una empresa DIVISO GRUPO FINANCIERO

RESUMEN DE LA GESTIÓN DE RIESGO OPERACIONAL

I- TRIMESTRE 2015

CREDINKA S.A.
Unidad de Riesgo Operacional

GESTIÓN DE RIESGO OPERACIONAL

1. SÍNTESIS

1.1. RESUMEN SITUACIÓN

La Gestión de Riesgo Operacional como parte del plan operativo viene aplicando las metodologías de eventos de pérdida, indicadores clave de riesgo y autoevaluación de riesgos y controles de la cadena de valor de CREDINKA.

1.2. PLAN OPERATIVO ROP I- 2015

Con el objetivo de una mejora continua del Sistema de la Gestión de Riesgo Operacional de CREDINKA, se ha trabajado de acuerdo al plan operativo de la Unidad, realizando diversas actividades.

Los resultados del plan de trabajo al I Trimestre 2015, son:

- Elaboración y envío del IGROP a SBS.
- Ejecución de Talleres de Autoevaluación de Riesgos y Controles: Atención al Usuario
- Revisión, seguimiento y actualización de la Base de Datos de Pérdidas e Incidentes y reportes relacionados.
- Reforzamiento a las áreas durante el Proceso de Recolección y Reporte de Eventos de Pérdida.
- Revisión, seguimiento y actualización de los KRI y reportes relacionados. Seguimiento y reforzamiento a las áreas durante el Proceso de Cálculo de KRI.
- Monitoreo de los Planes de acción

1.3. ACTIVIDADES DE INTEGRACIÓN: CREDINKA – NUEVA VISIÓN

Durante el primer trimestre de 2015 se realizaron actividades de integración con la Financiera Nueva Visión.

Se vienen realizando actividades de implementación interna de las políticas, procedimientos, y metodologías, a través de las visitas a la financiera Nueva Visión haciendo la presentación de las metodologías de Riesgo Operacional.

1.4. PARTICIPACIÓN INSTANCIA DE REVISIÓN - DOCUMENTOS NORMATIVOS

Durante el primer trimestre la unidad de riesgo operacional participó en la revisión de 26 documentos normativos (entre políticas, procedimiento, manuales y circulares), esto como órgano de control en la etapa de revisión.

1.5. ACTUALIZACIÓN DE LA MATRIZ DE APETITO Y TOLERANCIA POR RIESGO OPERACIONAL.

- Se actualizó la metodología de autoevaluación de riesgos y controles estableciendo 10 niveles a los criterios (probabilidad e impacto) para la evaluación de los riesgos.
- Se agregaron 18 indicadores para el monitoreo del cumplimiento del plan estratégico.

2. METODOLOGIA DE AUTOEVALUACIÓN DE RIESGOS Y CONTROLES (RCSA)

2.1. TALLER DE AUTOEVALUACIÓN DE RIESGOS Y CONTROLES (RCSA)

La autoevaluación de riesgos y controles en los procesos se basa en 4 fases: conocimiento 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 presente Trimestre se ha iniciado con los Talleres de Autoevaluación de Riesgos y Controles (RCSA) de los procesos: Seguridad de la Información y Continuidad de Negocio, culminando la etapa de Identificación de procesos, elaborando los diagramas de bloque, diagramas de flujo e identificación de Controles.

3. METODOLOGÍA DE INDICADORES CLAVE DE RIESGOS – KRI

3.1. RESUMEN DE SITUACIÓN Y OBJETIVOS

Con la finalidad de identificar y tomar acción ante posibles alertas de riesgo o variaciones significativas en los Indicadores actualmente establecidos, este Primer Trimestre del 2015, la Unidad de Riesgo Operacional se ha mantenido constante con el monitoreo de los Indicadores Clave de Riesgo (KRI) mediante la información obtenida de las distintas unidades con el apoyo de los OGIR y CGIR designados.

4. METODOLOGÍA DE MANTENIMIENTO Y RECOLECCIÓN DE EVENTOS DE PÉRDIDA.

4.1. INTRODUCCIÓN:

Con el objetivo de mitigar la frecuencia e impacto de los eventos de pérdida por riesgo operacional en Credinka, la Unidad de Riesgo Operacional ha continuado poniendo en práctica la Metodología de Eventos de Pérdida a fin de identificar, evaluar, mitigar, monitorear, reportar eventos de pérdidas reales o potenciales y proponer planes de acción.

4.2. RESUMEN DE SITUACIÓN Y OBJETIVOS

Durante el periodo Enero – Marzo 2015, la Unidad de Riesgo Operacional ha continuado recibiendo de los Oficiales y Coordinadores de la Gestión Integral de Riesgos los reportes de eventos de riesgo operacional, con el objetivo de continuar administrando adecuadamente los eventos de riesgo operacional de Credinka.

4.3. MEJORAS EN LA GESTIÓN DE RIESGO OPERACIONAL – I TRIMESTRE 2015

Con el objetivo de lograr una mayor eficiencia en la Gestión de Riesgo Operacional, se decidió realizar ciertas modificaciones:

a) ***Actualización del Centro de Costos:*** Los centros de costos permiten asociar las pérdidas ocurridas con las unidades en las que se originan. De esta manera, se puede determinar qué unidades son las que generan mayor cantidad de eventos (frecuencia) y cuáles son las unidades más afectadas (impacto), permitiéndonos analizar de manera independiente cada una.

