una empresa DIVISO GRUPO FINANCIERO

RESUMEN DEL INFORME DE GESTIÓN DE RIESGO OPERACIONAL

II- TRIMESTRE 2014

CREDINKA S.A.
Unidad de Riesgo Operacional

GESTIÓN DE RIESGO OPERACIONAL

1. SÍNTESIS

1.1. RESUMEN DE SITUACIÓN

En orden al cumplimiento del Plan Operativo 2014, y con la intención de promover una cultura de riegos, la Gestión de Riesgo Operacional, viene trabajando las siguientes metodologías: Mantenimiento y Recolección de Eventos de Pérdida, Indicadores Clave de Riesgo (KRI) y Autoevaluación de Riesgos y Controles (RCSA) de los procesos correspondientes a la cadena de valor de CREDINKA.:

1.2. PLAN OPERATIVO ROP II- 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.

1.3. METODOLOGIA 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 está realizando los talleres de autoevaluación de riesgos y controles (RCSA) de los procesos Hipotecario y de Fondeo e Inversiones, elaborando el diagrama de bloques; diagramas de Flujo para trasladarlos a la respectiva matriz de riesgos para su identificación.

2. METODOLOGÍA DE INDICADORES CLAVE DE RIESGOS – KRI

2.1. RESUMEN DE SITUACIÓN Y OBJETIVOS

Con la finalidad de realizar un óptimo análisis y un adecuado seguimiento a los Indicadores Clave de Riesgos (KRI), la Unidad de Riesgo Operacional ha continuado recopilando durante el II Trimestre del 2014, la información proporcionada por los OGIR´S y CGIR´S acerca de las variaciones de los indicadores de sus respectivas unidades. De la información obtenida, se realiza el cálculo correspondiente de cada indicador para, posteriormente, tomar acción sobre aquellas variaciones o señales de alerta significativas que se puedan evidenciar.

3. METODOLOGÍA DE MANTENIMIENTO Y RECOLECCIÓN DE EVENTOS DE PÉRDIDA

3.1 RESUMEN DE SITUACIÓN Y OBJETIVOS

Como parte de la adecuada administración de los eventos de pérdida por riesgo operacional de Credinka, la Unidad de Riesgo Operacional ha continuado recibiendo, de los Oficiales y Coordinadores de la Gestión Integral de Riesgos, los reportes de eventos de pérdida durante el II trimestre del 2014.

a) Plataforma Virtual de Reportería de Eventos de Riesgo Operacional

La Unidad de Riesgo Operacional ha desarrollado una nueva plataforma virtual de Reportería de Eventos de Riesgo Operacional ,con el objetivo de brindar una mayor agilidad, orden e integridad de la información recolectada. Es importante mencionar que esta nueva plataforma no solo tiene el propósito de brindar mayor facilidad en cuanto a la Gestión Integral de Riesgos, sino también el de brindar mayor facilidad a los OGIR´S y CGIR´S, ya que les permitirá emitir sus reportes de eventos de pérdida de forma más estandarizada y ordenada, logrando así la motivación por el cumplimiento constante de esta reportería. Por ello, se ha difundido a todos los Oficiales y Coordinadores de la Gestión Integral de Riesgos los nuevos lineamientos que se deberán seguir para el éxito de esta innovadora reportería virtual.

b) ***Reporting ejecutivo***

Como parte de la gestión de Riesgo Operacional, la Unidad ROP tiene la responsabilidad de diseñar, difundir e implementar las metodologías para identificar, evaluar, medir y controlar el riesgo operacional a través de la recolección de datos de eventos de pérdida, autoevaluación de riesgos y controles de los procesos e indicadores clave de riesgo.

De esta manera, con el objetivo de continuar con las Buenas Prácticas para la Gestión y Supervisión de Riesgo Operacional, la Unidad ROP ha desarrollado un Reporting Ejecutivo, en el cual las Gerencias, OGIR´S y CGIR´S podrán tener conocimiento de la evolución, seguimiento y calificación de su desempeño, de esta

manera lograr una cultura organizativa que conceda gran prioridad a la gestión eficaz del riesgo operativo y al cumplimiento de estrictos controles operativos.

