

Con el fin de asegurar el adecuado funcionamiento del Sistema de Gestión del Riesgo Operacional, se han definido los siguientes lineamientos:

- 1** Todo el personal de la empresa tiene la responsabilidad de gestionar el riesgo operacional dentro de los límites, normas y procedimientos establecidos por la Institución e informar a Unidad de Riesgo Operacional.
- 2** El Directorio, La Gerencia de Administración, Finanzas y Outsourcing de remuneraciones y la GRC aprueban las políticas, normas y procedimientos para la gestión de riesgo operacional de la compañía.
- 3** La responsabilidad inicial de la gestión del riesgo operacional recae en toda la organización de la empresa, bajo un criterio de autocontrol, dado que no es responsabilidad únicamente de la GRC.
- 4** De la identificación, análisis y evaluación del riesgo.
 - Para la identificación y evaluación de los riesgos operacionales, se aplicará la metodología descrita en el presente documento.
 - Las políticas generales que rigen la gestión del riesgo operacional y en particular las referidas al apetito y tolerancia al riesgo serán aprobadas por la Gerencia de Administración, Finanzas y Outsourcing de Remuneraciones.
 - Se debe ejecutar evaluaciones periódicas a los procesos con el fin de identificar, analizar y evaluar el riesgo operacional inherente a todas las actividades, procesos, sistemas y servicios relevantes.
 - Las evaluaciones de riesgo operacional de los procesos críticos del Grupo TAWA, se realizan de manera anual a través de talleres de autoevaluación de riesgos operacionales, donde se desarrollan las diversas etapas desde el establecimiento del contexto hasta la definición de planes de acción para el respectivo tratamiento de los riesgos basados en el apetito y tolerancia definidos por la empresa.
 - Posterior al proceso de autoevaluación donde se efectúa la identificación y evaluación del riesgo operacional las matrices de Riesgo Operacional deberán ser validados por la Unidad de Riesgo Operacional y de forma complementaria la GRC validará y aprobará aquellos riesgos que han sido calificados con niveles de exposición Altos y Extremos.
- 5** Del tratamiento y Control del Riesgo.
 - Se deberá establecer medidas de acción y tratamientos para aquellos riesgos que cuenten con controles débiles o sin control. Los planes de acción a implementar deben ser aprobados por la GRC en coordinación con su Gerencia dueña del proceso (de forma electrónica o física). En caso se presenten planes de acción que requieran presupuestos específicos para su implementación, las iniciativas deben ser informadas por los Gerentes de área al Gerente de Administración, Finanzas y Outsourcing de Remuneraciones para su aprobación.
 - Para aquellos riesgos que no pueden ser controlados, GRC en conjunto con la Gerencia de Administración, Finanzas y Outsourcing de Remuneraciones decidirán si aceptan estos riesgos o reducen el nivel de actividad implicado.
 - La unidad de Riesgo Operacional deberá verificar el cumplimiento de los controles establecidos.

- 6** Se debe gestionar los riesgos operacionales asociados a nuevos productos, servicios o cambios significativos en el ambiente operativo y/o informático. Para el desarrollo de nuevos productos o significativos, se dará énfasis en las actividades de control interno y administración de riesgo operacional cuando:
- Se ingrese a mercados no conocidos.
 - Se realicen negocios que son geográficamente distantes de la Oficina Principal.
 - La infraestructura de control de riesgos no esté acorde con el crecimiento de la nueva actividad del negocio.
 - Implice cambios significativos en los procesos operativos, de negocio o servicios informáticos utilizados.
 - Se debe gestionar los riesgos asociados a los bienes y/o servicios críticos y/o significativos provistos por terceros. críticos y/o significativos provistos por terceros.
 - Cuando se realice un proceso a través de servicios por terceros, los contratos que se firmen con el proveedor del servicio deben ser precisos con la finalidad que garanticen una clara asignación de responsabilidades. El alcance de la responsabilidad de terceros para compensar a cualquiera de las empresas del Grupo TAWA por errores, negligencia y otras fallas operativas debe ser parte de la evaluación de riesgos, debiendo establecer cláusulas de riesgo operacional en dichos contratos y en los casos que corresponda, de acuerdo con su criticidad se deberán elaborar SLA que establezcan y aseguren los acuerdos del servicio.
- 7** De las Incidencias y Eventos de Pérdida por Riesgo Operacional.
- La Unidad de Riesgo Operacional será la encargada de la administración de la Base de datos de pérdida para lo cual desarrollará políticas y procedimientos para la gestión de los eventos de pérdida de acuerdo con la normativa vigente.
 - Se clasificará los eventos en base al factor que lo origina y el tipo de evento, proponiendo, en coordinación con los dueños de procesos, las acciones correctivas y preventivas que eviten futuras situaciones similares.
- 8** De la gestión de la continuidad del negocio y de la seguridad de la información.
- El Sistema de Gestión de la Continuidad del Negocio, debe tener como objetivo implementar respuestas efectivas, para que la operatividad del negocio de la empresa continúe de una manera razonable ante la ocurrencia de eventos que puedan crear una interrupción o inestabilidad en las operaciones de la empresa. Dicho sistema estará enmarcado en el Plan de Continuidad del Negocio.
 - Asimismo, el Sistema de Gestión de la Seguridad de la Información, debe tener como objetivo garantizar la integridad, confidencialidad y disponibilidad de la información. Dicho sistema estará enmarcado en la SGSI-POL-01 Política de Seguridad de la Información.