RESUMEN DE LA GESTIÓN DE RIESGO OPERACIONAL

II 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.

A continuación se muestra el resultado de la Gestión de Riesgo Operacional en el II Trimestre del 2016:

- Se recopiló la información de Indicadores Claves de Riesgo, a través de los reportes que hicieron llegar los Coordinadores de Gestión Integral de Riesgos, dicha información ha permitido concluir que es necesario rediñerar los KRI's.
- Se identificó y registro los eventos de pérdida presentados en el segundo trimestre.
- Se evaluó el desempeño de los Oficiales de Gestión Integral de Riesgos, a través de la oportunidad y consistencia de la información reportada por los Coordinadores de Gestión Integral de Riesgos a su cargo.

Indicadores Clave de Riesgos – KRI

Los Indicadores de Riesgo – KRI, ayudan a detectar señales tempranas sobre la exposición creciente de los riesgos a los que están expuestas las diversas áreas de negocios, de manera que alerten sobre esta situación y puedan adoptarse las medidas correctivas que resulten pertinentes, antes de que los efectos negativos se hayan materializado sobre los objetivos.

Mantenimiento y Recolección de Eventos de Pérdida

Con el propósito de establecer la línea metodológica de la gestión de Riesgo Operacional, mediante la identificación, evaluación, seguimiento, control y mitigación de riesgos que conlleva la Financiera CREDINKA, los distintos Departamentos son responsables de identificar y reportar al Departamento de Riesgo Operacional las pérdidas operacionales que se produzcan, a fin de continuar con las buenas prácticas para la gestión y supervisión de los Riesgos Operacionales.

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%).

II. CONTINUIDAD DEL NEGOCIO

Capacitación a CRAC Cajamarca sobre la gestión de continuidad del negocio en relación a la fusión con Financiera CREDINKA

Durante el pasado mes de mayo, la Unidad de Continuidad del Negocio de Financiera Credinka procedió a realizar una capacitación al personal de las áreas administrativas y agencias de CRAC Cajamarca a fin de informarles sobre la forma de gestión que se viene trabajando en Financiera Credinka respecto a "Continuidad del Negocio", esto en relación con el proceso de fusión que se viene llevando a cabo entre las dos empresas anteriormente citadas.

Prueba al Plan de Emergencia y Evacuación: Participación en el Simulacro Nacional de Sismo

El jueves 16 de Junio a las 4:00 p.m. se realizó el Simulacro Nacional de Sismo, la Unidad de Seguridad Interna en coordinación con la Unidad de Continuidad del Negocio, se encargaron de informar, concientizar y orientar a las brigadas de emergencia y colaboradores en general sobre el desarrollo del simulacro de sismo, el cual se llevó a cabo a nivel nacional con la participación de todas las agencias y oficinas de gestión.

Los resultados de la prueba fueron satisfactorios.

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 relacionados a los indicadores clave de riesgo de la gestión de la continuidad del negocio.

Se cumplió con remitir la información de los reportes RO1 y RO2 dentro de la primera quincena de abril del 2016, los mencionados reportes corresponden a información de sucesos ocurridos en los meses de enero, febrero y marzo 2016, la periodicidad de estos reportes es trimestral.

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° 02-2016) el cual trata de las páginas web no permitidas, y uso responsable de los medios de almacenamiento (dispositivo USB, Lectora CD/DVD).

2. Registros de Pistas en Base de Datos

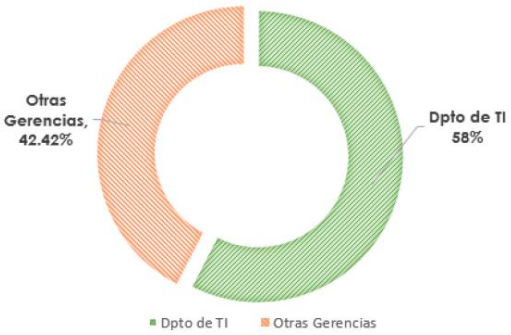
2.1. Registro de Transacciones en la Base de Datos de Credinka

Las trazas proporcionadas por TI de los 23 Base de Datos ubicados en los ambientes de Producción de Credinka las cuales son cargadas en el Servidor de Riesgos, se identificó que las trazas de los días 11, 12 y 13 de Mayo no hubieron registros; la causa fue un error en el Disco por saturación, el cual almacenaba los archivos temporales en formato (.TRC)

2.2. Modificación de montos y saldos del SisCredinka y SisDebito

El 58% de las consultas realizadas en la base de datos fueron con la conformidad de la División de TI, y el 42.42% cuenta con las conformidades de otras Gerencias (Operaciones, Comercial y General).

Porcentaje de consultas con sus respectivas autorizaciones



3. Gestión de Incidencias de Seguridad de la Información

3.1. Registro de Transacciones en la Base de Datos de Credinka

Los incidencias de seguridad de la información deben ser reportadas de tal manera que permitan realizar acciones correctivas de forma oportunas. Para ello, es necesario registrar los incidentes de seguridad de la información que ocurren en nuestra empresa para poder analizar las causas que los producen, y verificar que se hayan ejecutado las actividades de respuestas que permitan solucionar las causas que originan el incidente.

Durante el II trimestre de 2016, el Dpto. de Servicios Informáticos, Dpto. de Desarrollo y Mantenimiento de Sistemas han reportado un total de 119 incidentes de seguridad de la información.

Porcentaje de incidencias de Seguridad de la Información