RESUMEN TRIMESTRAL DE GESTIÓN DE RIESGO OPERACIONAL

DICIEMBRE DEL 2012

CREDINKA S.A.
Unidad de Riesgos

CAPITULO I GESTIÓN DEL RIESGO OPERACIONAL

La División 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.

RESUMEN DE LA GESTIÓN DE RIESGO OPERACIONAL

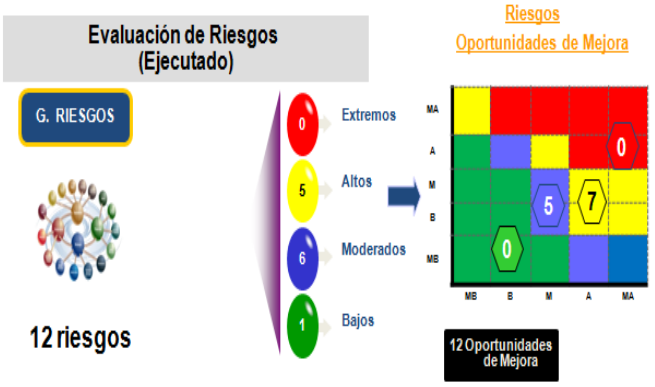
1. SÍNTESIS

1.1. TALLER RCSA DE PROCESO GESTION DE RIESGOS

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 presente Trimestre se ha culminado con los Talleres de Autoevaluación de Riesgos y controles (RCSA) al proceso de la Gestión de Riesgos.

Cuadro 1 – Mapa de Riesgo Residual- Oportunidad de Mejora



1.2. PLANES DE ACCIÓN PARA EL PROCESO DE GESTION DE RIESGOS

El en taller de RCSA para el proceso Gestión de Riesgos se determinó 12 oportunidades de mejora y 07 planes de acción a fin de mitigar sus riesgos.

2. NUEVOS PRODUCTOS O CAMBIOS IMPORTANTES

2.1. INFORME DE RIESGOS POR NUEVOS PRODUCTOS UNIVERSIDAD ANDINA DEL CUSCO.

CREDINKA viene gestionando con la Universidad Andina del Cusco un convenio de recaudación cuyo objeto tiene la finalidad de efectuar la cobranza de matriculas, pensiones de enseñanza y demás pagos diversos que efectúen los alumnos y usuarios en general dentro de las agencias de CREDINKA, en tal sentido la División de Riesgo Operacional realizó un análisis de riesgo sobre este nuevo servicio.

3. CONTRATACION SIGNIFICATIVA.

3.1. INFORME DE EVALUACION DE SUBCONTRATACION SIGNIFICATIVA

La División de Riesgo Operacional elaboró los informes de las visitas a 06 empresas proveedoras de servicios cuyo scoring las clasificó como significativas.

4. METODOLOGÍA DE INDICADORES CLAVE DE RIESGOS – KRI

Un Indicador Clave de Riesgo o Key Risk Indicador, por sus siglas anglosajonas (KRI), son variables que ofrecen una base razonable para estimar la probabilidad y severidad de uno o más eventos de riesgo operacional

A continuación se presenta un detalle de los KRI´s por categorías.

Categorías	Número de KRI´s
ATENCION AL USUARIO	6
RECURSOS HUMANOS	5
OPERACIONES CON TARJETA DE DÉBITO	7
COLOCACIONES	4
REGULATORIO	8
PASIVOS	3
SEGURIDAD	1
CONTRATOS Y SLA´s	3
CONTABILIDAD	3
TESORERIA	2

CAPITULO II GESTIÓN DE CONTINUIDAD DEL NEGOCIO

La Gestión de la Continuidad del Negocio es un conjunto de acciones orientadas a planificar, organizar y mejorar la capacidad de repuesta de la organización frente a los probables efectos de eventos adversos que por fallas técnicas, humanas o/ y desastres naturales y que interfieren en la operativa de los procesos de la organización, a partir de este plan se busca un rápido retorno a la normalidad ante cualquier advenimiento de una catástrofe, minimizando el impacto que pudiese ocasionar dicho evento en el giro del negocio.

GESTIÓN DE CONTINUIDAD DEL NEGOCIO

5. ACTIVACIÓN DE LOS PLANES ESPECÍFICOS DE CONTINUIDAD

Durante el año 2012 se activaron en diversas oportunidades los planes específicos de continuidad del negocio en distintas agencias de CREDINKA.

