RESUMEN DE INFORME DE GESTIÓN DE RIESGO OPERACIONAL

II-TRIMESTRE 2013

CREDINKA S.A.
Unidad de Riesgo Operacional

CAPITULO I GESTIÓN DEL RIESGO OPERACIONAL

La Unidad de Riesgo Operacional como parte de la Gestión Integral de Riesgos, es la responsable de evaluar, dirigir y supervisar las actividades operacionales, en base al cumplimiento de la normativa regulatoria, el desarrollo de metodologías de medición y el establecimiento de planes de acción para la mitigación de los Riesgos Operacionales que afectan a la Caja Rural de Ahorro y Crédito CREDINKA.

Enfocándose en tres principales Gestiones: Gestión de Riesgo Operacional, Gestión de Seguridad de Información y Gestión de Continuidad del Negocio.

GESTIÓN DE RIESGO OPERACIONAL

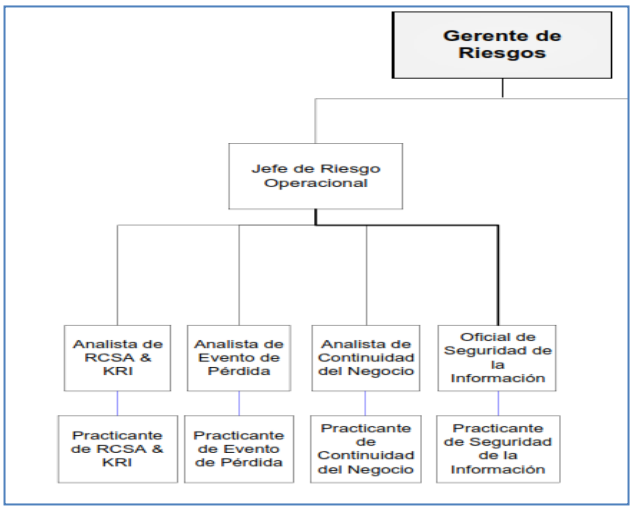
1. SÍNTESIS

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.

Con el fin de lograr los objetivos trazados y fortalecer la unidad de Riesgo Operacional, actualmente se encuentra conformada de la siguiente manera:

Cuadro 1 – Conformación de la Unidad de Riesgo Operacional



1.2. PLAN OPERATIVO ROP II- 2013

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 II Trimestre 2013, son:

- ✓ Elaboración y envío del IGROP a SBS.
- ✓ Monitoreo de los Planes de acción de Talleres de Autoevaluación de Riesgos y Controles: Colocaciones - Captaciones - Gestión de Riesgos - Gestión de Recursos Humanos - Legal, Control y Cumplimiento - Soporte Contable - Soporte Tecnológico.
- ✓ 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.

2. METODOLOGÍA DE INDICADORES CLAVE DE RIESGOS – KRI

2.1. RESUMEN DE SITUACIÓN Y OBJETIVOS

Los Indicadores de Riesgo – KRI, nos ayudan a detectar señales tempranas sobre la exposición creciente de los riesgos a los que están expuestas las diversas áreas de negocios, de manera que alerten sobre esta situación y puedan adoptarse las medidas correctivas que resulten pertinentes, antes de que los efectos negativos se hayan materializado sobre los objetivos.

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, así también, es una herramienta que permite la validación, cálculo y monitoreo de los indicadores clave de riesgo, para todos los procesos clave de las Unidades de apoyo o Soporte y Negocios.

2.2. SEGUIMIENTO Y ANALISIS

La Unidad de Riesgo Operacional es la encargada de consolidar la información enviada por los Oficiales y Coordinadores de la gestión integral de riesgos (OGIR y CGIR) para luego analizarla y procesarla.

Como resultado, a partir del mes de Mayo, se cuenta con 39 indicadores redefinidos y reorganizados

Las fluctuaciones son alertas que nos indican la existencia de una posible exposición ante un evento de riesgo operacional por lo que, conjuntamente con los OGIR y CGIR, se analiza la información, de manera tal, que si se detecta una brecha se defina un plan de acción correctivo con el fin de reducir nuestro nivel de exposición acorde a nuestra metodología de apetito y tolerancia al riesgo operacional.

