INFORME DE GESTIÓN DE RIESGO OPERACIONAL

I- TRIMESTRE 2014

CREDINKA S.A.
Unidad de Riesgo Operacional

ÍNDICE GENERAL

1. SÍNTESIS....3
   1.1. RESUMEN SITUACIÓN....3
   1.2. PLAN OPERATIVO ROP I- 2014....3
   1.3. INFORME IG-ROP....3
   1.4. TALLER DE AUTOEVALUACIÓN DE RIESGOS Y CONTROLES (RCSA)....3
   1.5. CAPACITACIONES DE LA GESTIÓN INTEGRAL DE RIESGOS....4
2. METODOLOGÍA DE INDICADORES CLAVE DE RIESGOS – KRI....4
   2.1. RESUMEN DE SITUACIÓN Y OBJETIVOS....4
3. SISTEMA DE INCENTIVOS....4
   3.1. RESUMEN DE SITUACIÓN Y OBJETIVOS....4
4. SÍNTESIS....4
   4.1. RESUMEN SITUACIÓN....4
5. DETALLE DEL INFORME....4
   5.1. ACTUALIZACIÓN DE RELACIÓN DE BRIGADISTAS....4
   5.2. ACTUALIZACIÓN DE LA NORMATIVA INTERNA DE CONTINUIDAD DEL NEGOCIO....5
6. SÍNTESIS....5
   6.1. RESUMEN SITUACIÓN....5
7. DETALLE DEL INFORME....5
   7.1. NORMATIVA Y ORGANIZACIÓN DEL SGSI....5
      7.1.1. PROCEDIMIENTOS....5
   7.2. GESTIÓN DEL CONTROL DE ACCESOS....5
      7.2.1. MONITOREO DE ACCESOS....6
   7.3. INFORME DE REVISIÓN DE PERFILES DE CORREO E INTERNET Y BLOQUEOS DE USUARIOS DE DIRECTORIO ACTIVO....6
   7.4. REVISIÓN DEL MANTENIMIENTO PREVENTIVO DE LOS EQUIPOS DEL CENTRO DE COMPUTO PRINCIPAL Y ALTERNO....6
   7.5. COMUNICADOS DE SEGURIDAD DE LA INFORMACIÓN....6

GESTIÓN DE RIESGO OPERACIONAL

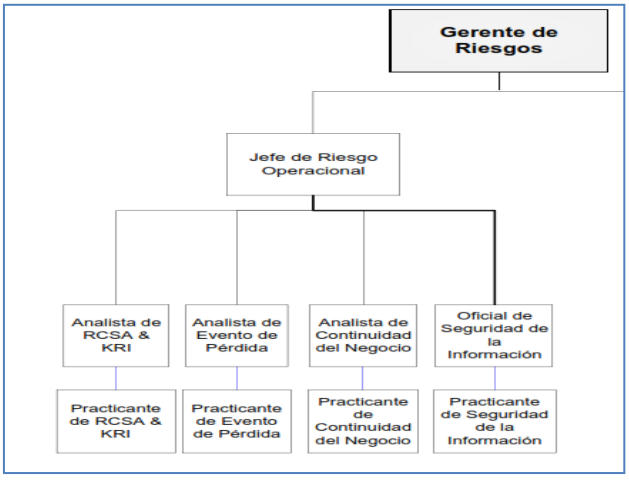
1. SÍNTESIS

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 I- 2014

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 2014, 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. INFORME IG-ROP

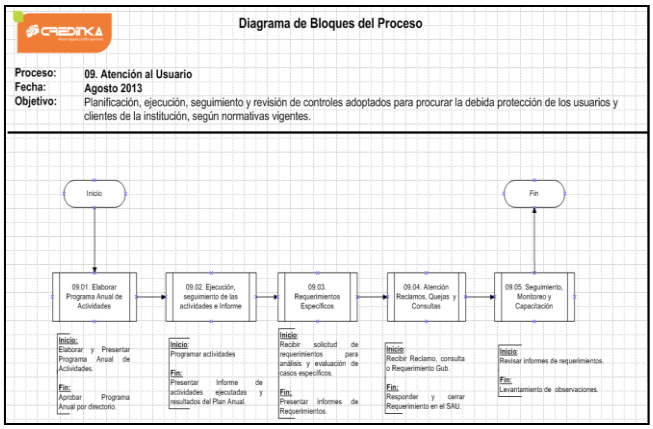
El 31 de Enero del 2014, La Unidad de Riesgo Operacional cumplió con la presentación del IG-ROp Informe de la Gestión de Riesgo Operacional del 2013 a través de la extranet de la SBS, dicho informe consta de 14 puntos de información, cumpliendo con presentarlo dentro de la fecha establecida.