4. SISTEMA DE INCENTIVOS

4.1. RESUMEN DE SITUACIÓN Y OBJETIVOS

Durante este periodo Abril – Junio 2014, se puede afirmar que se está logrando consolidar el compromiso en cuanto al cumplimiento de la gestión de riesgo operacional en Credinka, y este se ve reflejado a través de los resultados del sistema de incentivos que realiza la Unidad de Riesgo Operacional.

4.2. CUMPLIMIENTO DE REPORTERÍA DE EVENTOS DE PÉRDIDA

Al término del II Trimestre del 2014, se puede apreciar la continuidad y constancia en cuanto al compromiso de reportar los eventos de pérdida identificados en cada una de las Gerencias, esta constancia se ve reflejada en el **99%** de cumplimiento de Reportería de Eventos de Pérdida, respecto al 93% que se había logrado el primer trimestre del 2014.

- ✓ Con el objetivo de que los OGIR´S y CGIR´S se familiaricen con la nueva Plataforma de Reportería de Eventos de Riesgo Operacional, en el mes de Junio del 2014, se difundió los nuevos lineamientos para la Reportería de Eventos de Pérdida, de tal manera que desde este mes se dé inicio a la utilización del mismo. Siendo esta plataforma totalmente nueva e innovadora, la Reportería de Eventos de Pérdida correspondiente al mes de Junio 2014 logró el 100% en cuanto al cumplimiento.

4.3. CUMPLIMIENTO DE REPORTERÍA DE INDICADORES CLAVE DE RIESGO - KRI

Para este segundo trimestre, en base a la información que se recabó para el análisis de los Indicadores Clave de Riesgos (KRI), se determinó que el 100% de los OGIR y CGIR cumplieron con reportar lo requerido según el cronograma de reportería del presente año.

4.4. ACTUALIZACIÓN DE LA NORMATIVA INTERNA.

Durante el II trimestre del 2014 se actualizó las normativas internas de la unidad.

- ✓ Guía Metodológica de Incentivos en la Gestión de Riesgo Operacional

GESTIÓN DE CONTINUIDAD DEL NEGOCIO

5. SÍNTESIS

5.1. RESUMEN SITUACIÓN

La gestión de la 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 II trimestre del período 2014 correspondiente a la Unidad de Riesgo Operacional (Continuidad del Negocio).

5.2. PARTICIPACIÓN EN EL SIMULACRO NACIONAL DE SISMO

CREDINKA participó en el Simulacro Nacional de Sismo y Tsunami, realizado el viernes 30 de Mayo a las 3:00 p.m., el cual simuló un temblor de 8 grados de magnitud en escala de Richter.

Se elaboró el informe de Simulacro de Sismo para hacer de conocimiento la participación de CREDINKA en el ejercicio, así como la puesta en práctica del Plan de Emergencia y Evacuación.

5.3. ACTUALIZACIÓN DE TARJETA DE CONTACTO DEL EQUIPO LOCAL DE ADMINISTRACIÓN DE INCIDENTES - LIMT

Se actualizó los miembros titulares y suplentes del Equipo Local de Administración de Incidentes – LIMT, en vista de los recientes cambios en su conformación, así como los datos de los contactos de emergencias, a fin de tener una óptima comunicación en caso de producirse una crisis que podría afectar las operaciones de CREDINKA.