3. SISTEMA DE INCENTIVOS

3.1. RESUMEN DE SITUACIÓN Y OBJETIVOS

La evaluación para la aplicación de incentivos es realizada por la Gerencia de la Unidad de Riesgos con la finalidad de calificar la gestión de riesgo operacional de las áreas/unidades de negocio y soporte. No obstante se realizan calificaciones parciales de manera trimestral con el objetivo que las gerencias evaluadas puedan conocer como están gestionando el riesgo operacional de su unidad o área y tomar las medidas de acción respectiva para mejorar dicha gestión.

4. PLANES DE ACCIÓN

Una gestión eficiente del riesgo operacional requiere una revisión continua de los riesgos identificados así como de las acciones planteadas por los usuarios como parte del tratamiento de los mismos, por lo que la unidad de ROP desarrolló una matriz de seguimiento de Planes de Acción, los mismos que son monitoreados mensualmente con el fin de asegurar su implementación dentro de los plazos pactados.

Dicho monitoreo de planes de acción se realiza de acuerdo a nuestras metodologías de Riesgo Operacional, teniendo a la fecha 19 planes de acción implementadas por la metodología de Talleres de Autoevaluación de Riesgos y Controles (RCSA), Monitoreando el proceso de implementación de 93 planes de acción por la metodología (RCSA) ; 04 planes de acción por la metodología de Indicadores Clave de Riesgo (KRI) y 07 planes de acción y por la metodología de eventos de Pérdida (EP).

5. GESTIÓN DE CONTINUIDAD DEL NEGOCIO

5.1. SÍNTESIS

5.1.1. RESUMEN SITUACIÓN

La gestión de continuidad del negocio de CREDINKA se viene aplicando la mejora continua de la metodología y busca estar alineado con las buenas prácticas internacionales BS-25999 y las exigencias de la SBS Circular G-139-2009, en ese sentido se cumplió con el 100% del plan operativo correspondiente al 2do trimestre del período 2013

- ✓ Análisis de impacto al negocio – BIA.
- ✓ Aprobación y difusión de los planes específicos de continuidad – PEC.
- ✓ Actualización de gestión de incidentes de continuidad del negocio - árbol de llamadas.
- ✓ Concientización sobre la gestión de incidentes.
- ✓ Ejecución del simulacro de sismo.

5.1.2. APROBACIÓN Y DIFUSIÓN DE LOS PLANES ESPECÍFICOS DE CONTINUIDAD – PEC

En la Sesión de Directorio de junio de 2013, se aprobó la actualización de los planes específicos de continuidad – PEC:

- PEC de Operaciones Centrales.
- PEC de Control de Préstamos y Garantías.
- PEC de Banca Electrónica.
- PEC de Tesorería.
- PEC de Captaciones y Servicios.

5.1.3. EJECUCIÓN DEL SIMULACRO DE SISMO

Objetivo del Simulacro

- Estar preparados para salvaguardar la integridad física de los colaboradores, de los clientes y visitantes que se encuentren en las instalaciones de CREDINKA.
- Poner en práctica el Plan de Emergencia y Evacuación lo cual permite que todos los colaboradores estén familiarizados ante una emergencia real.
- Estar preparados para salvaguardar la integridad física de los colaboradores, de los clientes y visitantes que se encuentren en las instalaciones de CREDINKA.

- Corregir las deficiencias que pudieran observarse durante la realización del simulacro.
- Detectar errores u omisiones en las actuaciones del Plan de Emergencia y Evacuación.
- Estimar los tiempos de evacuación.
- Cumplir con los procedimientos de emergencia especificados en el Plan de Emergencia y Evacuación.

Organización de CREDINKA ante una Emergencia

CREDINKA ante una emergencia se encuentra conformado por brigadistas, que tienen la responsabilidad de actuar antes, durante y después de la emergencia, e informar las medidas de seguridad que deben tener los colaboradores de CREDINKA ante una situación de emergencia.

6. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

6.1. SÍNTESIS

6.1.1. RESUMEN SITUACIÓN

En el año 2013, se ha enfocado en la implementación del Sistema de Gestión de Seguridad de la Información en CREDINKA, de acuerdo a la Circular N° G-140-2009 Ref. Gestión de la Seguridad de la Información emitida por la SBS, en ese sentido se ha cumplido con el plan operativo del segundo trimestre del año 2013.

