RESUMEN DE INFORME DE GESTIÓN DE RIESGO OPERACIONAL

IV- TRIMESTRE 2013

CREDINKA S.A.
Unidad de Riesgo Operacional

ÍNDICE GENERAL

GESTIÓN DE RIESGO OPERACIONAL

1. SÍNTESIS

La Gestión de Riesgo Operacional en cumplimiento del plan operativo 2013 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.

1.1. PLAN OPERATIVO ROP IV TRIMESTRE 2013

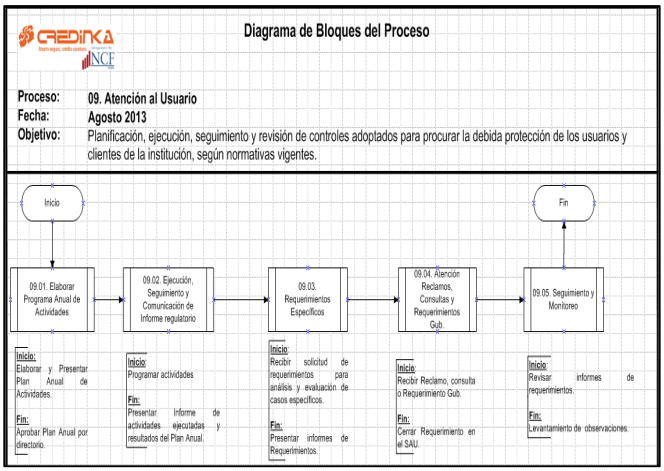
Los resultados del plan de trabajo al IV Trimestre 2013, son:

- Capacitación y evaluación a todos los colaboradores de CREDINKA sobre la Gestión de Riesgo Operacional.
- Ejecución de talleres de autoevaluación de riesgos y controles: gestión de recursos humanos- legal, control y cumplimiento – soporte contable – soporte tecnológico y atención al usuario
- Visita a los proveedores con subcontratación significativa.
- 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 por las metodologías de talleres de autoevaluación de riesgos y controles, Indicadores claves de riesgo y mantenimiento y recolección de eventos de pérdida.

2. TALLER DE AUTOEVALUACION DE RIESGOS Y CONTROLES

A la fecha se viene ejecutando Taller de Autoevaluación de Riesgos y controles (RCSA) del proceso de Atención al Usuario; En la cual, nos encontramos en la segunda fase de la metodología "Identificación de riesgos y controles" en donde se identifican los riesgos internos y externos registrados en el Mapa de proceso a fin de evaluarlos y posteriormente establecer planes de acción para la mitigación del mismo.

Cuadro 1 – Diagrama de Bloques del Proceso: Atención al Usuario



3. SUBCONTRATACION SIGNIFICATIVA

Según Resolución SBS N° 2116–2009- Reglamento para la Gestión del Riesgo Operacional, indica que con el fin de gestionar los riesgos operacionales asociados a la subcontratación, las empresas deberán establecer política y procedimientos apropiados para evaluar, administrar y monitorear los procesos subcontratados. Dichas políticas y procedimientos deberán considerar:

- El proceso de selección del proveedor del servicio.
- La elaboración del acuerdo de subcontratación.
- La gestión y monitoreo de los riesgos asociados con el acuerdo de subcontratación.
- La implementación de un entorno de control efectivo.
- Establecimiento de los Planes de Continuidad.

Los acuerdos de subcontratación deberán formalizarse mediante contratos firmados, los cuales deben incluir acuerdos de niveles de servicio, y definir claramente las responsabilidades del proveedor de la Empresa.

En el ejercicio 2013 se identificó 04 empresas proveedoras calificadas con subcontratación significativa, para ello se utilizó las siguientes herramientas de validación:

- ✓ **Cuestionario de Autoevaluación de Servicio Significativos Subcontratados**
- ✓ **Visita de Inspección**

Se realizaron coordinaciones con los proveedores para efectuar la visita a sus instalaciones a fin de validar las respuestas del cuestionario y determinar el nivel de riesgo de dichas empresas.

