 La empresa debe mantener un registro centralizado y actualizado de los incidentes operacionales, sean o no significativos, el cual debe estar a disposición de la Superintendencia para su consulta en cualquier momento. Para tal efecto, la empresa debe asegurar la protección de la información contenida en dicho registro frente a alteraciones accidentales o intencionadas.
- 6.2 El registro de incidentes operacionales debe apoyar los procesos de análisis, seguimiento y reporte, y contener, como mínimo, los siguientes campos:
- a) ID interno del incidente
 - b) Responsable de la gestión integral del incidente
 - c) Descripción del incidente
 - d) Clasificación del incidente operacional como significativo o no significativo, incluyendo la fecha y hora de clasificación como significativo, de corresponder.
 - e) Fecha y hora de inicio del incidente operacional
 - f) Fecha y hora de detección del incidente operacional
 - g) Fecha y hora del restablecimiento a operaciones normales
 - h) Fecha y hora de reclasificación del incidente operacional como no significativo
 - i) Fechas y horas de reporte a la Superintendencia y tipos de reportes remitidos
 - j) Acciones ejecutadas durante el incidente
 - k) Productos y servicios afectados
 - l) Canales afectados
 - m) Proveedores involucrados, de ser el caso
 - n) Causas conocidas o preliminares
 - o) Acciones correctivas y preventivas definidas para el incidente, incluyendo su estado de implementación y, de ser el caso, la fecha de implementación
- 6.3 La empresa debe registrar oportunamente los incidentes operacionales en el registro desde su detección. Los campos deben completarse y actualizarse de manera continua, conforme se disponga de nueva información.
- 6.4 El registro de incidentes operacionales podrá integrarse con el registro centralizado de eventos de interrupción de la provisión de productos y servicios priorizados a través de canales digitales, exigido por el párrafo 18.4 del artículo 18 del Reglamento para la Gestión de la Continuidad del Negocio, así como con otros registros exigidos por la normativa vigente de la gestión de riesgos, siempre que se asegure el cumplimiento de los requisitos y campos mínimos exigidos por cada normativa, así como la consistencia, integridad y trazabilidad de la información.
- 6.5 En base al registro de incidentes operacionales, las empresas deben realizar análisis de tendencias, identificación de incidentes recurrentes y evaluación de la efectividad de las acciones correctivas y preventivas adoptadas.

CAPÍTULO II
FASES DEL REPORTE DE INCIDENTES OPERACIONALES SIGNIFICATIVOS



Artículo 7. Reporte inicial de incidentes operacionales significativos

- 7.1 La empresa debe remitir a la Superintendencia un reporte inicial de incidentes operacionales significativos de acuerdo con los siguientes plazos computados desde el tiempo de clasificación como significativo del incidente, según corresponda:
- a) Dentro de un plazo de dos (02) horas en el caso de empresas con concentración de mercado;
 - b) Dentro de un plazo de cinco (05) horas en el caso de las empresas bancarias, las empresas financieras, las CMAC, la CMCP y las CRAC;
 - c) Dentro de un plazo de un (01) día hábil en el caso de las empresas distintas a las señaladas en los literales a) y b) del presente párrafo.
- 7.2 Sin perjuicio de los plazos establecidos en el párrafo 7.1, las empresas comprendidas en los literales a) y b) de dicho párrafo deben remitir el reporte inicial dentro de los plazos allí previstos y, en cualquier caso, dentro de un plazo máximo de veinticuatro (24) horas computado desde el tiempo de detección del incidente.
- 7.3 Cuando la empresa cuente con información suficiente para determinar que un incidente calificado inicialmente como no significativo es significativo, estará obligada a reclasificarlo. Los plazos de remisión del párrafo 7.1 correrán estrictamente desde el momento en que se tuvo acceso a dicha información.
- 7.4 En el caso de eventos de interrupción significativa de operaciones, los plazos para la remisión del reporte inicial de incidentes operacionales significativos son computados desde el tiempo de inicio, conforme con lo establecido en el Reglamento para la Gestión de la Continuidad del Negocio. Al respecto, la empresa deberá remitir a la Superintendencia el reporte inicial de incidentes operacionales significativos en los plazos establecidos en los párrafos 15.1, 15.2 y 15.3 del artículo 15 de dicho Reglamento.
- 7.5 Cuando un mismo incidente configure simultáneamente un evento de interrupción significativa de operaciones y un incidente de seguridad significativo o cualquier otro incidente operacional significativo, la empresa debe remitir un único reporte inicial. En tal caso, el plazo para remisión de dicho reporte es el correspondiente al establecido en el artículo 15 en el Reglamento para la Gestión de la Continuidad del Negocio.
- 7.6 La empresa debe remitir el reporte inicial de incidentes operacionales significativos en el formato respectivo de acuerdo con lo siguiente:
- a) Si el estado del incidente al momento del reporte inicial es Abierto, debe remitir el formato IOS-A.
 - b) Si el estado del incidente al momento del reporte inicial es Resuelto, debe remitir el formato IOS-B.
- 7.7 El reporte inicial tiene carácter preliminar y puede contener información estimada, siempre que permita a la Superintendencia conocer oportunamente la ocurrencia del incidente y su impacto potencial.
- 7.8 Si, posteriormente al envío del reporte inicial de incidentes operacionales significativos, la empresa reclasifica el incidente operacional como no significativo, deberá remitir nuevamente el formato IOS-



