Resolución SMV
Nº **[NUMERO_DOCUMENTO]**

Lima, [FECHA_DOCUMENTO]

VISTOS:

El Expediente Nº 2018039905 y el Informe Conjunto N° 1356-2018 del 23 de noviembre del 2018, emitido por la Oficina de Asesoría Jurídica, la Superintendencia Adjunta de Riesgos y la Superintendencia Adjunta de Investigación y Desarrollo; así como el Proyecto de Modificación del Reglamento de Gestión del Riesgo Operacional (en adelante, el PROYECTO);

CONSIDERANDO:

Que, conforme a lo dispuesto en el literal a) del artículo 1° del Texto Único Concordado de la Ley Orgánica de la Superintendencia del Mercado de Valores – SMV (en adelante, la Ley Orgánica de la SMV), aprobado mediante Decreto Ley Nº 26126 y sus modificatorias, la SMV está facultada para dictar las normas legales que regulen materias del mercado de valores;

Que, de acuerdo con el literal b) del artículo 5° de la precitada norma, el Directorio de la SMV tiene por atribución aprobar la normativa del mercado de valores, así como aquella a la que deben sujetarse las personas naturales y jurídicas sometidas a su supervisión;

Que, el artículo 16-B de la Ley del Mercado de Valores - LMV, aprobada por Decreto Legislativo N° 861, establece que las personas jurídicas autorizadas por la SMV deberán constituir un Sistema de Administración de Riesgos de acuerdo con las normas que establezca la SMV;

Que, el 20 de diciembre de 2015, se publicó en el Diario Oficial El Peruano el Reglamento de Gestión Integral de Riesgos, aprobado mediante Resolución SMV N° 037-2015-SMV/01, el cual establece criterios mínimos para que las Entidades a las que la SMV otorga autorización de funcionamiento desarrollen de manera adecuada su gestión integral de riesgos;

Que, el 18 de septiembre del 2016, se publicó en el Diario Oficial El Peruano el Reglamento de Gestión del Riesgo Operacional, aprobado mediante Resolución SMV N° 027-2016-SMV/01, con la finalidad de establecer disposiciones que regulen con mayor especificidad y de manera independiente diversos aspectos asociados al riesgo operacional, como parte de la gestión de los riesgos inherentes a los que se encuentran expuestas dichas Entidades;

Que, como parte del proceso de implementación de la supervisión basada en riesgos en la SMV, es preciso que se realicen ciertas modificaciones para proporcionar lineamientos para el registro de eventos de pérdida por riesgo operacional, fijar requerimientos para la identificación y evaluación del impacto de cambios significativos en la Entidad, así como proporcionar lineamientos para monitorear adecuadamente los servicios subcontratados e incorporar la obligación de reporte de

indicadores de riesgo operacional; con la finalidad de garantizar el correcto desarrollo de las operaciones por parte de las Entidades supervisadas por la SMV y contribuir a mejorar los procesos de supervisión *extra-situ* e *in-situ*.

Que, la evolución de la industria financiera, particularmente la incorporación de las tecnologías de la información en la forma de generar, procesar y administrar sus activos de información; involucran nuevos riesgos que afectan a los procesos intrínsecos del negocio de la institución así como también posibilitan cambios en el desarrollo de sus operaciones. Por lo que, resulta fundamental regular estándares mínimos de gestión de la ciberseguridad aplicables a las Entidades a las que la SMV otorga autorización de funcionamiento, y brindar pautas para el procesamiento de datos en la nube, con la finalidad de que sean desarrollados de manera adecuada.

Que, se ha considerado conveniente establecer un período razonable para la adecuación a la presente norma, por parte de las personas jurídicas obligadas a su cumplimiento, a cuyo fin, se diferencia el caso de las Entidades que pertenecen a conglomerados financieros, de las que no forman parte de ellos, estableciéndose que las primeras, entre otras razones por su mayor exposición al riesgo sistémico dentro del mercado de valores, son las que tendrían que estar adecuadas en enero de 2020, mientras que las demás, en diciembre del mismo año ;

Que, el PROYECTO fue difundido en consulta ciudadana en el Portal del Mercado de Valores de la SMV por el plazo de treinta (30) días hábiles, conforme lo dispuso la Resolución SMV N° XXX-2018-SMV/01, publicada el XXX de XXX de 2018 en el Diario Oficial El Peruano; y,

Estando a lo dispuesto por el literal a) del artículo 1° y el literal b) del artículo 5° de la Ley Orgánica de la SMV; el segundo párrafo del artículo 8° de la Ley del Mercado de Valores, Decreto Legislativo N° 861 y sus modificatorias; el numeral 2 del artículo 9 del Reglamento de Organización y Funciones de la SMV, aprobado por Decreto Supremo Nº 216-2011-EF; así como a lo acordado por el Directorio en su sesión del XX de XX de 2018;

SE RESUELVE:

Artículo 1°.- Modificar los artículos 2 y 3 del **TÍTULO I DISPOSICIONES GENERALES** del Reglamento de Gestión del Riesgo Operacional, aprobado mediante Resolución SMV N° 027-2016-SMV/01, de acuerdo con el siguiente texto:

"ARTÍCULO 2.- DEFINICIONES
Para la aplicación y/o implementación de lo establecido en el presente Reglamento se considerarán las siguientes definiciones:

- **a)** ***Activo:*** *Cualquier elemento que tenga valor para un individuo, una entidad o un gobierno.*
- **b)** ***Activo virtual:*** *Representación de un activo en el Ciberespacio.*
- **c)** ***Base de datos de eventos de pérdida (BDEP):*** *La base de datos de eventos de pérdida por riesgo operacional a que hace referencia el artículo 8° del presente Reglamento.*
- **d)** ***Cambio Significativo:*** *Todo aquel cambio en el ambiente operativo, informático o de negocios que tenga una influencia significativa en el perfil de riesgo de una Entidad.*
- **e)** ***CERT*** *(Computer Emergency Response Team): Centro de respuesta a incidentes*

de seguridad en tecnologías de la información.

f) ***CSIRT** (Computer Security Incident Response Team): Equipo responsable del desarrollo de medidas preventivas y de respuesta ante incidentes informáticos.*

g) ***Ciberamenaza o amenaza cibernética:** Aparición de una situación potencial o actual que pudiera convertirse en un ciberataque.*

h) ***Ciberataque o ataque cibernético:** Acción criminal organizada o premeditada de uno o más agentes que usan los servicios o aplicaciones del ciberespacio o son el objetivo de la misma o donde el ciberespacio es fuente o herramienta de comisión de un crimen.*

i) ***Ciberespacio:** Entorno complejo resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos conectados a dicha red, el cual no existe en ninguna forma física.*

j) ***Ciberseguridad:** Proceso de protección de la información mediante la prevención, detección y respuesta a los ataques.*

k) ***Confidencialidad:** La información debe mantenerse en reserva, pudiendo ser accesible únicamente a aquellos usuarios que se encuentren debidamente autorizados, capacitados y supervisados.*

l) ***Disponibilidad:** La información debe ser accesible a los usuarios autorizados cuando sea requerida.*

m) ***Evento de pérdida por Riesgo Operacional:** El evento que conduce a una o varias pérdidas, cuyo origen corresponde al riesgo operacional. En el presente Reglamento se utilizarán indistintamente los términos "evento de pérdida por riesgo operacional" y "evento de pérdida" con el mismo significado.*

n) ***Indicadores Clave de Riesgo:** Métrica que provee información acerca del nivel de exposición de la Entidad a un riesgo operacional específico en un momento dado.*

o) ***Interrupción del negocio:** Evento que genera la interrupción total o de parte importante de una o más líneas de negocio o sus procesos de soporte por treinta (30) minutos continuos o más.*

