RESUMEN DE LA GESTIÓN DE RIESGO OPERACIONAL

III TRIMESTRE 2016

FINANCIERA CREDINKA S.A.

I. GESTIÓN DEL RIESGO OPERACIONAL

La Gestión de Riesgo Operacional de Financiera Credinka ha venido aplicando las exigencias de la Superintendencia de Banca, Seguros y AFP's en su Resolución SBS N° 2116 - 2009, a fin de continuar con el buen Gobierno Corporativo que caracteriza a las empresas del Grupo Diviso.

Indicadores Clave de Riesgos – KRI

Los indicadores clave de riesgo son variables que ofrecen una base razonable para estimar la probabilidad e impacto de uno o más eventos de riesgo operacional, así también, es una herramienta que permite la validación, cálculo y monitoreo de los indicadores clave de riesgo, para todos los procesos clave de los Departamentos de apoyo o Soporte y Negocios.

Mantenimiento y Recolección de Eventos de Pérdida

Con el objetivo de crear un marco de gestión permanente que permita controlar el Riesgo Operacional mediante el desarrollo e implementación de una metodología que permita identificar, medir, valorar y mitigar los riesgos operacionales que afecten a Financiera Credinka, las distintas unidades orgánicas son responsables de identificar y reportar al Departamento de Riesgo Operacional las pérdidas operacionales que se produzcan, asegurando así la integridad de la información presentada para analizar las causas que generaron las mismas y así determinar medidas preventivas y correctivas necesarias. Por tanto, constantemente el Departamento de Riesgo Operacional captura los casos presentados, a fin de evaluar las causas que los originan y plantear acciones que permitan evitar situaciones similares.

Sistema de incentivos: oportunidad y consistencia de la información recolectada

Con la finalidad de establecer incentivos de reconocimiento a los Oficiales y Coordinadores de la Gestión Integral de Riesgos de las Divisiones / Departamentos que hayan destacado en la Gestión de Riesgo Operacional, tal cual lo indica los reglamentos internos y de la SBS, el Departamento de Riesgo Operacional evalúa el desempeño de los mismos mediante un sistema de incentivos no monetarios.

Requerimiento de Capital por Riesgo Operacional

Actualmente Financiera CREDINKA utiliza el método del indicador básico para el cálculo del requerimiento patrimonial por riesgo operacional el que es equivalente al promedio de los saldos anualizados de los márgenes operacionales brutos de la empresa considerando los 3 últimos años, multiplicado por un factor fijo (15%).

Capacitación Gestión de Riesgo Operacional: División de Contabilidad

Como parte del entrenamiento y concientización al personal de CREDINKA sobre la gestión de Riesgo Operacional, se capacitó en temas puntuales como tipologías de impacto del evento por Riesgo Operacional, ciclo de vida de un evento, registros contables y casuísticas de eventos de pérdida por Riesgo Operacional.

II. CONTINUIDAD DEL NEGOCIO

Pruebas específicas de Continuidad del Negocio en Agencias.

Se realizaron pruebas de continuidad del negocio en agencias, esto con el fin de poner en práctica los Planes de Continuidad del Negocio existentes y probar su viabilidad. Así mismo, se buscó concientizar a los colaboradores de CREDINKA sobre cómo responder eficazmente ante la ocurrencia de una incidencia que afecte la operatividad de las agencias.

Normativas de Continuidad del Negocio

En el III Trimestre del 2016 se procedió con la actualización y elaboración de guías metodológicas que apoyan la gestión de continuidad del negocio.

Indicadores clave de la gestión de Continuidad del Negocio

De acuerdo a lo dispuesto por la Circular SBS G-180-2015, a través del aplicativo SUCAVE se cumplió con el envío por SUCAVE a la SBS de los Reportes RO-1, RO-2, RO-3, y RO-4 relacionados a los indicadores clave de riesgo de la gestión de la continuidad del negocio.

III. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La creciente dependencia y los sistemas que procesan información, junto con los riesgos, beneficios y oportunidades que esos recursos representan, han transformado a la gestión de la seguridad de la información en una función vital en todo ámbito. En especial si se tiene en cuenta que las tecnologías de la información mejoran sensiblemente las posibilidades de negocio, con lo cual su seguridad añade un valor significativo al momento de minimizar riesgos y, así mismo, disminuir pérdidas derivadas de eventos relacionados a la seguridad.

1. Buenas prácticas de Seguridad de la Información

1.1. Boletín Informativo

Con el fin de difundir a todos los colaboradores de Credinka las buenas prácticas en Seguridad de la Información, se elaboró el Comunicado informativo (N° 03-2016) el cual trata del buen uso del correo electrónico.

2. Prueba de Restauración de Copias de Respaldo

Se realizó exitosamente la prueba de restauración de copias de respaldo, manejando un escenario en donde se perdió toda la información de base de datos del sistema principal y alterno, procediendo a realizar la restauración de la base de datos a partir de las cintas offsite que se encuentran resguardadas.

3. Revisión de Equipos de Cómputo

	Agencias
Tacna	Tacna I
	Tacna II
Cusco	Gestion
	San Sebastian
	El Sol
	San Jeronimo
	Sicuani
	Urcos
	Quillabamba
	Magisterio
	Tica Tica
	Anta
Arequipa	Camana
	Cayma
	Pampilla
	Pedregal
	Paucarpata
	La Negrita
	Rio Seco
	San Camilo
	La Joya

Con el fin de revisar los controles de Seguridad de Información en Financiera CREDINKA, se ha realizado una inspección de una muestra de 112 equipos de cómputo de los trabajadores de las siguientes agencias:

Para esta revisión se tomó como referencia los controles de seguridad de la información que se hace referencia en la Circular de la SBS N° G-140-2009 “Gestión de Seguridad de la información”