A con los campos de reclasificación completos dentro de un plazo máximo de un (01) día hábil desde el tiempo de reclasificación. En ningún otro supuesto deben completarse los campos de reclasificación.

- 7.9 Los reportes iniciales de incidentes operacionales significativos no podrán registrar el estado "Cerrado", a menos que el incidente sea reclasificado como "no significativo". Este supuesto constituye la única excepción bajo la cual el formato IOS-A admitirá dicho estado.
- 7.10 Cuando el vencimiento del plazo máximo para la remisión ocurra después de las 4:00 p. m. y hasta las 7:00 a. m. del día siguiente, o en un día no hábil, el reporte deberá remitirse, como máximo, al inicio de la siguiente jornada hábil. Lo dispuesto en el presente párrafo no aplica a aquellos incidentes que correspondan a eventos de interrupción significativa de operaciones, los cuales se rigen por lo establecido en el Reglamento para la Gestión de la Continuidad del Negocio.

Artículo 8. Reporte intermedio de incidentes operacionales significativos

- 8.1 Una vez remitido el reporte inicial de incidentes operacionales significativos correspondiente a un incidente en estado Abierto, la empresa deberá remitir un primer reporte intermedio dentro de un plazo máximo de veinticuatro (24) horas computadas a partir del envío del reporte inicial, aplicando, de corresponder, la regla de cómputo de plazos prevista en el párrafo 7.10.
- 8.2 Si al momento del envío del primer reporte intermedio el incidente se encontrara en estado Resuelto, no corresponde remitir reportes intermedios adicionales y el siguiente reporte a remitir corresponde al reporte final de acuerdo con lo señalado en el artículo 9 del presente Procedimiento.
- 8.3 Si al momento del envío del primer reporte intermedio el incidente continuara en estado Abierto, la empresa debe remitir reportes intermedios cuando exista información relevante y actualizada que compartir, hasta que el incidente sea resuelto. La Superintendencia puede establecer una frecuencia mínima de remisión de reportes intermedios actualizados.
- 8.4 Una vez se resuelva el incidente la empresa debe remitir un último reporte intermedio con estado "Resuelto" en un plazo máximo de un (01) día hábil contado desde el tiempo de resolución del incidente.
- 8.5 Luego del envío del último reporte intermedio conforme a lo señalado en el párrafo precedente, o cuando se hubiera remitido un reporte inicial con estado Resuelto, la empresa no deberá remitir reportes intermedios adicionales a la Superintendencia, salvo requerimiento expreso de esta.
- 8.6 Los reportes intermedios de incidentes operacionales significativos deberán remitirse según el formato IOS-B.

Artículo 9. Reporte final de incidentes operacionales significativos

- 9.1 A partir del tiempo de resolución del incidente, la empresa debe remitir a la Superintendencia un reporte final de incidentes operacionales significativos en un plazo máximo de 20 días hábiles. Al momento de la remisión del reporte final, la empresa debe haber cerrado el incidente y, por lo tanto, reportarlo en estado cerrado. El plazo para remitir el reporte final podrá ser ampliado por única vez mediante requerimiento justificado realizado ante esta Superintendencia antes del vencimiento del plazo de envío del reporte final.



- 9.2 En el caso de incidentes de seguridad significativos, la empresa debe haber efectuado el análisis forense al que se refiere el párrafo 15.2 del Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad previamente a la remisión del reporte final.
- 9.3 La empresa debe haber efectuado un análisis de causa raíz previamente a la remisión del reporte final.
- 9.4 El reporte final de incidentes operacionales significativos debe presentarse según el formato IOS-C, adjuntando los análisis señalados en los párrafos 9.2 del presente artículo, según corresponda.