p) ***Incidente de seguridad de información:** Evento asociado a una posible falla en la política de seguridad, una falla en los controles, o una situación previamente desconocida relevante para la seguridad, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.*

q) ***Información**: Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.*

r) ***Integridad:** La información debe ser completa, exacta y veraz.*

s) ***Insourcing:** Modalidad de gestión mediante la cual una Entidad vuelve a desarrollar un proceso que anteriormente fue subcontratado.*

t) ***Nube Comunitaria:** Infraestructura de nube disponible para el uso exclusivo de una comunidad específica de entidades, incluido el caso de varias entidades de un mismo grupo.*

u) ***Nube Híbrida:** Infraestructura de nube compuesta por dos o más infraestructuras de nube distintas.*

v) ***Nube Privada:** Infraestructura de nube disponible para el uso exclusivo de una sola entidad.*

w) ***Nube Pública**: Infraestructura de nube disponible para el uso abierto del público en general.*

x) ***Pérdida:** Es un impacto negativo en los resultados o en el patrimonio de la Entidad.*

y) ***Periodo máximo tolerable de interrupción:** Es el periodo, determinado por la Entidad, luego del cual la viabilidad de la Entidad sería afectada seriamente, si un producto o servicio en particular no es reanudado.*

z) ***Proveedor principal:** Es aquel que, de interrumpir sus operaciones afectaría de manera importante la continuidad del negocio de la Entidad. Además de aquellos con los que se tiene una subcontratación significativa, deben considerarse a los proveedores de servicios públicos como: telecomunicaciones, energía, entre otros.*

*aa) **Reglamento:** El Reglamento de Gestión del Riesgo Operacional.*
*bb) **Reglamento de GIR:** El Reglamento de Gestión Integral de Riesgos, aprobado por Resolución SMV N° 037-2015-SMV/01.*
*cc) **Servicios en la nube:** Servicios prestados usando computación en la nube, es decir, un modelo que permite el acceso de red ubicuo, conveniente y bajo demanda, a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden suministrar y desplegar rápidamente, requiriendo un esfuerzo de gestión o una interacción con el proveedor del servicio mínimos.*
*dd) **SIEM (Security Information and Event Management):** Sistema de información que proporciona análisis en tiempo real de las alertas de seguridad generadas por las aplicaciones, dispositivos de seguridad y los elementos de red. Suelen ser sistemas de centralización de logs.*
*ee) **Subcontratación:** Modalidad de gestión mediante la cual una Entidad contrata a un tercero para que este desarrolle un proceso que podría ser realizado por la Entidad contratante.*
*ff) **Subcontratación en cadena:** Es aquella subcontratación donde el proveedor de la subcontratación subcontrata partes del servicio a otros proveedores.*
*gg) **Subcontratación significativa:** Es aquella subcontratación que, en caso de falla o suspensión del servicio, puede poner en riesgo a la Entidad, al afectar sus ingresos, solvencia o continuidad del negocio de manera importante.*
*hh) **Tiempo objetivo de recuperación:** Es el tiempo establecido por la Entidad para reanudar un proceso, en caso de ocurrencia de un evento de interrupción de operaciones. Es menor al periodo máximo tolerable de interrupción.*

Asimismo, serán de aplicación las definiciones contenidas en el Reglamento GIR.

En adelante, los términos antes mencionados podrán emplearse en forma singular o plural, sin que ello implique un cambio en su significado. Salvo mención en contrario la referencia a artículos determinados debe entenderse efectuada a los correspondientes del presente Reglamento.

ARTÍCULO 3.- FINALIDAD
El presente Reglamento establece lineamientos, criterios y parámetros generales mínimos que la Entidad debe observar en el diseño, desarrollo y aplicación de su gestión del riesgo operacional, de acuerdo con la naturaleza y proporcionalidad del negocio, la cual debe considerar el tamaño de la entidad, el volumen de transacciones y la complejidad de las operaciones que realizan.

Como parte de una adecuada gestión del riesgo operacional, las Entidades deben implementar un sistema de gestión de seguridad de la información y gestión de la continuidad del negocio".

Artículo 2°.- Modificar el **TÍTULO III GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** y los artículos 9, 10 y 11 del Reglamento de Gestión del Riesgo Operacional, aprobado mediante Resolución SMV N° 027-2016-SMV/01, de acuerdo con el siguiente texto:

"TÍTULO III
GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y DE CIBERSEGURIDAD

ARTÍCULO 9.- SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La Entidad debe implementar un sistema de gestión de seguridad de la información que permita garantizar la integridad, la confidencialidad y disponibilidad de la información, así como gestionar efectivamente los riesgos de ciberseguridad, mediante la adecuada combinación de políticas, procedimientos, controles, estructura organizacional y herramientas informáticas especializadas.

Para ello, deberá como mínimo realizar las siguientes actividades:

a) *Definición de una política de seguridad de la información y de ciberseguridad aprobada por el Directorio u órgano equivalente.*
b) *Definición e implementación de una metodología de gestión de seguridad de la información y de ciberseguridad, conforme a lo establecido en el artículo 7 del Reglamento, y que guarde consistencia con la gestión integral de riesgos de la Entidad.*
c) *Mantenimiento de registros adecuados que permitan verificar el cumplimiento de las normas, estándares, políticas, procedimientos y otros definidos por la Entidad, así como mantener una suficiente evidencia de auditoría.*

ARTÍCULO 10.- FUNCIÓN DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
La Entidad debe contar con una estructura organizacional que le permita implementar y mantener el sistema de gestión de la seguridad de información, para lo cual deberá:

a) Establecer, mantener y difundir las políticas y procedimientos de seguridad de información y de ciberseguridad.
b) Asignar y distribuir claramente los roles y responsabilidades.
c) Coordinar y monitorear la implementación de los controles de seguridad de información y de ciberseguridad.
d) Desarrollar actividades de concientización y entrenamiento en seguridad de información y ciberseguridad, para mantenerlos actualizados sobre las nuevas ciberamenazas, tanto al interior de la entidad como frente a usuarios y terceros que esta considere relevantes.
e) Evaluar de forma continua los eventos asociados a una posible falla en la política de seguridad, en los controles o una situación previamente desconocida relevante para la seguridad y recomendar acciones apropiadas.
f) Desarrollar planes de comunicación para determinar responsabilidades en la toma de decisiones, así como las políticas y procedimientos para divulgar potenciales vulnerabilidades;
g) Dirigir y promover que el personal contribuya con la efectividad del sistema de gestión de seguridad de la información; y,
h) Reportar al Directorio u órgano equivalente o al Comité de Riesgos, según su organización, sobre el desempeño del sistema de gestión de la seguridad de la información con la periodicidad que determine la Entidad, la que no podrá ser mayor a 6 meses.