5.1.1. ANÁLISIS DE IMPACTO AL NEGOCIO - BIA

Se identificaron 212 actividades en todos los Departamentos y Unidades de CREDINKA;. de acuerdo con nuestra metodología del BIA, se realiza el Análisis de Riesgo y las estrategias para mitigar las posibles amenazas de las actividades que más exponen a CREDINKA

5.1.2. REALIZACIÓN DEL INFORME DE RIESGOS POR CAMBIOS IMPORTANTES EN EL AMBIENTE INFORMATICO

El Directorio de CREDINKA tomó la decisión de trasladar toda la oficina de Gestión Lima ubicada en el piso 14 del edificio Capital al piso 19, con el fin de centralizar todas sus oficinas de gestión y disponer de un mejor ambiente de trabajo, para llevar a cabo CREDINKA activó su centro de cómputo alterno ubicado en el departamento del Cusco, a fin de garantizar la continuidad en la funcionalidad y operatividad a largo del traslado.

La división de Riesgo Operacional comunicó a la SBS, con las siguientes cartas:

- CARTA N° 179-2012-GG/CREDINKA S.A. “Fecha Recepción SBS: 03/12/2012”
- CARTA N° 144-2012-GG/CREDINKA S.A. “Fecha Recepción SBS: 30/10/2012”

5.1.3. PRUEBA INTEGRAL DE CONTINUIDAD DEL NEGOCIO

CREDINKA realizó por primera vez la prueba integral de continuidad del negocio, involucrando la participación de sus principales Gerentes y Directorio, dicha prueba tuvo un escenario de un sismo igual o superior a grado IX de Mercalli o 8 de Richter, la cual afectó la Oficina de Gestión - Lima y el Centro de Cómputo Principal, la duración de la prueba fue aproximadamente de 06 horas y se realizó en el Centro de reanudaciones de labores ubicado en el centro de Lima, activando el Centro de Computo Alterno donde se verificó la correcta operatividad y funcionalidad de los servicios informáticos.

CAPITULO III GESTIÓN DE SEGURIDAD DE LA INFORMACION

La Seguridad de la Información consiste en la adecuada combinación de tecnología y política empresarial, tendiente a la protección de los recursos de información de un conjunto de amenazas entre las que se encuentran el daño, la alteración, el robo y la pérdida. No significa solo tratar con recursos y procesos informáticos, sino de la adecuada integración de personas, procesos y tecnología.

La gestión efectiva de la seguridad de la información es una responsabilidad compartida por todos los miembros de CREDINKA: los directivos, los administradores de los sistemas de información y los usuarios.

GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

6. SÍNTESIS

En el presente trimestre se ha continuado con la Implementación del Sistema de Gestión de Seguridad de la Información en CREDINKA.

Las políticas y procedimientos de Administración de Usuarios y Perfiles aprobadas en directorio de 2011 fueron implementadas a lo largo de todo el año 2012.

Teniendo como resultados la implementación de:

- ✓ Seguridad lógica - Gestión de Accesos.
- ✓ Aprobación de Política de Seguridad Lógica y la Política de Gestión de Incidentes.
- ✓ Visita de Inspección.
- ✓ Concurso SEGURINFO.
- ✓ Capacitación en seguridad de la información.
- ✓ Comunicados de seguridad de la información.

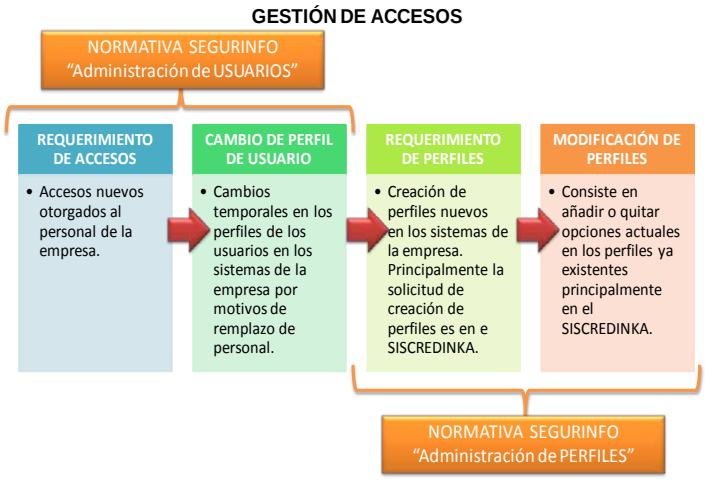
7. DETALLE DEL INFORME

7.1. 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 e 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



7.2. BÓVEDA DE COPIAS DE RESPALDO (BACKUP)

Se ha Implementado un ambiente para la bóveda de backup en el centro de Lima; a fin de resguardar todas las cintas y CD´S de las copias de respaldo de CREDINKA., implementando un control de acceso triangular.