1.4. 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 concluido con los Talleres de Autoevaluación de Riesgos y controles (RCSA) del proceso Atención al Usuario, donde se elaboraron Diagrama de bloques; Diagramas de Flujo, Matrices de Riesgos identificando los Riesgos, Controles y estableciendo Planes de acción para su monitoreo correspondiente.

Cuadro 2 – Diagrama de Bloques del Proceso: Atención al Usuario



1.5. CAPACITACIONES DE LA GESTIÓN INTEGRAL DE RIESGOS.

La capacitación de la Gestión Integral de Riesgos del periodo del 2013 se realizó de forma virtual en dos etapas. En la primera etapa se realizó la difusión del material de apoyo para la resolución de la evaluación (diapositivas) por medio del correo electrónico a todos los colaboradores de CREDINKA con fecha 03 de Diciembre del 2013. En la segunda etapa, se procedió con el envío del examen con fecha 09 de Diciembre del 2013 para su desarrollo por los colaboradores vía electrónica (escaneado), los colaboradores que no disponían de correo, realizaron el envió físico de sus exámenes a la unidad ROP.

2. METODOLOGÍA DE INDICADORES CLAVE DE RIESGOS – KRI

2.1. RESUMEN DE SITUACIÓN Y OBJETIVOS

Con el fin de continuar con los resultados obtenidos en el año 2013 producto de la adecuada gestión de los Indicadores Clave de Riesgo (KRI´S), la Unidad de Riesgo Operacional, con el apoyo de los Oficiales de la Gestión Integral de Riesgos (OGIR) y los Coordinadores de la Gestión Integral de Riesgos (CGIR), ha continuado recibiendo la información necesaria de los indicadores para su cálculo y posterior análisis.

3. SISTEMA DE INCENTIVOS

3.1. RESUMEN DE SITUACIÓN Y OBJETIVOS

Para este I Trimestre 2014 se puede observar que se han logrado mejores resultados, respecto al año anterior.

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 y el grado de implementación de los planes de acción. De esta manera, se logra obtener una calificación cuantitativa respecto al desempeño de los OGIR y CGIR en la Gestión Integral de Riesgo Operacional.

GESTIÓN DE CONTINUIDAD DEL NEGOCIO

4. SÍNTESIS

4.1. 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 plan operativo correspondiente al 1er trimestre del período 2014 correspondiente a la Unidad de Riesgo Operacional (Continuidad del Negocio).

A continuación se muestra los resultados de la gestión de continuidad del negocio del primer trimestre de 2014:

- ✓ Se activaron con normalidad los planes específicos de continuidad del negocio en determinadas agencias en cumplimiento a la gestión de incidentes de continuidad del negocio.
- ✓ Se actualizó la relación de brigadistas de las agencias y oficinas de CREDINKA, debido a los colaboradores cesados que formaban parte de las brigadas de emergencia.
- ✓ Se actualizó normativas internas de Continuidad del Negocio.
- ✓ Participación en el "Taller de Continuidad de Negocios para el Sector Financiero" ofrecido la Superintencia de Banca, Seguros y AFPs.

5. DETALLE DEL INFORME

5.1. ACTUALIZACIÓN DE RELACIÓN DE BRIGADISTAS

En cumplimiento con la Circular SBS G-139-2009 y la normativa interna "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.

Se solicitó a la Unidad de Gestión del Talento y Capital Humano, la relación de los colaboradores cesados que formaban parte de las brigadas de emergencia, por lo cual se convocó a nuevos colaboradores que puedan apoyar reemplazando a los brigadistas faltantes.

5.2. ACTUALIZACIÓN DE LA NORMATIVA INTERNA DE CONTINUIDAD DEL NEGOCIO

Durante el 1er trimestre del 2014 se actualizó las normativas internas de continuidad del negocio, con el objetivo de mejorar la base para el entendimiento, desarrollo e implementación de la continuidad del negocio en CREDINKA.

Así mismo se revisó la documentación a fin de que se encuentre alineada con las buenas prácticas del Estándar Británico BS-25999, referido a la Gestión de Continuidad del Negocio.

Los documentos que se listan a continuación se encuentran bajo la revisión de la Unidad de Organización y Métodos, para su posterior aprobación.

- ✓ Política de Gestión de la Continuidad del Negocio
- ✓ Guía Metodológica de Gestión de la Continuidad del Negocio.

GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

6. SÍNTESIS

6.1. RESUMEN SITUACIÓN

En el primer trimestre del 2014, la Unidad de Riesgo Operacional (Seguridad de la Información) ha realizado las siguientes actividades:

- ❖ Normativa y Organización del SGSI.
- ❖ Gestión del Control de Accesos.
- ❖ Revisión de los Perfiles del Correo e Internet y Bloqueos de Usuarios del Directorio Activo
- ❖ Incidentes de Seguridad de la Información.
- ❖ Revisión del mantenimiento preventivo de equipos del Centro de Cómputo Principal y Alterno.
- ❖ Comunicados de seguridad de la información.
- ❖ Llamados de atención a usuarios por el incumplimiento de las políticas.

