RESUMEN DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

II TRIMESTRE 2017

FINANCIERA CREDINKA S.A.

I. 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.

Actualización de normativas de seguridad de la Información

Como parte de la mejora continua de la normatividad interna para la gestión de Seguridad de la Información y en cumplimiento del Plan Operativo Anual para el año 2017, se ha actualizado la "Política de uso de Internet y Correo Electrónico y se ha elaborado el "Procedimiento de Gestión de Incidentes de Seguridad de la Información".

Incidencias de Seguridad de la Información

Las incidencias de Seguridad de la información deben ser reportadas de tal manera que permitan realizar las acciones correctivas de forma oportuna. En Credinka se registra los incidentes de seguridad y las soluciones respectivas. En el II trimestre se detectó un total de 76 eventos relacionadas a seguridad de la información. Cabe indicar que para los eventos clasificados como incidencias, se han implementado respuestas efectivas por la División de Tecnologías de la Información.

Indicadores de Control de Seguridad de la Información

Se verificó los indicadores de control de seguridad de la información relacionados al control de accesos, seguridad de personal, la seguridad física y ambiental, la administración de las operaciones y comunicaciones y el desarrollo y mantenimiento de sistemas informáticos teniendo resultados favorables dentro de niveles esperados, el cual nos permite garantizar confidencialidad, integridad y disponibilidad.

Pruebas de restauración de copias de respaldo

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

El proceso de restauración se realizó en tres fases:

- ✓ Fase 01: Identificación y traslado de información
- ✓ Fase 02: Preparación de la información.
- ✓ Fase 03: Restauración de base de datos.
- ✓ Fase 04: Preparación del aplicativo.
- ✓ Fase 05: Verificación de información restaurada.

Buenas Prácticas de Seguridad de la Información

Con el fin de concientizar a todos los colaboradores de Credinka acerca de las buenas prácticas en Seguridad de la Información, se realizó la difusión de una alerta y consejos de seguridad mediante la plataforma de correo Gmail.

.