7. Garantizar que somos un banco confiable y seguro

—

7.1 Enfoque de gestión

Tema material: Garantizar que somos un banco confiable y seguro	
Justificación de relevancia	Para desarrollar en óptimas condiciones nuestro trabajo en todas las áreas y superar los desafíos que nos hemos impuesto, es una condición de posibilidad contar con excelentes niveles de continuidad operacional y con los más robustos sistemas de seguridad de la información.
Cobertura	El impacto se genera en nuestros clientes de los segmentos banca corporativa, grandes empresas y banca institucional, así como en el segmento clientes personas.
Gestión asociada	Nuestra gestión se centró en gestiones que aseguran las transacciones de nuestros clientes y la continuidad operacional. Destacamos: • Plan de Ciberseguridad. • Implementación del Segundo Data Center, COQUENA.
Evaluación	Principales cifras al cierre de 2018: • Importante crecimiento de transacciones y fortalecimiento de ciberseguridad • En promedio 270 millones de transacciones al mes, crecimiento de un 37%. • Más del 60% son digitales, con un crecimiento de 55% el 2018. • Importantes inversiones en ciberseguridad y continuidad operacional

7.2 Ciberseguridad y continuidad operacional

Como parte de nuestros lineamientos estratégicos 2018-2022 para garantizar que somos un banco confiable y seguro, la inversión en ciberseguridad y continuidad operacional fue una gran prioridad durante este 2018. En específico, avanzamos en establecer un Plan Director de Ciberseguridad, incorporando iniciativas cuyo objetivo es mantener la confidencialidad, integridad y disponibilidad de la información.

En materia de continuidad operacional, seguimos trabajando en mejorar nuestros estándares de disponibilidad a través de la implementación del segundo datacenter certificado que estará implementado durante el año 2020.

Los dos grandes retos que enfrentamos son la seguridad de la información y de los datos de nuestros millones de clientes y -dado el tamaño de nuestra red y nivel de cobertura- ofrecer un excelente nivel de continuidad operativa. En los próximos años invertiremos con especial énfasis en mejorar el nivel de continuidad operativa y seguridad en la información y soporte tecnológico.

La cantidad de transacciones procesadas ha crecido con fuerza, en línea con el fortalecimiento de la inclusión financiera. En efecto, el creciente número de operaciones asociadas al avance progresivo en el número de clientes del banco ha demandado una importante ampliación en su red de atención, tanto a través de canales presenciales como automatizados.

Importante crecimiento de transacciones y fortalecimiento de ciberseguridad

- En promedio 270 millones de transacciones al mes, crecimiento de un 37%.
- Más del 60% son digitales, con un crecimiento de 55% el 2018.
- Importantes inversiones en ciberseguridad y continuidad operacional.

En 2018, las operaciones procesadas por BancoEstado promediaron cerca de 270 millones de transacciones mensuales. La masividad alcanzada por los medios de pago ha requerido potenciar la digitalización de diversos procesos y el uso de nuevas tecnologías, para así alcanzar una gestión más eficiente y con menores costos operacionales.

En este contexto, destaca la carga transaccional que sostienen canales como CajaVecina, internet y web móvil, junto a la app BancoEstado, los que en conjunto procesan cerca de 120 millones de transacciones al mes. Estos canales se han complementado por distintas aplicaciones tecnológicas que han incrementado el procesamiento de distintas operaciones de carácter financiero y administrativo a través de sus teléfonos móviles y/o computadores.

Continuidad operacional

·En BancoEstado, preocupados de contar con un servicio tecnológico seguro, robusto y disponible para sus clientes, iniciamos la implementación de su segundo data center, el cual contará con la última tecnología disponible y los más altos estándares y certificaciones a nivel internacional y que tras su puesta en marcha, mejorará la continuidad de la infraestructura tecnológica que soporta sus sistemas y servicios. Ambos datacenters contarán con la certificación Constructed Facility Tier III que otorga Uptime Institute, la cual asegura que la infraestructura está apta para prestar servicios de primera calidad y sin interrupciones ante cualquier contingencia. Adicionalmente, esta implementación significará que el banco tendrá dos datacenters autocontenidos de primer nivel, lo que implica que cada uno de ellos puede soportar la carga operacional tecnológica completa de nuestra operación. Este cambio implica también, la renovación tecnológica necesaria y ajustar los procesos de implementación de infraestructura, la cual debe ser redundante, así como también el diseño de las aplicaciones tecnológicas, las cuales deben operar en este escenario.

·Realizamos durante el año 2018 una serie de pruebas al plan de contingencia tecnológico del banco, con el propósito de robustecer dichos planes y mejorar el entrenamiento de los equipos que deben estar siempre preparados, frente a una contingencia real. El resultado de estas pruebas permiten establecer los espacios de mejora que sean necesarias implementar.

·Se hicieron pruebas a los planes de continuidad operativos durante todo el año y en toda la red de sucursales, simulando situaciones de contingencia y verificando que nuestro personal esté capacitado para enfrentar situaciones de contingencia reales.

Fortalecimiento de ciberseguridad

- En BancoEstado contamos con un Plan director de Seguridad de la Información y Ciberseguridad el cual aborda el modelo de gobierno en los aspectos estratégicos, tácticos y operacionales, y también una serie de iniciativas orientadas a mantener y proteger la confidencialidad, integridad y disponibilidad de la información. Entre ellos, destacan la identificación y protección de los activos de información críticos, renovación del plan de concienciación de ciberseguridad, el diseño de un nuevo marco normativo de seguridad, definición de lineamientos y acciones generales para reaccionar / responder frente a un ciberataque, la integración de todas las plataformas de seguridad actualmente instaladas en BancoEstado, implementación de las nuevas directrices de seguridad para el ambiente SWIFT, incorporación de soluciones para administrar cuentas con altos privilegios, soluciones avanzadas de protección para estaciones de trabajo y dispositivos, nuevos filtros de información entrante y saliente, mejoras en el acceso a la red, etc. Esta incorporación de nuevas tecnologías nos permitirán mejorar nuestros mecanismos de protección para prevenir y detectar de manera oportuna amenazas que pongan en riesgo al Banco y sus clientes, así como también de herramientas y procesos que nos permiten recuperarnos en el menor tiempo posible ante un incidente, todo esto conducido por un equipo de trabajo de primer nivel y en constante capacitación y desarrollo.
- Mejoramos nuestra organización interna, incorporando más especialistas de ciberseguridad y se fortaleció a áreas responsables en forma específica de gestionar los riesgos de ciberseguridad.
- Hemos establecido un plan de educación interna y de cara clientes, cuyo objetivo ha sido dar a conocer las nuevas amenazas emergentes para prevenir ser víctimas de estas amenazas.
- Pensando en fortalecer la seguridad de la red de cajeros automáticos, el banco está renovando el sistema operativo de su red y actualizando las versiones del software de seguridad de los cajeros. También está actualizando el protocolo de protección de los canales de comunicación y la tecnología de cifrado de la información entre el cajero automático y el data center de BancoEstado. Del mismo modo, se está estandarizando el acceso a los medios de autenticación en un bus de seguridad.
- El desarrollo de las aplicaciones móviles se ha basado en tecnologías de última generación, las cuales consideran los más altos estándares de seguridad tanto para la plataforma tecnológica como para los modelos de desarrollo de estas.