4. SISTEMA DE INCENTIVOS

4.1. RESUMEN Y OBJETIVOS (IV TRIMESTRE 2013)

Con el objetivo de crear una cultura de gestión integral de riesgos en Credinka, la Gerencia de Riesgos ha diseñado un sistema de incentivos, no económicos, para los Oficiales y Coordinadores de la Gestión Integral de Riesgos (OGIR y CGIR) dentro de la cual se evalúa: 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 puede obtener una calificación cuantitativa respecto al desempeño de los OGIR y CGIR en la gestión de riesgo operacional.

4.2. CUMPLIMIENTO DE REPORTERÍA – EVENTOS

- ✓ Durante el IV Trimestre 2013 la unidad de riesgo operacional intensificó el seguimiento y control de los reportes de evento de pérdida teniendo como resultado un incremento progresivo en el cumplimiento de la reportería.

- ✓ En el presente trimestre, en base a la información que se recabó para el sistema de incentivos, se determinó que el 100% de los OGIR y CGIR cumplieron con reportar los indicadores clave de riesgo según el cronograma del presente año.

5. METODOLOGÍA DE INDICADORES CLAVE DE RIESGOS – KRI

5.1. RESUMEN DE SITUACIÓN Y OBJETIVOS

Con la finalidad de gestionar adecuadamente los Indicadores Clave de Riesgo (KRI's) y realizar un adecuado análisis, la Unidad de Riesgo Operacional durante el trimestre de Octubre – Diciembre del 2013, con el apoyo de los Oficiales de la Gestión Integral de Riesgo (OGIR) y los Coordinadores de la Gestión Integral de Riesgos (CGIR), se ha recibido la información necesaria de los indicadores para su cálculo y posterior análisis.

6. MONITOREO Y CUMPLIMIENTO DE PLANES DE ACCIÓN

6.1. RESUMEN DE SITUACIÓN Y OBJETIVOS

Se realizó monitoreo de los planes de acción establecidos por los usuarios hasta su implementación. Esto permite asegurar que dichas acciones se hayan implementado en la fecha pactada con cada uno de las unidades responsables para poder disminuir riesgos que se pueden presentar en la gestión y las operaciones del día a día.

6.2. MONITOREO DE LOS PLANES DE ACCIÓN

El monitoreo de los planes de acción se realiza mensualmente diseñando los planes de acción con los involucrados pactando una fecha límite para la su implementación mediante correo electrónico con copia a cada una de sus gerencias correspondientes. Una vez pactada la fecha, se da inicio al monitoreo solicitando información hasta el último día de cada mes con el estado en que se encuentran dichos planes de acción pendientes de implementación. Por último, se prosigue con el ingreso de dichos estados a una matriz diseñada por la unidad ROP.

6.3. MATRIZ DE SEGUIMIENTO DE LOS PLANES DE ACCIÓN

La matriz de seguimiento de los planes de acción tiene como finalidad integrar a las tres metodologías siendo éstos; Talleres de autoevaluación y controles (RCSA), Indicadores clave de riesgo (KRI) y Mantenimiento y recolección de eventos de pérdida (EP).

GESTIÓN DE CONTINUIDAD DEL NEGOCIO

7. SÍNTESIS

7.1. RESUMEN SITUACIÓN

La gestión de continuidad del negocio de CREDINKA se encuentra alineada con las buenas prácticas internacionales BS-25999 y las exigencias de la SBS Circular G-139-2009.

Entre las actividades más importantes realizadas en el IV Trimestre del 2013:

- ✓ 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 realizó la actualización de la normativa interna de continuidad del negocio.
- ✓ Se actualizó la relación de brigadistas de todas las agencias y oficinas de CREDINKA.
- ✓ Se planificó y realizó la prueba integral de continuidad del negocio.

