RESUMEN DE INFORME DE GESTIÓN DE RIESGO OPERACIONAL

III-TRIMESTRE 2013

CREDINKA S.A.
Unidad de Riesgo Operacional

ÍNDICE GENERAL

LISTA CUADROS

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

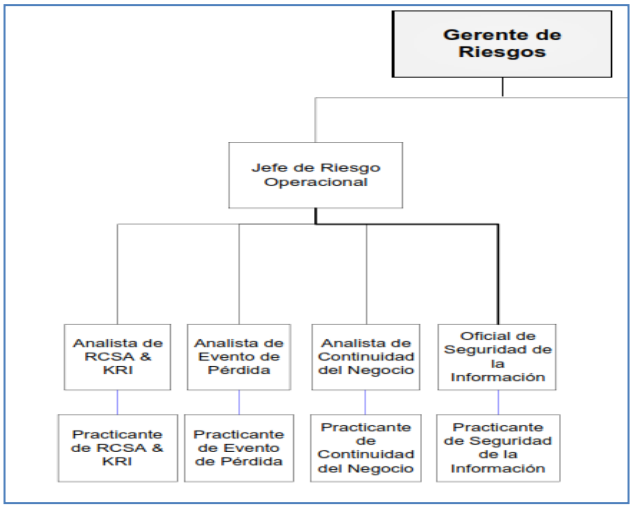
1. SÍNTESIS

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



2. TALLER DE AUTOEVALUACION DE RIESGOS Y CONTROLES

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.

En el III Trimestre se viene desarrollando Talleres de Autoevaluación de Riesgos y controles (RCSA) al proceso de Atención al Usuario a través de videoconferencia interviniendo el Oficial de Atención al usuario y El Jefe de Plataforma de Servicios y la Unidad Organización y Métodos, estando en la fase 1 de "Conocimiento del Proceso", programando su culminación en Diciembre del 2013 con los planes de acción.

3. CONTRATACION SIGNIFICATIVA.

3.1. IDENTIFICACION Y PROGRAMACION DE VISITA

En cumplimiento del plan operativo, se ha determinado la visita a 04 empresas Proveedora de servicios de Subcontratación Significativa, para ello se utilizará como herramientas de validación de la calidad de los servicios:

- Cuestionario de Evaluación de los proveedores con Contratación Significativa.
- Visita de Inspección mes de Noviembre del 2013.

4. CAPACITACION DE LA GESTION DE RIESGO OPERACIONAL

La capacitación sobre la Gestión de Riesgo Operacional (riesgo operacional, continuidad del negocio y seguridad de información), se programa su realización utilizando el aplicativo " Aula Virtual" en el mes de Noviembre del 2013.

5. SISTEMA DE INCENTIVOS

Es importante destacar a los OGIR y CGIR que obtuvieron la máxima calificación gracias al cumplimiento de las metodologías de Autoevaluación de Riesgos y Controles, Mantenimiento y Recolección de Eventos de Pérdida e Indicadores Clave de Riesgos, esta calificación responde a la oportunidad de la entrega de información, Consistencia de la información y Grado de Implementación de los Planes de Acción; La Unidad de Auditoría Interna a través de su Oficial y Coordinador de la gestión integral de riesgos obtuvieron la calificación más alta en el cumplimiento de la gestión de riesgo operacional.

GESTIÓN DE CONTINUIDAD DEL NEGOCIO

6. SÍNTESIS

6.1. RESUMEN SITUACIÓN

La gestión de continuidad del negocio de CREDINKA 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 3er trimestre del período 2013 correspondiente a la Unidad de Riesgo Operacional (Continuidad del Negocio).

6.2. PLANIFICACIÓN DE PRUEBA DEL PLAN DE CONTINUIDAD DEL NEGOCIO

- **Objetivo:**

  Con el fin de continuar con la puesta en práctica de los Planes de Continuidad del Negocio, así como la concientización de la Alta Dirección y los Colaboradores Claves de CREDINKA sobre cómo responder eficazmente ante una contingencia mayor, se ha planificado la prueba del Plan de Continuidad del Negocio, la cual se realizará en el mes de Noviembre del 2013

- **Escenario:**

  - ✓ Un sismo igual o superior a grado IX de Mercalli o 8 de Richter, que afecte la Oficina de Gestión - Lima y el Centro Principal de Cómputo.
  - ✓ Falla total de proveedores críticos de enlaces de comunicación.
  - ✓ Indisponibilidad total de los sitemas informáticos.
  - ✓ Indisponibilidad de telefonía móvil.

