RESUMEN DE LA GESTIÓN DE RIESGO OPERACIONAL

IV TRIMESTRE 2016

FINANCIERA CREDINKA S.A.

I. GESTIÓN DEL RIESGO OPERACIONAL

La Gestión de Riesgo Operacional de Financiera CREDINKA ha venido aplicando las exigencias de la Superintendencia de Banca, Seguros y AFP's en su Resolución SBS N° 2116 - 2009, a fin de continuar con el buen Gobierno Corporativo que caracteriza a las empresas del Grupo Diviso.

Indicadores Clave de Riesgos – KRI

Los indicadores clave de riesgo son variables que ofrecen una base razonable para estimar la probabilidad e impacto de uno o más eventos de riesgo operacional. Nos proporcionan alertas que ayudan a prevenir una posible materialización de los riesgos asociados a los procesos de la organización.

Mantenimiento y Recolección de Eventos de Pérdida

Con el objetivo de crear un marco de gestión permanente que permita controlar el Riesgo Operacional mediante el desarrollo e implementación de una metodología que permita identificar, medir, valorar y mitigar los riesgos operacionales que afecten a Financiera CREDINKA, las distintas unidades orgánicas son responsables de identificar y reportar al Departamento de Riesgo Operacional las pérdidas operacionales que se produzcan, asegurando así la integridad de la información presentada para analizar las causas que generaron las mismas y así determinar medidas preventivas y correctivas necesarias.

Por tanto, constantemente el Departamento de Riesgo Operacional captura los casos presentados, a fin de evaluar las causas que los originan y plantear acciones que permitan evitar situaciones similares.

Autoevaluación de Riesgos y Controles

La autoevaluación de riesgos y controles en los procesos se basa en 4 fases: entendimiento del proceso, identificación de riesgos y controles, evaluación de riesgos y controles; y el tratamiento a través de los planes de acción y monitoreo.

En el IV trimestre se ha realizado los talleres de autoevaluación de riesgos y controles (RCSA) de cuatro macro procesos, teniendo como resultado la respectiva matriz de riesgos para posteriormente realizar seguimiento a los planes de acción acordados a fin de mitigar riesgos relevantes.

Sistema de incentivos: oportunidad y consistencia de la información recolectada

Con la finalidad de establecer incentivos de reconocimiento a los Oficiales y Coordinadores de Gestión Integral de Riesgos de las Divisiones / Departamentos que hayan destacado en la Gestión de Riesgo Operacional, tal cual lo indica los reglamentos internos y de la SBS, el Departamento de Riesgo Operacional evalúa el desempeño de los mismos mediante un sistema de incentivos no monetarios.

Requerimiento de Capital por Riesgo Operacional

Actualmente se utiliza el método del indicador básico para el cálculo del requerimiento patrimonial por riesgo operacional el que es equivalente al promedio de los saldos anualizados de los márgenes operacionales brutos de la empresa considerando los 3 últimos años, multiplicado por un factor fijo (15%).

Capacitación Gestión de Riesgo Operacional: Departamento de Logística

Como parte del entrenamiento y concientización al personal sobre la gestión de Riesgo Operacional, se capacitó en temas puntuales como tipologías de impacto del evento por Riesgo Operacional, ciclo de vida de un evento, reportería y casuísticas de eventos de pérdida por Riesgo Operacional.

II. GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Prueba Integral de Continuidad de Negocio.

Se ejecutó la Prueba Integral de Continuidad del Negocio del periodo 2016, prueba que buscó poner en práctica los Planes de Continuidad del Negocio a fin de evaluar su viabilidad y asegurar que sean consistentes con los objetivos de la Financiera. El resultado de la prueba fue satisfactorio.

Pruebas específicas de Continuidad del Negocio en Agencias.

Se realizaron pruebas de continuidad del negocio en agencias, específicamente en las ciudades de Cusco y Cajamarca, esto con el fin de poner en práctica los Planes de Continuidad del Negocio existentes y probar su viabilidad. Así mismo, se buscó concientizar a los colaboradores sobre cómo responder eficazmente ante la

ocurrencia de una incidencia que afecte la operatividad de las agencias. Los resultados de las pruebas fueron satisfactorios.

Actualización del análisis de impacto al negocio

Se actualizó el Análisis de Impacto al Negocio (BIA) de la empresa, donde se identificó los procesos críticos, la prioridad de cada actividad dentro de cada proceso crítico y el tiempo en las que deben reanudarse (RTO) ante una paralización significativa podrían afectar la normal operatividad de la financiera.

Actualización de la evaluación de riesgos de interrupción del negocio

Se actualizó la Evaluación de Riesgos de Interrupción del Negocio, en esta actividad se identificaron los posibles riesgos y escenarios que podrían causar una interrupción de operaciones, con esta información y la identificada en el BIA se podrán definir y actualizar estrategias adecuadas para garantizar la continuidad del negocio de la financiera.

Indicadores clave para la continuidad del negocio

De acuerdo a lo dispuesto por la Circular SBS G-180-2015, a través del aplicativo SUCAVE se cumplió con el envío por SUCAVE a la SBS de los Reportes RO-1, RO-2, RO-3, y RO-4 relacionados a los indicadores clave de riesgo de la gestión de la continuidad del negocio.

Se cumplió con remitir la información de los reportes RO1 y RO2 dentro de la primera quincena de octubre de 2016, los mencionados reportes corresponden a información de sucesos ocurridos en los meses de julio, agosto, y setiembre 2016, la periodicidad de estos reportes es trimestral.

III. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La creciente dependencia y los sistemas que procesan información, junto con los riesgos, beneficios y oportunidades que esos recursos representan, han transformado a la gestión de la seguridad de la información en una función vital en todo ámbito. En especial si se tiene en cuenta que las tecnologías de la información mejoran sensiblemente las posibilidades de negocio, con lo cual su seguridad añade un valor significativo al momento de minimizar riesgos y, así mismo, disminuir pérdidas derivadas de eventos relacionados a la seguridad.

Capacitación Gestión de Seguridad de la Información

Se realizó la capacitación al personal sobre la gestión de Seguridad de la Información con el fin de concientizar, culturizar y desarrollar el sentido de responsabilidad para proteger la información de la Financiera. Asimismo se difundió un comunicado sobre el uso correcto de la nueva plataforma de correo.

Activos de Información

En el IV trimestre se realizó el taller de análisis y clasificación de los activos de información en coordinación con las jefaturas y/o gerencias, teniendo como resultado la matriz de inventario de activos de información. Cabe indicar que los activos de información se clasifican como Restringido, Confidencial, Uso Interno y de Uso Público.

Indicadores de Control de Seguridad de la Información

Se verificó los indicadores de control de seguridad de la información relacionados al control de accesos, seguridad de personal, seguridad física y ambiental, administración de las operaciones y comunicaciones y los controles de desarrollo y mantenimiento de sistemas informáticos.

Incidencias de Seguridad de la Información

Las incidencias de Seguridad de la información deben ser reportadas de tal manera que permitan realizar las acciones correctivas de forma oportuna. Se registra los incidentes de seguridad y las soluciones respectivas. En el IV trimestre se detectó varias incidencias relacionadas a seguridad de la información. Cabe indicar que todas estas incidencias ya fueron corregidas por la División de Tecnologías de la Información.