7.2. 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 solicitó la participación voluntaria de los colaboradores de todas las agencias y oficinas de CREDINKA, con el objetivo de actualizar y conformar las brigadas de emergencia, obteniendo un equipo de brigadistas por oficina y/o agencia, el cual tiene la siguiente estructura:

- Brigada de Evacuación
- Brigada Contra Incendios
- Brigada de Primeros Auxilios

Cabe resaltar que la convocatoria de brigadistas de emergencia, así como la evaluación para la determinación del número de brigadistas por oficina y/o agencia, se realizó en conjunto y con el apoyo de la Unidad de Seguridad Interna.

Asimismo se recomienda que la Unidad de Gestión del Talento y Capital Humano informe a la Unidad de Riesgo Operacional (Continuidad del Negocio), cuando se presente algún cese de los colaboradores que forman parte de las brigadas de emergencia, a fin de mantener permanentemente actualizada la relación de brigadistas..

7.3. PRUEBA INTEGRAL DE CONTINUIDAD DEL NEGOCIO

Se llevó a cabo la prueba integral de continuidad del negocio, con el objetivo de probar la viabilidad y poner en práctica los planes de continuidad del negocio, así mismo, concientizar a la Alta Dirección y a los Colaboradores claves de CREDINKA para responder eficazmente ante una contingencia mayor.

✓ Escenario de la Prueba:

1. El Viernes 22 de Noviembre del 2013 a las 8:00 p.m. ocurrió un sismo de 8 grados de magnitud en escala de Richter, con una intensidad IX en escala de Mercalli, afectó la Oficina de Gestión - Lima y el Centro de Cómputo Principal , ubicados en la Av. Rivera Navarrete Nº 501, Piso 19 - Edif. Capital - San Isidro, Lima.
2. No disponibilidad total de la Oficina de Gestión y del Centro de Cómputo Principal, ubicados en la Av. Rivera Navarrete Nº 501, Piso 19 - Edificio Capital - San Isidro, Lima.
3. Falla total del servicio de proveedores críticos de comunicación (Telefónica del Perú y Americatel) en el Centro de Computo Principal.

✓ Alcance:

Desde el momento que ocurre el sismo (viernes 22/11/2013 - 8:00 p.m.) hasta el retorno a la normalidad (sábado 23/11/2013 - 02:28 a.m.) del Centro de Computo Principal, se realizaron las siguientes actividades:

1. Ejecución del Plan de Manejo de Crisis.
2. Ejecución del árbol de llamadas del Plan de Manejo de Crisis.
3. Activación de los Planes Específicos de Continuidad del Negocio.
4. Activación del Plan de Recuperación de Desastres.
5. Notificación al Equipo de Recuperación de Desastres.
6. Actividades en período de contingencia del Plan de Recuperación de Desastres.
7. Ejecución de actividades para el retorno a la normalidad del Plan de Recuperación de Desastres.
8. Notificación al Equipo de Recuperación de la Unidad de Operaciones Centrales.
9. Ejecución de actividades en período de contingencia de la Unidad de Operaciones Centrales.
10. Notificación al Equipo de Recuperación de la Unidad de Control de Préstamos y Garantías.
11. Ejecución de actividades en período de contingencia de la Unidad de Control de Préstamos y Garantías.
12. Ejecución de comunicaciones a través de mensajes de texto vía celular.

✓ **Conclusiones:**

1. El Equipo Local de Administración de Incidentes - LIMT activó con normalidad el Plan de Manejo de C
2. risis, Plan de Recuperación de Desastres y Planes Específicos de Continuidad Departamentales.
3. El Equipo de Recuperación de Desastres realizó con normalidad la activación del Centro de Cómputo Alterno – CCA desde el Centro de Reanudación de Labores – Lima, donde se realizó la correcta operatividad y funcionalidad de los servicios informáticos críticos.
4. El Equipo de Recuperación de la Unidad de Control de Préstamos y Garantías realizó con normalidad la funcionalidad de las actividades críticas del Plan Específico de Continuidad de la Unidad de Control de Préstamos y Garantías en el Centro de Reanudación de Labores – Lima, todo ello interconectado al Centro de Cómputo Alterno – CCA.
5. El Equipo de Recuperación de la Unidad de Operaciones Centrales realizó con normalidad la funcionalidad de las actividades críticas del Plan Específico de Continuidad de la Unidad de Operaciones Centrales, en el Centro de Reanudación de Labores – Lima, todo ello interconectado al Centro de Cómputo Alterno – CCA).
6. El Equipo de Recuperación de la Gerencia de Operaciones realizó con normalidad la ejecución de las transacciones programadas para la realización de la prueba de Continuidad del Negocio .
7. La Unidad de Seguridad Interna informó y coordinó anticipadamente con ASBANC, sobre la realización de la prueba, a fin de contar con presencia policial (Departamento de Seguridad de Bancos – Águilas Negras), al momento de aperturar la agencia y no generar falsas alarmas de intrusión.

GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

8. SÍNTESIS

8.1. RESUMEN SITUACIÓN

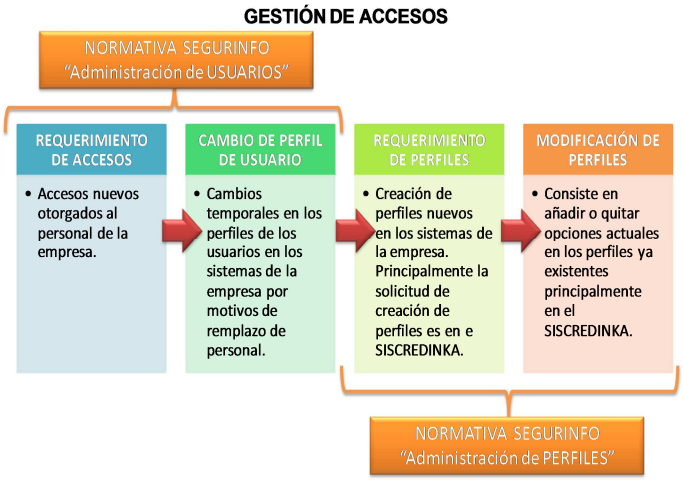
La gestión de seguridad de la información CREDINKA se encuentra alineada con las buenas prácticas a las exigencias de la SBS Circular G-140-2009, en ese sentido se cumplió con el plan operativo de la Unidad de Riesgo Operacional (seguridad de información).

Entre las actividades más importantes realizadas en el IV Trimestre del 2013:

- Seguridad lógica - Gestión de Accesos.
- Informe de prueba de restauración de copias de respaldo de los años 2009, 2010,2011 y 2012
- Gestión de incidencias de Seguridad de Información
- Capacitación virtual de Seguridad de la Información.
- Comunicados de seguridad de la información.
- Llamados de atención a usuarios por el no cumplimiento de las políticas.

9. DETALLE DEL INFORME

Cuadro 2 – Gestión de Accesos en CREDINKA



9.1. INFORME DE RESTAURACIÓN DE COPIAS DE RESPALDO AÑOS 2009,2010,2011 Y 2012

✓ Objetivo

Realizar la restauración de las copias Backup de la Base de datos del sistema principal SISCREDINKA, a fin de verificar la integridad de la información restaurada con la información que actualmente se encuentra en producción.

✓ Escenario de la prueba

Las pruebas se realizó en la Oficina Gestión Lima, se manejó un escenario en donde se perdió toda la información de la base de datos del sistema principal SISCREDINKA en el centro de procesamiento de datos principal y alterno, procediendo a realizar la restauración de la base de datos SISCREDINKA al 31 de Diciembre de los años 2009, 2010, 2011 y 2012 a partir de las cintas offsite que se encuentran resguardadas en bóveda externa.

✓ Verificación de la información restaurada

- Se verificó que la fecha de procesamiento del sistema concuerda con la base de datos restaurada correspondiente 31 de diciembre de los años 2009, 2010, 2011 y 2012.

9.2. COMUNICADOS DE SEGURIDAD DE LA INFORMACIÓN.

COMUNICADO N ° 003 -2013

El comunicado difundido en octubre del 2013 al personal de empresa tenía como finalidad concientizar a los colaboradores como evitar los virus propagados por correo electrónico o mensajes del tipo PHISHING a las cuentas individuales del personal de Credinka.