ARTÍCULO 11.- CONTROLES DE SEGURIDAD DE LA INFORMACIÓN Y DE CIBERSEGURIDAD
Las entidades deberán implementar, de acuerdo con su tamaño, volumen de transacciones y complejidad de sus operaciones, los siguientes controles como parte de la gestión de la seguridad de la información y de ciberseguridad:

1. Control de acceso:
a) Procedimientos formales para la concesión, administración de derechos y perfiles, así como la revocación de usuarios.
b) Revisiones periódicas sobre los derechos concedidos a los usuarios.

c) *Los usuarios deben contar con una identificación para su uso personal, de tal manera que las posibles responsabilidades puedan ser seguidas e identificadas.*
d) *Controles especiales sobre utilidades del sistema y herramientas de auditoría.*
e) *Seguimiento sobre el acceso y uso de los sistemas para detectar actividades no autorizadas.*
f) *Controles especiales sobre usuarios remotos y computación móvil.*

2. *Seguridad de los recursos humanos:*

a) *Definición de roles y responsabilidades establecidos sobre la seguridad de información y la ciberseguridad.*
b) *Verificación de antecedentes (penales, judiciales, crediticios, etc.), de acuerdo a la clasificación de información a la que tendrá acceso.*
c) *Concientización y entrenamiento sobre los nuevos y emergentes riesgos.*
d) *Procesos disciplinarios en caso de incumplimiento de las políticas de seguridad de la información.*
e) *Procedimientos definidos en caso de cese del personal, que incluyan aspectos como la revocación de los derechos de acceso y la devolución de activos.*

3. *Seguridad física y ambiental:*

a) *Controles para evitar el acceso físico no autorizado, daños o interferencias a los locales y a la información de la Entidad.*
b) *Controles para prevenir pérdidas, daños o robos de los activos, incluyendo la protección de los equipos frente a amenazas físicas y ambientales.*

4. *Gestión de activos:*

a) *Realizar y mantener un inventario de activos y asignar responsabilidades respecto a la protección de estos activos. Deben considerarse en este inventario aquellos activos virtuales relativos a la presencia de la entidad en el ciberespacio.*
b) *Realizar una clasificación de los activos, en función del tipo de información que contienen o procesan y en el valor que poseen para el negocio, indicando el nivel de riesgo existente para la Entidad, así como las medidas apropiadas de control que deben asociarse a las clasificaciones.*

5. *Administración de las operaciones y comunicaciones:*

a) *Procedimientos documentados para la operación de los sistemas.*
b) *Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos.*
c) *Separación de funciones para reducir el riesgo de error o fraude.*
d) *Separación de los ambientes de desarrollo, pruebas y producción.*
e) *Controles para proteger los datos en tránsito y en reposo.*
f) *Implementar herramientas o servicios que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad, tal como un SIEM.*
g) *Monitoreo del servicio brindado por terceros.*
h) *Configurar los servidores, incluyendo los sistemas operativos subyacentes, de acuerdo a una guía de configuración de seguridad base.*
i) *Ejecutar controles anti software malicioso (como spyware o malware) en el servidor.*
j) *Administración de la capacidad de procesamiento.*
k) *Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares.*
l) *Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas.*

m) *Seguridad sobre el intercambio de la información, incluido el correo electrónico.*
n) *Seguridad sobre canales electrónicos.*
o) *Mantenimiento de registros de auditoría y monitoreo del uso de los sistemas.*
p) *De acuerdo con la estructura, canales de atención, volumen transaccional y número de clientes, monitorear diferentes fuentes de información tales como sitios web, blogs y redes sociales, con el propósito de identificar posibles ataques cibernéticos contra la Entidad.*

6. *Adquisición, desarrollo y mantenimiento de sistemas informáticos:*

Para la administración de la seguridad en la adquisición, desarrollo y mantenimiento de sistemas informáticos, se debe tomar en cuenta, entre otros, los siguientes criterios:

a) *Incluir en el análisis de requerimientos para nuevos sistemas o mejoras a los sistemas actuales, controles sobre el ingreso de información, el procesamiento y la información de salida.*
b) *Aplicar técnicas de encriptación sobre la información crítica que debe ser protegida.*
c) *Definir controles sobre la implementación de aplicaciones antes del ingreso a producción.*
d) *Controlar el acceso a las librerías de programas fuente.*
e) *Mantener un estricto y formal control de cambios, que será debidamente apoyado por sistemas informáticos en el caso de ambientes complejos o con alto número de cambios.*
f) *Asegurar el scripting de las interfaces web para evitar ataques de XSS.*
g) *Implementar el manejo de sesiones para las aplicaciones web con acceso a información sensible y/o relevante para el negocio.*
h) *Controlar el manejo de las entradas de datos para prevenir ataques de inyección SQL.*
i) *Realizar revisiones de código fuente para los servicios provistos en el ciberespacio.*
j) *Controlar las vulnerabilidades técnicas existentes en los sistemas de la Entidad.*

7. *Procedimientos de respaldo:*

a) *Procedimientos de respaldos regulares y validados con la periodicidad que determine la Entidad. Estos procedimientos deben incluir las medidas necesarias para asegurar que la información esencial pueda ser recuperada en caso de falla en los medios o luego de un desastre. Estas medidas serán coherentes con la estrategia de continuidad de negocios de la Entidad.*
b) *Conservar la información de respaldo y los procedimientos de restauración en una ubicación, que evite exponerlos ante posibles eventos que comprometan la operación del centro principal de procesamiento*.

8. *Gestión de incidentes de seguridad de información:*

Para asegurar que los incidentes y vulnerabilidades de seguridad sean controlados de manera oportuna, la Entidad deberá considerar los siguientes aspectos:

a) *Procedimientos formales para el reporte de incidentes de seguridad de la información y las vulnerabilidades asociadas con los sistemas de información.*

b) *Procedimientos establecidos para dar una respuesta adecuada a los*

incidentes y vulnerabilidades de seguridad reportadas.

c) *Establecer los procedimientos para reportar, cuando se considere pertinente, al CERT nacional o quien haga sus veces, directamente o a través de CSIRT sectoriales, de ser el caso, los ataques cibernéticos que requieran de su gestión.*

9. Cumplimiento normativo:
La Entidad deberá asegurar que los requerimientos legales, contractuales, o de regulación sean cumplidos, y cuando corresponda, incorporados en la lógica interna de las aplicaciones informáticas.

10. Privacidad de la información:
La Entidad debe adoptar medidas que aseguren razonablemente la privacidad de la información que reciben de sus clientes y usuarios de servicios, conforme a la regulación vigente sobre la materia".

Artículo 3°.- Modificar el artículo 16 e incorporarlo al **TÍTULO V OTRAS DISPOSICIONES** del Reglamento de Gestión de Riesgo Operacional aprobado mediante Resolución SMV N° 027-2016-SMV/01, de acuerdo con el siguiente texto:

"TITULO V
OTRAS DISPOSICIONES

ARTÍCULO 16.- CAMBIOS SIGNIFICATIVOS
Se consideran cambios significativos de manera enunciativa, más no limitativa, a los siguientes:

a) *Prestación de nuevos servicios y productos, modificaciones importantes y/o cese en la prestación de los mismos.*
b) *Cambios de la infraestructura tecnológica que soportan los principales productos y/o servicios.*
c) *Nuevos canales de atención y/o modificaciones importantes de los mismos.*
d) *Fusiones, adquisiciones y/o cualquier reorganización societaria.*
e) *Cambio de oficina principal.*
f) *Subcontrataciones significativas, insourcing de actividades significativas y/o modificaciones en los mismos, u otro cambio relevante en procesos.*

Esta lista podrá ser ampliada mediante Resolución del Superintendente del Mercado de Valores.

La Entidad deberá realizar una evaluación de todos los riesgos que se encuentren asociados a los cambios significativos, tomando mínimamente como referencia los tipos de riesgo indicados en el Reglamento de Gestión Integral de Riesgos.

De forma previa a la toma de decisiones sobre los cambios significativos, se deberá remitir un informe que contenga los resultados de dicha evaluación al Directorio, Comité de Riesgos u órgano especializado. El informe mínimamente deberá contener la información del cambio (descripción, objetivos, procesos asociados, etc.), los riesgos identificados (diferenciados por tipos de riesgo), así como las medidas de tratamiento implementadas o a implementar, debiendo estar este a disposición de la Superintendencia.