CAPÍTULO III

REMISIÓN DE REPORTES DE INCIDENTES OPERACIONALES SIGNIFICATIVOS

Artículo 10. Formatos de los reportes de incidentes operacionales significativos

La empresa debe remitir los reportes de incidentes operacionales significativos a la Superintendencia de acuerdo con los formatos IOS-A, IOS-B y IOS-C del Reporte de Incidentes Operacionales Significativos y sus respectivas notas metodológicas, según corresponda al estado del incidente, que se encuentran en el Anexo de la presente Resolución.

Artículo 11. Envío de reportes de incidentes operacionales significativos a la Superintendencia

Los reportes de incidentes operacionales significativos deben ser remitidos mediante el buzón electrónico incidentes@sbs.gob.pe o el medio que la Superintendencia comunique posteriormente.

DISPOSICIÓN COMPLEMENTARIA FINAL

ÚNICA.- Para efectos de su gestión, atención y reporte, los incidentes ocurridos o detectados por las empresas supervisadas hasta el 31 de diciembre de 2026 continuarán rigiéndose bajo la normativa vigente al momento de su ocurrencia. Por el contrario, todo incidente ocurrido a partir del 1 de enero de 2027 se sujetará obligatoria y exclusivamente a las disposiciones del nuevo procedimiento regulado en la presente norma

Artículo Segundo. Modificar el artículo 15 del Reglamento para la Gestión de la Continuidad del Negocio, aprobado por Resolución SBS N° 877-2020 y sus modificatorias, de acuerdo con lo siguiente:

1. Sustituir los párrafos 15.4 y 15.5 de acuerdo con el siguiente texto:

“Artículo 15. Información de eventos de interrupción significativa de operaciones

(...)

15.4 La empresa debe remitir un reporte inicial de incidentes operacionales significativos en los plazos establecidos en los párrafos 15.1, 15.2 y 15.3, según corresponda, de acuerdo con lo dispuesto en el Procedimiento para el Reporte de Incidentes Operacionales Significativos, aprobado mediante la presente Resolución.



15.5 La empresa debe remitir reportes intermedios y un reporte final de incidentes operacionales significativos a la Superintendencia por el evento de interrupción significativa de operaciones, en caso corresponda, según lo dispuesto en el Procedimiento para el Reporte de Incidentes Operacionales Significativos.”

Artículo Tercero. Modificar el Reglamento para la Gestión de la Seguridad de la Información y la Ciberseguridad, aprobado por Resolución SBS N° 504-2021 y sus modificatorias, de acuerdo con lo siguiente:

1. Sustituir el literal l) del artículo 2 de acuerdo con el siguiente texto:

“Artículo 2. Definiciones

(...)

l) Incidente: Evento que se ha determinado que tiene o podría tener un impacto adverso sobre la empresa y que requiere de acciones de respuesta y recuperación.
(...)”

2. Sustituir el párrafo 15.3 del artículo 15 de acuerdo con el siguiente texto:

“Artículo 15. Reporte de incidentes de ciberseguridad significativos

(...)

15.3 La empresa debe remitir a la Superintendencia reportes iniciales, intermedios y finales de incidentes operacionales significativos por la ocurrencia de incidentes de ciberseguridad significativos de acuerdo con lo dispuesto en el Procedimiento para el Reporte de Incidentes Operacionales Significativos, aprobado mediante Resolución SBS N° xxx-2026.”

Artículo Cuarto. Aprobar los formatos de los Reportes IOS-A, IOS-B e IOS-C del Procedimiento para el Reporte de Incidentes Operacionales Significativos, de acuerdo con los formatos contenidos en el Anexo de la presente Resolución, los cuales se publican en el Portal Institucional (www.sbs.gob.pe), conforme a lo dispuesto en el Decreto Supremo N° 009-2024-JUS y sus modificatorias..

El Reporte IOS-A comprende los datos generales, campos iniciales y campos de reclasificación para el reporte inicial con incidente en estado abierto; también para el reporte de reclasificación a no significativo (estado cerrado).

El Reporte IOS-B comprende los datos generales, campos iniciales y campos intermedios para el reporte inicial con incidente en estado resuelto o reportes intermedios con incidente en estado abierto o resuelto.

El Reporte IOS-C comprende los datos generales, campos iniciales, campos intermedios y campos finales para el reporte final con incidente en estado cerrado, tras la revisión formal posterior al incidente.

Artículo Quinto. La presente resolución entra en vigencia a partir del 1 de enero de 2027.



SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

PROYECTO NORMATIVO

Regístrese, comuníquese y publíquese.