Financiera CREDINKA
una empresa DIVISO

RESUMEN DE LA GESTIÓN DE RIESGO OPERACIONAL

ACTIVIDADES DESTACADAS I TRIMESTRE 2018

I. GESTIÓN DEL RIESGO OPERACIONAL

En cumplimiento con las exigencias establecidas por el regulador, la Gestión de Riesgo Operacional de Financiera Credinka basa su gestión de acuerdo a los lineamientos establecidos en la Resolución SBS N° 2116 - 2009, a fin de continuar con el buen Gobierno Corporativo que caracteriza a las empresas del Grupo Diviso.

Indicadores Claves de Riesgo (KRI).

Los Indicadores clave de Riesgo, en adelante KRI, ayudan a detectar señales tempranas sobre la exposición creciente de los riesgos a los que están expuestas las diversas áreas del negocio a fin de adoptar las medidas correctivas que resulten pertinentes. Al I trimestre del mes de marzo se cuenta con 25 indicadores claves de riesgo.

Mantenimiento y Recolección de Eventos de Pérdida.

Con el objetivo de establecer un marco de gestión permanente que permita controlar la Gestión de 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 a la Unidad 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 para así plantear acciones que permitan evitar situaciones similares.
Es así que durante el primer trimestre del 2018, la Unidad de Riesgo Operacional ha registrado 79 eventos de pérdida en las cuentas contables durante el periodo Enero – Marzo 2018.

Análisis de Riesgos frente a cambios

Durante el I Trimestre se realizaron 3 evaluaciones de riesgo operacional; Sistema Topaz Risk, Apertura de cajero corresponsal y cambio del procedimiento de créditos.

Informe Anual de Gestión de Riesgo Operacional

En este I Trimestre se envió a la S.B.S. el IGROp – 2017, así mismo, se realizó el seguimiento al plan de adecuación a la resolución S.B.S 272-2017, siendo implementadas en su totalidad.

Cultura Organizacional de Riesgo Operacional

Se remitió boletines informativos sobre la Gestión de Riesgo Operacional al Personal de Credinka, así como las responsabilidades de los OGIR y CGIR. Por otro lado se realizó la capacitación y evaluación de la gestión de riesgo operacional, continuidad del negocio y Plan de continuidad en Agencias.

II. CONTINUIDAD DEL NEGOCIO

La Gestión de Continuidad de Negocio de Financiera Credinka va alineada con las buenas prácticas internacionales como la BS-25999 y las disposiciones establecidas por la Superintendencia de Banca y Seguros a través de su Circular G-139-2009.

Actualización de Normativas de Continuidad del Negocio

Se actualizaron normativas de la gestión de la continuidad del negocio debido a un cambio en el organigrama de la Financiera mediante el cual los procesos críticos "Comercialización de productos pasivos" y "Apertura de productos pasivos" pasan bajo la responsabilidad del Departamento de Gestión y Productos.

Prueba Integral de Continuidad del Negocio 2017

Se realizó la Prueba Integral de Continuidad del Negocio correspondiente al periodo 2017.

Programa de pruebas de Continuidad del Negocio 2018

Se elaboró el Programa de Pruebas de Continuidad del Negocio 2018 y la priorización de agencias y Departamentos significativos para la ejecución de visitas, pruebas, capacitaciones, entre otros, identificado un total de 25 agencias significativas disgregadas en 11 departamentos a nivel nacional.

Eventos de Interrupción de Continuidad del Negocio.

Se cumplió con la gestión de eventos de interrupción de continuidad del negocio atendiendo un total de 26 eventos de interrupción que activaron el Plan de Continuidad del Negocio, Plan de Continuidad de Agencias, y el Plan de Emergencia y Evacuación; además de cumplir con el envío de los reportes RO1-RO2 y RO3-RO4 correspondientes al IV Trimestre 2017 y II Semestre 2017 respectivamente.

III. SEGURIDAD DE LA INFORMACIÓN

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;

Gestión de Accesos

Se realizó el monitoreo de los controles de acceso a los usuarios, a fin de garantizar que los colaboradores cuenten únicamente con los accesos autorizados y que requieren para cumplir sus funciones, estableciendo diversos indicadores de cumplimiento.

Evaluación de Riesgos del Correo Electrónico.

Se realizó la evaluación del correo electrónico, el cual muestra los resultados de las vulnerabilidades tales como el acceso al correo personal gmail del colaborador desde CREDINKA y la información almacenada en el google drive pueda ser compartida con terceros.

Implementación de enmascaramiento de datos sensibles.

A fin de resguardar los datos sensibles de los clientes de CREDINKA se ha implementado el proyecto de técnicas de enmascaramiento de Datos.

Plan de activos de Información.

Se realizó el Plan de Activos de Información para los macroprocesos más críticos de CREDINKA, y las actividades iniciaran desde el mes de abril y finalizara en el mes noviembre.

Ethical Hacking.

A fin de no estar expuestos a los ataques maliciosos de terceros, se tiene 3 propuestas económicas sobre el servicio de evaluación de análisis de vulnerabilidades (Ethical Hacking).

Actualización de Normativas de seguridad de la Información.

Como parte de la mejora continua de la normativa interna de la gestión de Seguridad de la Información se elaboró el Procedimiento para la Gestión de Activos de Información y se actualizó la Política de Seguridad de la Información y la Guía Metodológica de Gestión de Riesgos y Clasificación de Activos de Información.