Artículo 4°.- Modificar los artículos 17 y 18 del **TÍTULO V OTRAS DISPOSICIONES** del Reglamento de Gestión del Riesgo Operacional, aprobado mediante Resolución SMV N° 027-2016-SMV/01, de acuerdo con el siguiente texto:

"ARTÍCULO 17.- SUBCONTRATACIÓN

Las entidades asumen plena responsabilidad de todos los servicios y actividades subcontratadas, así como de las decisiones de gestión que se deriven de ellas, pudiendo ser sancionadas por el incumplimiento de sus obligaciones en materia de regulación.

Por ello, las entidades deberán:

1. *Establecer políticas y procedimientos formales para determinar el nivel de riesgo que represente cada subcontratación.*
2. *Implementar mecanismos de control que deberían aplicarse desde el comienzo hasta la finalización de una subcontratación (selección del proveedor, diseño del contrato, monitoreo del servicio, planes de continuidad y estrategias de salida).*
3. *Mantener un registro actualizado de información sobre todas las subcontrataciones (significativas y no significativas).*

Las presentes disposiciones son aplicables también para las subcontrataciones intragrupo, es decir, la prestación de servicios por una entidad jurídica separada perteneciente al propio grupo económico.

Asimismo, toda subcontratación significativa deberá ser tratada como un cambio significativo.

En caso que las entidades deseen realizar una subcontratación significativa de su procesamiento de datos, de tal manera que éste sea realizado en el exterior, deberán actuar con especial prudencia, debido a los posibles riesgos relativos a la protección de datos, considerando lo siguiente:

- *La entidad que externaliza evaluará la localización de los datos y del procesamiento de datos con un enfoque basado en el riesgo. La evaluación tendrá en cuenta el impacto potencial de los riesgos, incluidos los riesgos legales y de cumplimiento, y las limitaciones a la vigilancia relacionados con los países en los que se van a llevar a cabo, o es probable que se lleven a cabo, los servicios subcontratados y en los que se van a almacenar, o es probable que se almacenen, los datos.*

- *La evaluación tomará en consideración la estabilidad política y en materia de seguridad de las jurisdicciones en cuestión, la legislación vigente en dichas jurisdicciones (incluidas las leyes de protección de datos), y los mecanismos para asegurar el cumplimiento de las leyes en dichas jurisdicciones, incluidas las disposiciones de la legislación de insolvencia que serían aplicables en caso de quiebra del proveedor de servicios. La entidad que subcontrata se asegurará de que esos riesgos permanezcan dentro de unos límites aceptables y proporcionales a la significatividad de la actividad externalizada.*

- *Asimismo, la Entidad deberá asegurarse de que el proveedor de los servicios objeto de subcontratación cuente con un examen anual de auditoría independiente, realizado por una sociedad auditora externa o una firma nacional o extranjera, que acredite contar con el conocimiento y experiencia requerida, que guarde conformidad con el estándar AT101 y que cumpla con lo señalado en la guía para la elaboración del reporte SOC 2, ambos emitidos por el Instituto Americano de Contadores Públicos Certificados (AICPA), debiendo la entidad supervisada poner a disposición de esta Superintendencia el reporte*

anual SOC 2 tipo 2.

Para el caso de subcontratación significativa en la nube, de forma adicional a las consideraciones mencionadas en los párrafos precedentes, de forma previa a la toma de decisiones sobre la externalización, se deberá realizar una diligencia reforzada del proveedor y del servicio, al menos considerando los siguientes aspectos:

1. ***Derechos de acceso y auditoría.*** *Las entidades que subcontratan deberán tener en cuenta los limitantes del ejercicio efectivo de los derechos de acceso y de auditoría. Sin embargo, la entidad podrá valerse de certificaciones externas e informes de auditoría internos o externos facilitados por el proveedor de servicios en la nube, siempre y cuando:*
    a. *La entidad que externaliza se asegure de que el alcance de la certificación o del informe de auditoría incluye los sistemas (es decir, los procesos, aplicaciones, infraestructuras, centros de datos, etc.) y los controles que ella considera clave asociados al servicio brindado.*
    b. *La entidad que externaliza evalúe en profundidad el contenido de las certificaciones o de los informes de auditoría de forma continua y, en particular, se asegure de que los controles clave sigan estando incluidos en versiones futuras de un informe de auditoría y verifique que la certificación o el informe de auditoría no estén obsoletos.*
    c. *Las certificaciones se emitan y las auditorías se lleven a cabo de acuerdo con los estándares generalmente aceptados e incluyan una prueba de la eficacia operativa de los controles clave establecidos.*

2. ***Seguridad de los datos y sistemas.*** *Las entidades deberán tener en cuenta los aspectos relacionados con la seguridad de datos y sistemas, llevando a cabo mínimamente las siguientes acciones:*
    a. *Identificar y clasificar las actividades, procesos y datos y sistemas relacionados en función de su sensibilidad y de las medidas de protección requeridas.*
    b. *Realizar una selección minuciosa, en función del riesgo, de las actividades, procesos y datos y sistemas relacionados que se esté considerando externalizar a un proveedor de soluciones de computación en nube.*
    c. *Definir y decidir el nivel apropiado de protección de la confidencialidad de la información, la continuidad de las actividades externalizadas, así como la integridad y trazabilidad de los datos y sistemas en el contexto de la externalización de servicios en la nube prevista.*
    d. *Considerar la adopción de medidas específicas cuando sean necesarias para proteger los datos en tránsito, los datos en memoria y los datos en reposo, como el uso de tecnologías de cifrado combinadas con una arquitectura de gestión de claves adecuada.*

3. ***Localización de los datos y del procesamiento de datos.*** *Considerar lo establecido en el quinto párrafo del presente artículo, solo en el caso de procesamiento de datos en el exterior.*

4. ***Subcontratación en cadena.*** *La entidad deberá tener en cuenta los riesgos asociados a la subcontratación "en cadena" cuando el proveedor del servicio subcontratado subcontrate partes del servicio a otros proveedores. La entidad aceptará la subcontratación en cadena solamente si el subcontratista cumple también plenamente con las obligaciones existentes entre la entidad (que subcontrata) y el proveedor del servicio (subcontratado).*

5. ***Planes de continuidad y estrategias de salida claramente definidas.*** *La entidad planteará e implantará medidas para mantener la continuidad de su negocio en caso de*

que la prestación de servicios por parte del proveedor falle o se deteriore hasta un grado inaceptable. Así mismo se asegurará de poder salir de los acuerdos de subcontratación de servicios en la nube, en caso necesario, sin que ello genere alteraciones excesivas en los servicios prestados, ni afecte negativamente su cumplimiento con el régimen regulatorio, ni comprometa la continuidad y la calidad de los servicios prestados a sus clientes.

ARTÍCULO 18.- REPORTES DE INDICADORES CLAVE DE RIESGO OPERACIONAL

Las Entidades deberán remitir reportes periódicos a la SMV sobre la gestión de Riesgo Operacional, Seguridad de la Información y de Ciberseguridad, y Continuidad del Negocio, con el objetivo de poder realizar un monitoreo permanente de las actividades y contar con un esquema organizado que permita tener información suficiente, pertinente y oportuna para la toma de decisiones.

La serie de indicadores de detallan en el Anexo III y se integran por los siguientes reportes:

Sistema de Gestión	*Reporte*	*Descripción*	*Frecuencia*
Riesgo Operacional	*RO_r1*	*Eventos de Pérdida por Riesgo Operacional.*	*Trimestral*
	RO_r2	*Cambios Significativos*	*Mensual*
Seguridad de la Información	*SI_r1*	*Vulnerabilidades identificadas.*	*Trimestral*
	SI_r2	*Inversión en Ciberseguridad.*	*Anual*
Continuidad del Negocio	*CN_r1*	*Eventos de Interrupción.*	*Trimestral*
	CN_r2	*Activación de Planes de Continuidad.*	*Trimestral*
	CN_r3	*Proveedores Principales.*	*Semestral*
	CN_r4	*Planes y Pruebas de Continuidad.*	*Semestral*

Todos los reportes de indicadores deberán ser remitidos a la SMV dentro de los treinta (30) días calendarios posteriores al cierre del periodo objeto de reporte.