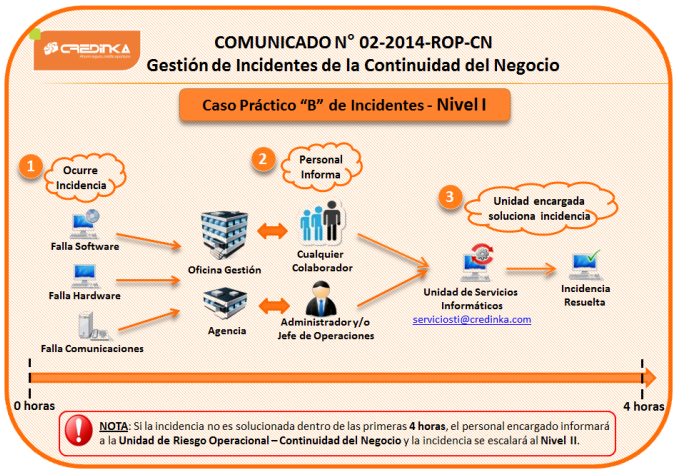
5.4. ACTUALIZACIÓN DE LA NORMATIVA INTERNA DE CONTINUIDAD DEL NEGOCIO

Durante el 2do 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.

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

5.5. COMUNICADOS DE CONTINUIDAD DEL NEGOCIO

Para una eficiente gestión de incidentes de continuidad del negocio, se elaboró y difundió comunicados a todo el personal CREDINKA, donde se muestra de forma clara y sencilla la aplicabilidad del árbol de llamadas ante una contingencia.



GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

6. SÍNTESIS

6.1. ACTUALIZACION DEL PROCEDIMIENTO DE GESTION DE ACCESOS Y PERFILES

Se actualizó el procedimiento de Gestión de Perfiles y Accesos.

El objetivo del procedimiento es establecer una correcta administración de los accesos que se brindan a los usuarios, que deberán ser asignados de acuerdo a las funciones y responsabilidades del colaborador; así como de controlar los accesos de los usuarios a los sistemas informáticos que administra CREDINKA, a fin de salvaguardar la información contenida en los mismos.

En el procedimiento se han establecido tres sub procesos principales, los cuales mencionamos a continuación:

- ❖ Creación y Mantenimiento de Perfil de Accesos
- ❖ Requerimiento y Validación de Perfiles y Accesos
- ❖ Control y Monitoreo de Perfiles y Accesos

Las cuales entrará en vigencia a partir del 31 de Julio del 2014

6.2. GESTIÓN DEL CONTROL DE ACCESOS

6.2.1. 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.

Las inconsistencias encontradas en los reportes generados por la Unidad de Base de Datos y procesamiento; El oficial de seguridad de la Información solicita a la Unidad de Servicios Informáticos realizar las correcciones a los accesos observados.

6.3. INVENTARIO DE ACTIVOS DE INFORMACIÓN

Para la actualización del inventario de activos de información se coordinó con las gerencias un cronograma de visitas tanto para Gestión Cusco y Gestión Lima.

El registro del inventario de activos de información se clasifican como, Restringido, Confidencial, Uso interno y Público.

6.4. REVISIÓN DEL MANTENIMIENTO PREVENTIVO DE EQUIPOS DEL CENTRO DE CÓMPUTO ALTERNO

Se verificó el mantenimiento preventivo del Centro de Computo Alterno(CCA), el sistema de protección eléctrica, el sistema de climatización y el sistema de seguridad.

6.5. INFORME DE REVISION DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Se verificó los controles de seguridad referente a la separación de los ambientes de desarrollo, prueba y producción, al monitoreo del servicio dado por terceras partes, administración de la capacidad de procesamiento, seguridad de las redes, mantenimiento de registros de auditoría y monitoreo de los sistemas.

6.6. INFORME REVISIÓN DE EQUIPOS DE COMPUTO

Se revisó una muestra de los equipos de computo, respecto a la protección contra el software de dudosa procedencia, la seguridad sobre los medios de almacenamiento y la seguridad sobre el intercambio de información.

6.7. COMUNICADOS DE SEGURIDAD DE LA INFORMACIÓN

El comunicado al personal de empresa tiene como finalidad concientizar a los colaboradores sobre las "Buenas practicas de Seguridad de la Información".