- **Alcance:**

  - ✓ Ejecución del plan de manejo de crisis.
  - ✓ Ejecución del árbol de llamadas del PMC.
  - ✓ Activación de los Planes Específicos de Continuidad del Negocio.
  - ✓ Notificación al Equipo de Recuperación de Desastres.
  - ✓ Actividades en Período de Contingencia del Plan de Recuperación de Desastres.
  - ✓ Ejecución de actividades para la vuelta a la Normalidad del Plan de Recuperación de Desastres.
  - ✓ Notificación a los Equipos de Recuperación.
  - ✓ Ejecución de todas las comunicaciones vía celular (mensajes de texto).

GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

6.3. SÍNTESIS RESUMEN SITUACIÓN

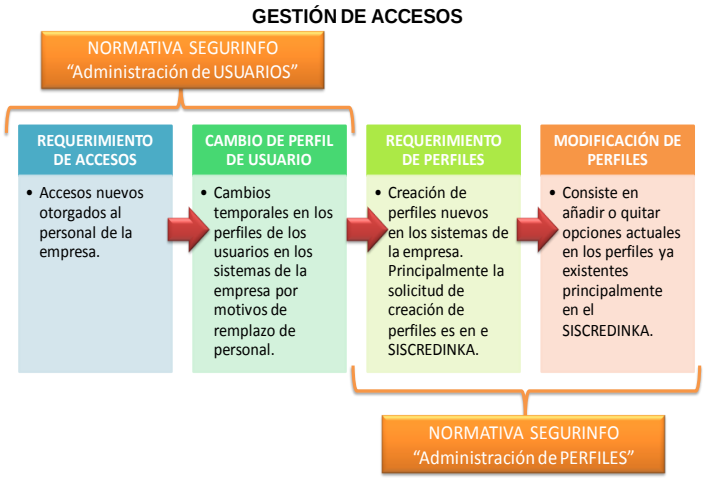
Actualmente CREDINKA, se ha enfocado en la implementación del Sistema de Gestión de Seguridad de la Información en de acuerdo a la Circular N° G-140-2009 y su modificatoria Circular SBS N° G-167-2012 Ref. Gestión de la Seguridad de la Información emitida por la SBS, en ese sentido se ha cumplido con el plan operativo del Tercer trimestre del año 2013.

6.4. SEGURIDAD LOGICA-GESTION 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.

Cuadro 2 – Gestión de Accesos en CREDINKA



6.5. VISITA A AGENCIAS

En el 3er trimestre el oficial de Seguridad de Información realizó visita a las Agencias Magisterio, Gestión Cusco, Av. El Sol, San Sebastián, Universidad Andina del Cusco; Abancay, Las Américas, Anta, Curahuasi, Urcos y Urubamba, a fin de verificar los acceso a internet , puertos USB, Lectora/Grabadora de CD , verificar que los equipos de los colaboradores tengan instalado el antivirus actualizado, entre otros, formulando las recomendaciones respectivas para una eficiente gestión de seguridad de la información.

6.6. INFORME DE RESTAURACION DE COPIAS DE RESPALDO

El oficial de Seguridad de Información a fin de verificar que las copias BACKUP se esten realizando correctamente realizó una prueba de restauración el cúal contempló un escenario en donde se perdió toda la información del centro de procesamiento de datos principal y alterno, procediendo a realizar la restauración de la base de datos a partir de las cintas offsite; concluyendo que la prueba de restauración de la base de datos se realizó de forma exitosa, verificando ademas que el acceso a la Bóveda de TIP donde se custodia las cintas Backup cumple con el acceso dual y el correcto almacenamiento, recomendando continuar con la realización de las prueba de restauración de las Base de datos del sistema principal por lo menos una vez al año, a fin de garantizar la confidencialidad, integridad y disponibilidad de la Información.