Mediante Circular, la SMV comunicará el canal de reporte, así como los formatos junto con sus respectivas notas metodológicas.

Artículo 5°.- Incorporar el artículo 19 al **TÍTULO V OTRAS DISPOSICIONES** del Reglamento de Gestión del Riesgo Operacional, aprobado mediante Resolución SMV N° 027-2016-SMV/01, de acuerdo con el siguiente texto:

"ARTÍCULO 21.- CONSERVACION DE INFORMACION
Las Entidades deberán conservar la información de que trata el presente Reglamento por un plazo no menor de diez (10) años".

Artículo 6°.- Modificar el contenido del ANEXO TIPOS DE EVENTOS DE PÉRDIDA POR RIESGO OPERACIONAL del Reglamento de Gestión del Riesgo Operacional, aprobado mediante Resolución SMV N° 027-2016-SMV/01, de acuerdo con el siguiente texto:

"ANEXO I
TIPOS DE EVENTOS DE PÉRDIDA POR RIESGO OPERACIONAL

Tipo de evento (Nivel 1)	***Definición***	***Tipo de evento (Nivel 2)***	***Ejemplos***
Fraude interno	*Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas internas en las que se encuentran implicados empleados de la Entidad, y que tiene como fin obtener un beneficio ilícito.*	*Actividades no autorizadas*	*Operaciones no reveladas (intencionalmente), operaciones no autorizadas (con pérdidas pecuniarias), valoración errónea de posiciones (intencional).*
		Robo y fraude	*Robo, malversación, falsificación, soborno, apropiación de cuentas, contrabando, evasión de impuestos (intencional).*
Fraude externo	*Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de un activo indebidamente o incumplir la legislación, por parte de un tercero, con el fin de obtener un beneficio ilícito.*	*Robo y fraude*	*Robo, falsificación.*
		Seguridad de los sistemas	*Daños por ataques informáticos, robo de información.*
Relaciones laborales y seguridad en el puesto de trabajo	*Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre salud o seguridad en el trabajo, el pago de reclamos por daños personales, o casos relacionados con la diversidad o discriminación.*	*Relaciones laborales*	*Cuestiones relativas a remuneración, prestaciones sociales, extinción de contratos.*
		Salud y seguridad en el trabajo	*Casos relacionados con las normas de salud y seguridad en el trabajo; indemnización a los trabajadores.*
		Diversidad y discriminación	*Todo tipo de discriminación.*
Prácticas relacionadas con los clientes, los productos, servicios y el Negocio	*Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación frente a clientes o generadas por la deficiencia en el producto o servicio.*	*Adecuación, divulgación de información y confianza*	*Abusos de confianza / incumplimiento de pautas, aspectos de adecuación / divulgación de información (conocimiento del cliente, etc.), quebrantamiento de la privacidad de información*

			sobre clientes, quebrantamiento de privacidad, ventas agresivas, abuso de información confidencial la privacidad de información sobre clientes, quebrantamiento de privacidad, ventas agresivas, abuso de información confidencial.
		Prácticas empresariales o de mercado improcedentes	*Prácticas restrictivas de la competencia, prácticas comerciales / de mercado improcedentes, manipulación del mercado, uso de información privilegiada, lavado de activos y financiamiento del terrorismo.*
		Productos defectuosos	*Defectos del producto (no autorizado, etc.), error de los modelos.*
		Selección, patrocinio y riesgos	*Ausencia de investigación a clientes conforme a las directrices, exceso de los límites de riesgo frente a clientes.*
		Actividades de asesoramiento	*Litigios sobre resultados de las actividades de asesoramiento.*
Daños a activos físicos	*Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.*	*Desastres y otros acontecimientos*	*Pérdidas por desastres naturales, pérdidas humanas por causas externas (terrorismo, vandalismo).*
Interrupción del negocio por fallas en la tecnología de información	*Pérdidas derivadas de interrupciones en el negocio y de fallas en los sistemas.*	*Sistemas*	*Pérdidas por fallas en equipos de hardware, software o telecomunicaciones; falla en energía eléctrica.*

Deficiencia en la ejecución, entrega y gestión de procesos	*Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes, tales como proveedores, clientes, entre otros.*	*Recepción, ejecución y mantenimiento de operaciones*	*Errores de introducción de datos, mantenimiento o descarga, incumplimiento de plazos o de responsabilidades, ejecución errónea de modelos / sistemas, errores contables. Errores en el proceso de compensación de valores y liquidación de efectivo (p.ej. en el Delivery vs. Payment).*
		Seguimiento y presentación de informes	*Incumplimiento de la obligación de informar, inexactitud de informes externos (con generación de pérdidas).*
		Aceptación de clientes y documentación	*Inexistencia de autorizaciones /rechazos de clientes, documentos jurídicos inexistentes / incompletos.*
		Gestión de cuentas de clientes	*Acceso no autorizado a cuentas, registros incorrectos de clientes (con generación de pérdidas), pérdida o daño de activos de clientes por negligencia.*
		Contrapartes comerciales	*Fallos de contrapartes distintas de clientes, otros litigios con contrapartes distintas de clientes.*
		Distribuidores y proveedores	*Subcontratación, litigios con proveedores.*

Artículo 7°.- Incorporar los siguientes anexos: **ANEXO II LINEAMIENTOS PARA EL REGISTRO DE EVENTOS DE PÉRDIDA POR RIESGO OPERACIONAL y ANEXO III INDICADORES CLAVE DE RIESGO** al Reglamento de Gestión del Riesgo Operacional, aprobado mediante Resolución SMV N° 027-2016-SMV/01, de acuerdo con el siguiente texto:

"ANEXO II

LINEAMIENTOS PARA EL REGISTRO DE EVENTOS DE PÉRDIDA POR RIESGO OPERACIONAL

1. ***Valoración de los eventos de pérdida***

El monto bruto de pérdida asociada a un evento, que será registrado en la BDEP, deberá incluir los siguientes aspectos, según sean aplicables:

a. *Impacto directo en los estados financieros, incluyendo gastos, disminución del valor de los activos, entre otros.*

b. *Gastos de reparación o reemplazo para restablecer la situación existente antes de la ocurrencia del evento, incluyendo el pago de deducibles asociados a los seguros contratados.*

c. *Provisiones reconocidas en los estados financieros asociadas con eventos de pérdida por riesgo operacional.*

Los siguientes aspectos no deben ser considerados en la determinación del monto bruto de pérdida:

a. *Recuperaciones posteriores a la ocurrencia del evento de pérdida.*

b. *Gastos provenientes de contratos generales de mantenimiento de equipos o locales.*

c. *Gastos asociados con mejoras realizadas luego del evento de pérdida.*

d. *Primas de seguros.*

Los eventos de pérdida asociados a daños en activos fijos que los inhabilitan deberán registrarse en la BDEP siguiendo las siguientes disposiciones:

a. *Si se reemplaza el activo dañado, debe registrarse como pérdida el costo de adquisición del nuevo activo.*

b. *Si no se reemplaza el activo dañado, debe registrarse como pérdida el precio estimado de mercado de dicho activo o, en caso éste no se conozca, debe registrarse el costo histórico de adquisición. Por otro lado, de reemplazarse el activo de manera posterior, se deberá modificar el monto de pérdida registrado en la BDEP por el costo de adquisición del nuevo activo.*

En los casos en que un evento produce simultáneamente pérdidas y ganancias para la Entidad, con un saldo neto negativo, dicho saldo debe ser considerado para el cálculo del monto de pérdida y su registro en la BDEP.