7. DETALLE DEL INFORME

7.1. NORMATIVA Y ORGANIZACIÓN DEL SGSI

7.1.1. PROCEDIMIENTOS

Se actualizó la Metodología para la gestión de Activos, y su publicación se realizó el día 21 de enero del 2014.

El procedimiento de Administración de Perfiles y administración de cuentas de usuarios se encuentra en proceso de revisión.

Cabe mencionar que se viene realizando reuniones con la Unidad de Organización y Métodos, para la elaboración de los sub procesos del proceso de gestión de Seguridad de la Información, se han establecido cuatro sub procesos principales, los cuales mencionamos a continuación:

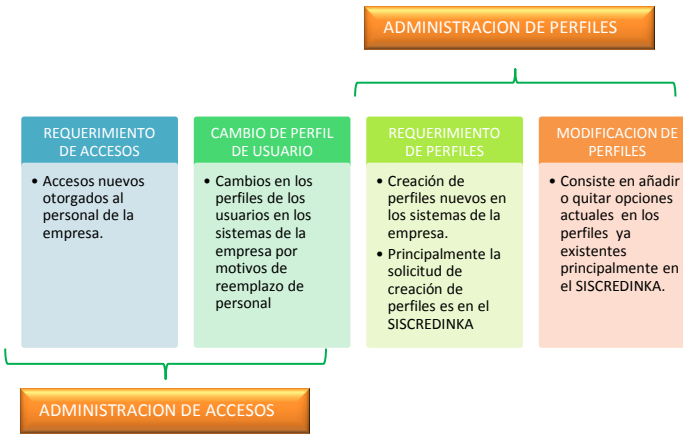
- ❖ Subproceso de Gestión de accesos y perfiles.
- ❖ Subproceso de Gestión de activos de la información.
- ❖ Subproceso de Gestión de incidencias de seguridad de la información.
- ❖ Subproceso de Operaciones y comunicaciones.

7.2. GESTIÓN DEL CONTROL DE ACCESOS

La Gestión de accesos y perfiles comprende:

- ❖ REQUERIMIENTO DE ACCESOS: Accesos nuevos otorgados al personal de la empresa.
- ❖ CAMBIO DE PERFIL DE USUARIO: Cambios 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 3 – Gestión de Accesos en CREDINKA



7.2.1. MONITOREO DE ACCESOS

Se realiza dos veces por semana el monitoreo de los accesos comparando los reportes enviados por la Unidad de Gestión del Talento y Capital Humano (personal cesado y personal de vacaciones) y los requerimientos de accesos, cambios de perfil, modificaciones de perfil y requerimientos de perfil enviados a la Unidad de Servicios Informáticos.

Monitoreo de Bloqueos de los Accesos a Usuarios.

Para medir la efectividad de los bloqueos solicitados a servicios TI, hemos establecido un indicador de monitoreo de los bloqueos que no han sido atendidos de manera oportuna respecto al total de bloqueos solicitados.

$$Ind_1 = \frac{Bloqueos\ no\ atendidos\ oportunamente}{Total\ de\ bloqueos\ solicitados}$$

7.3. INFORME DE REVISIÓN DE PERFILES DE CORREO E INTERNET Y BLOQUEOS DE USUARIOS DE DIRECTORIO ACTIVO

✓ Objetivo

- Revisar que la asignación de los Perfiles de accesos a internet y correo electrónico de los colaboradores se encuentre de acuerdo a los perfiles establecidos en CREDINKA.
- Revisar que el bloqueo de accesos en el directorio activo por ceses, licencias, vacaciones, u otros motivos, se realice en las fechas solicitadas por la Unidad de Gestión del Talento y Capital Humano.

7.4. REVISIÓN DEL MANTENIMIENTO PREVENTIVO DE LOS EQUIPOS DEL CENTRO DE COMPUTO PRINCIPAL Y ALTERNO

Con la información proporcionada por parte de la Jefatura de Infraestructura, en las HOJAS DE MANTENIMIENTO, se verificó el mantenimiento preventivo a los equipos del Centro de Cómputo Principal (CCP), siendo estos los sistemas revisados:

- Sistema de Seguridad
- Sistema de Protección Eléctrica.
- Sistema de Respaldo.
- Sistema de Climatización.

Además de la revisión de los INFORMES TÉCNICOS, 0129, 0130 y 0132 del 2014, se verificó el mantenimiento preventivo del Centro de Computo Alterno (CCA), siendo estos los sistemas revisados:

- Sistema de Climatización.
- Sistema de Seguridad

7.5. COMUNICADOS DE SEGURIDAD DE LA INFORMACIÓN