5. REQUERIMIENTO DE CAPITAL POR RIESGO OPERACIONAL

5.1. RESUMEN DE SITUACIÓN Y OBJETIVOS

Las empresas supervisadas por la Superintendencia de banca y seguros – SBS deben destinar patrimonio efectivo para cubrir el riesgo operacional que enfrentan. Para el cálculo de dicho requerimiento, las empresas deberán aplicar uno de los siguientes métodos:

a. Método del indicador básico
b. Método estándar alternativo
c. Métodos avanzados

Actualmente CREDINKA 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%).

6. SISTEMA DE INCENTIVOS

6.1. RESUMEN DE SITUACIÓN Y OBJETIVOS

El Sistema de incentivos, no económicos, para los Oficiales y Coordinadores de la Gestión Integral de Riesgos (OGIR y CGIR) consiste en la evaluación de: la oportunidad de entrega de la información, consistencia de la información, grado de implementación de los planes de acción y otras responsabilidades definidas juntos a los mismos que involucren temas de Riesgo Operacional. De esta manera, se logra obtener una calificación cuantitativa respecto al desempeño de los OGIR y CGIR durante un periodo determinado; Por ello, en el transcurso de este Trimestre 2015, la Unidad de Riesgo Operacional se ha mantenido constante con el seguimiento de dicho desempeño.

7. PLANES DE ACCIÓN

7.1. RESUMEN DE SITUACIÓN Y OBJETIVOS

Contribuyendo con la adecuada implementación de las 3 Metodologías de Riesgo Operacional dentro de la organización y con la finalidad de mitigar los riesgos identificados, se han definido, junto a las distintas Unidades involucradas, planes de acción, los mismos que son constantemente monitoreados mes a mes a fin de lograr su correcta implementación cumplimiento con los plazos determinados.

GESTIÓN DE CONTINUIDAD DEL NEGOCIO

8. SÍNTESIS

8.1. RESUMEN SITUACIÓN

La Gestión de Continuidad de Negocio de CREDINKA viene aplicando la mejora continua y el constante alineamiento con las buenas prácticas internacionales como la BS-25999 y las exigencias de la SBS en su Circular G-139-2009.

En tal sentido, informamos que se cumplió con el 100% de lo estipulado en el plan operativo correspondiente al I Trimestre del período 2015 de la Unidad de Riesgo Operacional - Continuidad del Negocio.

8.2. SIMULACRO DE ASALTO AL CENTRO DE REANUDACIÓN DE LABORES

El pasado 29 de enero del 2015 se desarrolló un Simulacro de Asalto programado con Asbanc y el comando de Águilas Negras de la Policía Nacional del Perú en las instalaciones del Centro de Reanudación de Labores de CREDINKA ubicado en la Av. Nicolás de Piérola #626 – Cercado de Lima. Este simulacro fue coordinado por la Unidad de Seguridad Interna donde la Unidad de Riesgo Operacional participó de veedor.

Al respecto podemos informar que se han obtenido resultados positivos en la reacción para estos casos, el Escuadrón PNP DEPSEBAN "Águilas Negras" tiene determinado patrullaje de motocicletas en la zona donde se ubica nuestro Centro de Reanudación de Labores debido al alto tráfico que existe, logrando una reacción (movilización) de aproximadamente 4 minutos luego de la activación de las alarmas del Centro de Reanudación de Labores.

8.3. ACTUALIZACIÓN DE RELACIÓN DE BRIGADISTAS DE EMERGENCIA

En cumplimiento con la Circular SBS G-139-2009 y la normativa interna como el "Plan de Emergencia y Evacuación" de Continuidad del Negocio y la "Política de Seguridad en caso de Siniestros" de Seguridad Interna, se actualizó las brigadas de emergencia de las oficinas y/o agencias de CREDINKA.

GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

9. SÍNTESIS

9.1. RESUMEN SITUACIÓN

En el primer trimestre de 2015, la Unidad de Riesgo Operacional (Seguridad de la Información) ha realizado entre las actividades más resaltantes:

- Detección de vulnerabilidades relacionadas con la fuga de información.
- Revisión de pistas de Auditoria.
- Revisión de controles de Seguridad de la Información.
- Monitoreo a los Incidentes de Seguridad de la Información.

10. PLATAFORMA DE GESTIÓN INTEGRAL DE RIESGOS-ARCOMYL

10.1. ASPECTOS RELEVANTES

La Plataforma de Gestión Integral de Riesgos viene siendo trabajada de forma continua según los requerimientos funcionales proporcionados por los dueños del proceso, la misma que ya nos muestra alcances certeros para cada una de las metodologías.

10.2. MÓDULO DE RIESGO OPERACIONAL

El Módulo de Riesgo Operacional se viene avanzando de manera progresiva modificando el diseño en base a estándares proporcionados por TI. Además, se está realizando la inclusión del Reporte de Evento de Riesgo Operacional dentro de ARCOMYL con el fin de centralizar las tareas de los OGIR/CGIR en un solo entorno.

10.2.1. FASES DE ELABORACIÓN DEL MÓDULO DE RIESGO OPERACIONAL

El Módulo de Riesgo Operacional consta de 4 fases de elaboración:

Fase 1 : Módulo de Recolección y Mantenimiento de Eventos de Pérdida
Fase 2 : Módulo de Autoevaluación de Riesgos y Controles
Fase 4 : Módulo de Identificadores de Riesgo KRI's
Fase 5 : Módulo de Seguimiento y Monitoreo de Planes de Acción

11. MÓDULO DE AUTOEVALUACIÓN DE RIESGOS Y CONTROLES

El módulo de Autoevaluación de Riesgos y Controles se viene desarrollando de manera progresiva en base a los requerimientos funcionales obtenidos. Actualmente dicho proceso se encuentra en la etapa de Desarrollo e Implementación del Sistema.