Los eventos de pérdida asociados a reclamos presentados por los usuarios deben ser incorporados en la BDEP, incluyendo aquellos casos de operaciones no reconocidas por los usuarios por tratarse de operaciones presumiblemente fraudulentas, y aquellos en que la Entidad decida asumir la pérdida sin realizar una investigación completa.

2. Recuperaciones

Toda recuperación asociada al evento debe ser registrada en la BDEP de manera separada al monto bruto de pérdida. Se considerará una recuperación siempre que esta se produzca de manera independiente y posterior a la ocurrencia del evento de pérdida original.

A continuación, se incluye una relación no limitativa de recuperaciones:

a. *Pagos recibidos de una compañía de seguros luego de la ejecución de pólizas contratadas.*

b. *Pagos recibidos como resultado favorable de un proceso judicial o arbitral.*

c. *Pagos entregados por un tercero que preste servicios a la Entidad, con el objetivo de mitigar el impacto negativo de la ocurrencia de un evento de pérdida de su responsabilidad que afectó a ambas partes.*

d. *Pagos recibidos de clientes o empleados como resultado del proceso de recuperación.*

3. Provisiones

Las provisiones a que se refiere el literal c del numeral 1, deben ser registradas en la BDEP, incluyendo entre otras, las relacionadas a controversias judiciales, procesos arbitrales y procedimientos administrativos.

El monto asignado en la BDEP a esta provisión deberá ser actualizado tantas veces como la provisión sea modificada. En el momento que se conozca con certeza el monto de pérdida definitivo asociado al evento, se deberá reemplazar el monto de la provisión registrada por el importe definitivo. La Entidad debe establecer procedimientos específicos para la adecuada ejecución de las tareas mencionadas.

Las provisiones registradas en la BDEP deberán estar claramente identificadas, de forma que puedan distinguirse de otros impactos asociados al evento, para lo cual las Entidades deberán desarrollar e implementar procedimientos internos apropiados.

4. Evento con pérdidas múltiples

En el caso de un evento con pérdidas múltiples, las Entidades podrán registrar la información mínima requerida por cada pérdida, y deben establecer una forma de agrupar dicha información por el evento que las originó, es decir, aquel evento inicial sin el cual ninguna de las pérdidas relacionadas hubiera ocurrido.

A continuación, se incluye una relación no limitativa de pérdidas múltiples:

a. *Errores repetidos originados por una falla en un proceso de negocio o en un servicio.*
b. *Reembolsos a varios clientes provenientes de un reclamo común u originados por un solo evento (por ejemplo, la pérdida de documentos durante una mudanza o por un incendio).*
c. *Pérdidas por fraude realizadas a través de una misma acción y por la misma persona o grupo criminal.*
d. *Una interrupción de los servicios de tecnología que afecte a múltiples líneas de negocio.*
e. *Un individuo o grupo de funcionarios que recibe instrucciones erradas que genera pérdidas múltiples.*

Los errores múltiples originados por una misma persona a través de un determinado periodo de tiempo deben ser tratados como eventos independientes, por lo cual no deben ser agrupados en la BDEP. Por ejemplo, las pérdidas en mesa de negociación por errores operativos de un representante en tiempos diferentes.

La Entidad debe establecer procedimientos que garanticen el registro en la BDEP de aquellos eventos con pérdidas múltiples que en su conjunto superen el monto mínimo de registro de pérdidas establecido por la Entidad, pese a que el monto bruto de cada pérdida individual originada por el mismo evento, sea inferior al monto mínimo de registro.

5. Casos particulares

Los eventos que conducen a costos de oportunidad o ganancias no realizadas pueden ser registrados en la BDEP siempre que sean objetivamente medibles y contrastables con operaciones de similar naturaleza en condiciones normales de negocio, por ejemplo comisiones no cobradas en los rescates de cuotas de un fondo por errores asociados a un riesgo operacional.

Existen diversos eventos cuyo registro en la BDEP no es obligatorio. A continuación se provee una lista no limitativa de este tipo de eventos:

a. Aquellos que no condujeron a pérdidas, pero que bajo otras circunstancias podrían haber sido pérdidas reales, conocidos como "pérdidas cercanas". Por ejemplo, cuando se transfiere dinero a una cuenta errónea pero luego de su identificación se produce su extorno en el mismo día de la transferencia, evitando el impacto negativo para la Entidad.

b. Eventos que condujeron a ganancias, excepto que haya existido en simultáneo un evento que genera pérdidas y ganancias, con un resultado neto negativo, el cual deberá registrarse en la BDEP según lo señalado en el párrafo 4 del numeral 1 del presente anexo.

c. Eventos que representan solo pérdidas contables temporales debido a fallas en el registro en la información financiera de la Entidad, y que una vez corregidas no significan pérdidas financieras reales, salvo que producto de dichas fallas se produzcan sanciones administrativas u otras relacionadas, las cuales deben ser registradas en la BDEP.

d. Gastos de naturaleza interna o costos de transferencia, que se hubieren generado independientemente de la ocurrencia del evento, aunque si se incluyen los gastos asociados a sobretiempo al compararlos con los horarios habituales, siempre que estos representen pérdidas efectivas asociadas a eventos de pérdida por riesgo operacional.

Las Entidades evaluarán las posibles ventajas asociadas de contar con la información indicada en los literales precedentes. Si la Entidad decide registrarla, los eventos se encontrarán claramente identificados en la base de datos, de forma que pueda distinguirse con precisión dichos eventos de aquellos requeridos por la normativa, para lo cual deberán desarrollar e implementar procedimientos internos apropiados".

ANEXO III
INDICADORES CLAVE DE RIESGO

RO_r1: Reporte de Eventos de Pérdida por Riesgo Operacional

Año de reporte	Trimestre	Tipo de evento (Nivel 1)	Tipo de evento (Nivel 2)	Número de eventos por trimestre	Maxima pérdida por trimestre	Monto total bruto (a)	Monto total recuperado (b)	Monto total neto (a)-(b)	% del Total (a-b)/(c)
2019	3	Fraude interno	Actividades no autorizadas					S/. -	%
			Robo y fraude						
		Fraude externo	Robo y fraude					S/. -	%
			Seguridad de los sistemas						
		Relaciones laborales y seguridad en el puesto de trabajo	Relaciones laborales					S/. -	%
			Salud y seguridad en el trabajo						
			Diversidad y discriminación						
		Prácticas relacionadas con los clientes, los productos y el negocio	Adecuación, divulgación de información y confianza					S/. -	%
			Prácticas empresariales o de mercado improcedentes						
			Productos defectuosos						
			Selección, patrocinio y riesgos						
			Actividades de asesoramiento						
		Daños a activos fisicos	Desastres y otros acontecimientos					S/. -	%
		Interrupción del negocio por fallas en la tecnología de información	Sistemas					S/. -	%
		Deficiencia en la ejecución, entrega y gestión de procesos	Recepción, ejecución y mantenimiento de operaciones					S/. -	%
			Seguimiento y presentación de informes						
			Aceptación de clientes y documentación						
			Gestión de cuentas de clientes						
			Contrapartes comerciales						
			Distribuidores y proveedores						
			Total trimestre	0	S/. -	S/. -	S/. -	(c)	0%

Notas metodológicas:

1) Para fines de este reporte, considerar la definición para cada tipo de evento de acuerdo a lo establecido en los Anexos I y II del RSMV 027-2016.

2) En la columna "Año de reporte" consignar el año con cuatro dígitos. Asimismo, en la columna "Trimestre" consignar 1, 2, 3 o 4 según corresponda.