Los resultados del segundo trimestre del año 2013, se resume en lo siguiente:

- ✓ Seguridad Lógica- Gestión de accesos y monitoreo de los accesos otorgados.
- ✓ Informe de revisión de Directorio activo
- ✓ Informe de pruebas de intrusión y vulnerabilidad en los sistemas informáticos.
- ✓ Informe de Revisión de Información para el ambiente de pruebas.
- ✓ Informe de inspección realizada a Bóveda de TIP-La colmena.
- ✓ Informe de navegación de internet – Recibidor Pagador.
- ✓ Informe de navegación de internet – ejecutivo de Captaciones y Oficiales de Negocios Hipotecarios
- ✓ Llamados de atención a usuarios por el no cumplimiento de las políticas

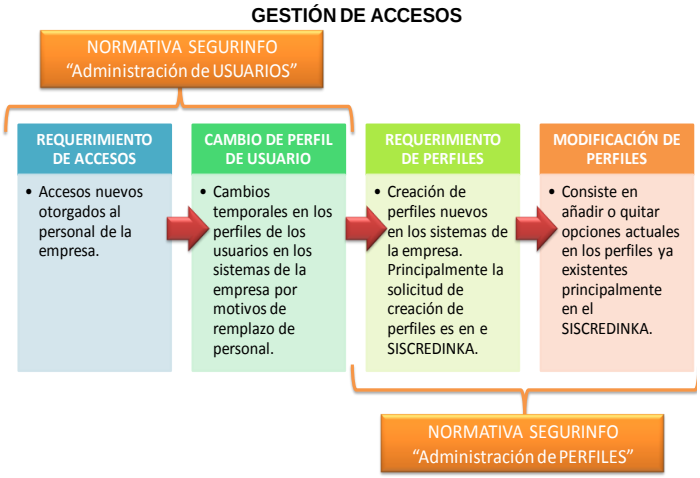
6.2. SEGURIDAD LOGICA-GESTION DE ACCESOS Y MONITOREO DE LOS ACCESOS OTORGADOS A LOS COLABORADORES

6.2.1. GESTIÓN DE ACCESOS

La Gestión de Accesos comprende:

- ✓ REQUERIMIENTO DE ACCESOS: Accesos nuevos otorgados al personal de la empresa.
- ✓ CAMBIO DE PERFIL DE USUARIO: Cambios temporales en los perfiles de los usuarios en los sistemas de la empresa por motivos de remplazo de personal.

- ✓ REQUERIMIENTO DE PERFILES: Creación de perfiles nuevos en los sistemas de la empresa. Principalmente la solicitud de creación de perfiles es en el SISCREDINKA.
- ✓ MODIFICACIÓN DE PERFILES: Consiste en añadir o quitar opciones actuales en los perfiles ya existentes principalmente en el SISCREDINKA.



6.3. REVISIÓN DE DIRECTORIO ACTIVO

✓ Objetivo

- Verificar que se cumpla el correcto bloqueo de usuarios del directorio activo en lo referente a la gestión de accesos al Directorio Activo.

6.4. PRUEBAS DE INTRUSIÓN Y VULNERABILIDAD EN LOS SIST. INFORMATICOS

✓ Objetivo

Evaluar la seguridad de los sistemas informáticos de CREDINKA, con la finalidad de identificar sus vulnerabilidades y emitir observaciones y recomendaciones de seguridad a fin de garantizar la integridad, confidencialidad y disponibilidad de la información.

6.5. REVISIÓN DE INFORMACIÓN PARA EL AMBIENTE DE PRUEBAS.

✓ Objetivo

Revisar que la información confidencial de CREDINKA a utilizar en el ambiente de pruebas, se encuentre alterada a fin de proteger la información del core del negocio.

6.6. INSPECCIÓN DE BOVEDA DE TIP-LA COLMENA.

✓ Objetivo

Revisar el ambiente de bóveda asignado a la Gerencia de Tecnologías de la Información y Procesos a fin de verificar el cumplimiento del internamiento y resguardo del backup en cumplimiento de la Circular SBS G-140-2009 Gestión de la Seguridad de la Información.

6.7. NAVEGACIÓN DE INTERNET .

✓ Objetivo

Revisar el reporte de navegación de internet de los colaboradores, a fin de verificar que los perfiles de acceso a internet definidos en CREDINKA se otorguen de forma correcta y de acuerdo al cargo de cada colaborador.