3) Se ingresará información relacionada con los eventos de pérdida registrados en la base de datos. Según el tipo de evento (nivel 1 y 2), se deberá llenar el número de eventos registrados, el monto de la máxima pérdida registrada (el mayor evento registrado), el monto total bruto de la pérdida (referido al total de número de eventos), el monto total recuperado con coberturas existentes, el monto total neto de la pérdida, y finalmente el ratio del monto neto sobre el total de la pérdida neta acumulada.

RO_r2: Reporte de Cambios significativos

Año de reporte	Trimestre	Cambio significativo (a)	Descripción del cambio (b)	Línea de Negocio	Producto relacionado	Proceso de soporte relacionado	Número de informe de riesgos	Total de cambios en el trimestre (c)	% del Total (c)/(d)
2019	3								%
	4								%
							Total anual de Cambios significativos (d)	0	0%

Notas metodológicas:
1) En la columna "Año de reporte" consignar el año con cuatro dígitos. Asimismo, en la columna "Trimestre" consignar 1, 2, 3 o 4 según corresponda.
2) El reporte debe elaborarse tomando en consideración lo siguiente:
(a): Tomar como referencia la lista de cambios significativos que se indican en el Artículo 19 del RSMV 027-2016.
(b): Indicar una breve descripción del cambio significativo.
3) Para todos los casos, se deberá escoger la línea de negocio donde se realizó el cambio significativo, así como el producto y/o proceso de soporte que afectó el cambio significativo.

SI_r1: Reporte de Vulnerabilidades

			Vulnerabilidades	
Año de reporte	Trimestre de reporte	Mes	Número de vulnerabilidades altas y críticas identificadas (a)	Número de vulnerabilidades altas y críticas corregidas (b)
2019	3	1		
		2		
		3		
		Total trimestre	0	0

Notas metodológicas:

1) El reporte debe elaborarse tomando en consideración lo siguiente:
(a): Indicar el número total de vulnerabilidades altas y críticas identificadas durante el periodo (mes) de medición
(b): Indicar el número total de vulnerabilidades altas y críticas corregidas durante el periodo (mes) de medición
2) En la columna "Año de reporte" consignar el año con cuatro dígitos. Asimismo, en la columna "Trimestre" y "Mes" consignar 1, 2, 3 o 4 según corresponda.
3) Se deberá entender por **vulnerabilidad** a cualquier deficiencia y/o debilidad de un sistema operativo, aplicación o equipo tecnológico, la cual puede ser explotada por usuarios no autorizados con fines no genuinos (usualmente para ocasionar daño). Se considerará a una vulnerabilidad como alta o crítica cuando tenga una puntuación CVSS (Common Vulnerability Scoring System) mayor o igual a 7.

SI_r2: Reporte de Inversión en Ciberseguridad

	Total			
(Cifras en Miles de soles)	2018	2019	2020	2021
Inversión en TI (a)				
a/c	%	%	%	%
a/d	%	%	%	%
Inversión en Ciberseguridad (b)				
b/c	%	%	%	%
b/d	%	%	%	%
Seguridad perimetral				
Seguridad de redes				
Protec. de dispo. de acceso a la red				
Seguridad de aplicativos				
Desarrollo de Sistemas				
Capacitación Interna				
Consultorías				
Otros				
Total Inversión (a+b)				
(a+b)/c	%	%	%	%
(a+b)/d	%	%	%	%
Utilidad Bruta (c)				
Gastos Operativos (d)				

Notas metodológicas:

1) El reporte debe elaborarse tomando en consideración lo siguiente:
(a): Indicar el monto de inversión en TI del periodo señalado.
(b): Indicar el monto de inversión en Ciberseguridad (considerando la sumatoria de los campos detallados para cada dominio) del periodo señalado.
(c): Indicar la Utilidad Bruta (individual) del periodo señalado.
(d): Indicar los Gastos Operativos (individual) del periodo señalado.

.

CN_r1: Reporte de Eventos de Interrupción

				Interrupciones del negocio		Interrupciones debido a fallas en los sistemas informáticos				Interrupciones por fallas en proveedores principales			
	Año de reporte	Trimestre de reporte	Mes	Numero de interrupciones (a)	Tiempo (min) total de interrupción (b)	Numero de interrupciones (c)	Tiempo (min) total de interrupción (d)	Proporción de interrupciones por fallas en los sistemas (c)/(a)	Proporción del tiempo de interrupción por fallas en los sistemas (d)/(b)	Numero de interrupciones (e)	Tiempo (min) total de interrupción (f)	Proporción de interrupciones por fallas en proveedores principales (e)/(a)	Proporción de tiempo de interrupción por fallas en proveedores principales (f)/(b)
Total de la empresa			1										
			2										
			3										

Notas metodológicas:

1) El reporte debe elaborarse tomando en consideración lo siguiente:
- **(a):** Indicar el número total de interrupciones ocurridas durante el periodo (mes) de medición, en la correspondiente línea de negocio
- **(b):** Indicar el tiempo total de interrupción durante el periodo (mes) de medición, en la correspondiente línea de negocio
- **(c):** Indicar el número de interrupciones debido a fallas en los sistemas durante el periodo (mes) de medición, en la correspondiente línea de negocio
- **(d):** Indicar el tiempo de interrupción debido a fallas en los sistemas durante el periodo (mes) de medición, en la correspondiente línea de negocio
- **(e):** Indicar el número total de interrupciones debido a fallas en los proveedores durante el periodo (mes) de medición, en la correspondiente línea de negocio
- **(f):** Indicar el tiempo de interrupción debido a fallas en los proveedores durante el periodo (mes) de medición, en la correspondiente línea de negocio

2) En aquellos casos en los que una interrupción no llega a ser mayor a treinta (30) minutos debido a la activación de planes de continuidad del negocio, dicha interrupción no deberá ser considerada para fines de este reporte.

3) Si un evento afecta a más de una línea de negocio, dicho evento deberá ser reportado en cada una de las líneas de negocio afectadas.

4) Dado que existen eventos de interrupción que pueden afectar a más de una línea de negocio, conforme se señala en el numeral anterior, el reporte de la línea "Total de la empresa" no siempre será la suma del número de interrupciones y tiempos registrados en cada una de las líneas de negocio.

5) Los eventos de interrupción que afecten de forma significativa la continuidad operativa de cualquier canal de atención, como agencias, cajeros automáticos, cajeros corresponsales u otros, deberán ser reportados en la(s) línea(s) de negocio que se vea(n) afectada(s) por dicho evento. Cabe señalar que se deberá considerar como interrupción significativa de un canal de atención la indisponibilidad del 50% o más puntos de atención de dicho canal a nivel nacional o en una determinada región.

6) En la columna "Año de Reporte" consignar el año con cuatro dígitos. Asimismo, en la columna "Trimestre de Reporte" consignar 1, 2,3 o 4, según corresponda.

CN_r2: Reporte de activación de planes de continuidad

			Numero de veces que se activó algun plan de continuidad del negocio				Porcentaje de TORs que no se cumplieron	
Año de reporte	Trimestre del reporte	Mes	Plan de gestion de crisis (a)	Plan de emergencia (b)	Plan(es) de continuidad del negocio (c)	Plan de recuperación de servicios de TI	Al activar el (los) plan(es) de continuidad del negocio (e)	Al activar el plan de recuperación de servicios de TI (f)
		1						
		2						
		3						

Notas metodológicas:

1) TOR: Tiempo objetivo de recuperación

2) TI: Tecnología de información

3) El reporte debe elaborarse tomando en consideración lo siguiente:
- **(a):** Indicar el número de veces que el Plan de Gestión de Crisis fue activado durante el periodo (mes) de medición.
- **(b):** Indicar el número de veces que alguno(s) de los planes de emergencia de la empresa fue(ron) activado(s) durante el periodo (mes) de medición.
- **(c):** Indicar el número de veces que alguno(s) de los planes de continuidad del negocio de la empresa fue(ron) activado(s) durante el periodo (mes) de medición.
- **(d):** Indicar el número de veces que el Plan de recuperación de servicios de TI fue activado durante el periodo (mes) de medición.
- **(e):** (N° TORs sin alcanzar / N° total TORs que debieron alcanzarse al activar los planes de continuidad del negocio activados durante el periodo de medición)*100%.
- **(f):** (N° TORs sin alcanzar / N° total TORs que debieron alcanzarse al activar el plan de recuperación de servicios de TI durante el periodo de medición)*100%.

4) En la columna "Año de reporte" consignar el año con cuatro dígitos. Asimismo, en la columna "Trimestre de reporte" consignar 1, 2, 3 o 4, según corresponda.

CN_r3: Reporte de Proveedores Principales

Año de reporte	Semestre de reporte	N° total de proveedores principales (a)	N° de proveedores principales con PCN o para los cuales la empresa cuenta con un proveedor alternativo (b)	Ratio (b)/(a)

Notas metodológicas:

1) PCN: Plan de continuidad de negocios

2) Para fines de este reporte, considerar la definición de proveedor principal que se describe en el numeral 2 del RSMV 027-2016.

3) El reporte debe elaborarse tomando en consideración lo siguiente:
- **(a):** Indicar el número total de proveedores principales.
- **(b):** Indicar el número de proveedores principales que cuenten con un plan de continuidad del negocio y/o con un proveedor alternativo. Si el proveedor principal cuenta con plan de continuidad del negocio y, además, se tiene un proveedor

4) En la columna "Año de reporte" consignar el año con cuatro dígitos. Asimismo, en la columna "Semestre de reporte" consignar 1 o 2, según corresponda.

CN_r4: Reporte de Planes y Pruebas de Continuidad del Negocio

		Plan de gestión de crisis		Plan de emergencia		Plan(es) de continuidad del negocio		Plan de recuperación de los servicios de TI	
Año de reporte	Semestre de reporte	Número de planes (a)	Número de planes probados (b)	Número de planes (c)	Número de planes probados (d)	Número de planes (e)	Número de planes probados (f)	Número de planes (g)	Número de planes probados (h)

1) TI: Tecnología de información

2) El reporte debe elaborarse tomando en consideración lo siguiente:

(a), (c), (e) y (g): Indicar el número de planes de gestión de crisis (a), de emergencia (c), de continuidad del negocio (e) y de recuperación de los servicios de TI (g), respectivamente.

(b), (d), (f) y (h): Indicar el número de planes de gestión de crisis (b), de emergencia (d), de continuidad del negocio (f) y de recuperación de los servicios de TI (h) que hubieran sido probados en el semestre de reporte.

3) En la columna "Año de reporte" consignar el año con cuatro dígitos. Asimismo, en la columna "Semestre de reporte" se deberá consignar 1o 2, según corresponda

		Planes de continuidad de negocios		Plan de recuperación de los servicios de TI	
Año de reporte	Semestre de reporte	Número total de pruebas realizadas (a)	Porcentaje de TORs que no se cumplieron (b)	Número total de pruebas realizadas (c)	Porcentaje de TORs que no se cumplieron (d)

1) TI: Tecnología de información

2) El reporte debe elaborarse tomando en consideración lo siguiente:

(a): Indicar el número total de pruebas realizadas a los planes de continuidad del negocio.

(b): (N° TORs sin alcanzar / N° total TORs que debieron alcanzarse al probar los planes de continuidad del negocio)*100%

(c): Indicar el número total de pruebas realizadas su plan de recuperación de los servicios de TI

(d): (N° TORs sin alcanzar / N° total TORs que debieron alcanzarse al probar el plan de recuperación de servicios de TI)*100%

3) Para efectos de este reporte se entenderá el término "prueba de continuidad" como todo tipo de ejercicio, test, simulación, entre otros, que se realice con el fin de verificar el funcionamiento de los planes de continuidad del negocio.

4) Si se realizara alguna prueba en la que no se verificara el cumplimiento del TOR, dicha prueba no deberá ser considerada para efectos del reporte.

5) En la columna "Año de reporte" consignar el año con cuatro dígitos. Asimismo, en la columna "Semestre de reporte" se deberá consignar 1o 2, según corresponda.

Artículo 8°.- Incorporar la **TERCERA DISPOSICIÓN COMPLEMENTARIA TRANSITORIA** al Reglamento de Gestión del Riesgo Operacional, aprobado mediante Resolución SMV N° 027-2016-SMV/01, de acuerdo con el siguiente texto:

"TERCERA.- *Respecto de los reportes de indicadores establecidos en el artículo 18 del Reglamento, el primer envío corresponderá:*

1. *Para las entidades que formen parte de un conglomerado financiero, al segundo trimestre del año 2020 (en el caso de los reportes RO_r1, RO_r2, SI_r1, CN_r1 y CN_r2), al primer semestre del 2020 (en el caso de los reportes CN_r3y CN_r4) y al ejercicio del 2020 (en el caso del reporte SI_r2)*

2. *Para las entidades que no formen parte de un conglomerado financiero, al primer trimestre del año 2021 (en el caso de los reportes RO_r1, RO_r2, SI_r1, CN_r1 y CN_r2), al primer semestre del 2021 (en el caso de los reportes CN_r3y CN_r4) y al ejercicio del 2021 (en el caso del reporte SI_r2)".*

Artículo 9°.- Las presentes disposiciones no son de aplicación a las Empresas Clasificadoras de Riesgos y a las Empresas Proveedoras de Precios. Las obligaciones sobre gestión de riesgo operacional aplicables a las Empresas Clasificadoras de Riesgo y a las Empresas Proveedoras de Precios se establecerán en sus respectivos reglamentos.

Artículo 10°.- Las modificaciones incorporadas por la presente resolución deberán ser implementadas de acuerdo a los siguientes plazos:

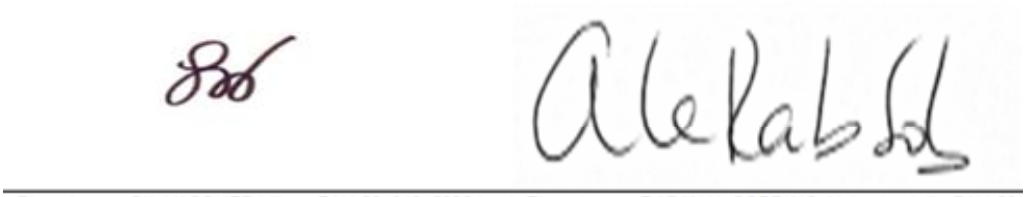
1. Para entidades que formen parte de un conglomerado financiero: a más tardar el 31 de enero de 2020.

2. Para entidades que no formen parte de un conglomerado financiero: a más tardar el 31 de diciembre de 2020.

Artículo 11°.- Publicar la presente resolución en el Diario Oficial El Peruano y en el Portal del Mercado de Valores de la Superintendencia del Mercado de Valores (www.smv.gob.pe).

Regístrese, comuníquese y publíquese.

Regístrese, comuníquese y publíquese.
José Manuel Jesús Peschiera Rebagliati
Superintendente del Mercado de Valores



Firmado por: GIL VASQUEZ Liliana FAU 20131016396 hard
Razón:

Firmado por: RABANAL SOBRINO Alejandro Julio FAU 201
Razón:

Firmado por: RIVERO ZEVALLOS Carlos Fabian FAU 201
Razón: