

Contexto y Estrategia de Ciberseguridad en BancoEstado

Junio 2018



BancoEstado®

CON TODOS
DE TODOS
PARA TODOS.



Agenda

1. Situación internacional de la CiberSeguridad y su influencia en la región.
2. Marco normativo de la CiberSeguridad en el país.
3. Perspectiva del posicionamiento de BancoEstado en CiberSeguridad y los desafíos que nuestra posición nos impone.

Agenda

1. Situación internacional de la CiberSeguridad y su influencia en la región.
2. Marco normativo de la CiberSeguridad en el país.
3. Dar una perspectiva del posicionamiento de BancoEstado en CiberSeguridad y los desafíos que que nuestra posición nos impone.

Antecedentes

- Las nuevas amenazas en ciberseguridad requieren; detección temprana y respuestas oportunas.
- Para lograr lo anterior, no sólo se requieren herramientas tecnológicas, sino también visión, estrategia y organización, lo cual permite hacer frente en forma recurrente a las amenazas y dinamismo del entorno.
- Lo anterior se puede visualizar con las amenazas hoy presentes en las diferentes industrias. En la financiera podemos destacar: Wannacry, Petya, Malware en discos duros, clonaciones y los constantes ataques de ingeniería social (phishing) que reciben todos los días los clientes bancarios.
- Conscientes de este escenario, como BancoEstado durante 2017 potenciamos nuestro programa de seguridad de la información acompañados por una consultora internacional, lo cual nos permitió determinar nuestro nivel de madurez y las mejores prácticas que debemos incorporar.

Algunos casos





Agenda

1. Situación internacional de la CiberSeguridad y su influencia en la región.
2. Marco normativo de la CiberSeguridad en el país.
3. Dar una perspectiva del posicionamiento de BancoEstado en CiberSeguridad y los desafíos que que nuestra posición nos impone.

La política nacional de Ciberseguridad impone desafíos a todo el país, y también a BancoEstado



BancoEstado®

CON TODOS
DE TODOS
PARA TODOS.

Tópicos:

Infraestructura de la información robusta y resiliente

El Estado velará por los derechos de las personas en el ciberespacio

Chile desarrollará una cultura de la Ciberseguridad

Establecer relaciones de cooperación y participar en foros y discusiones internacionales

Promover el desarrollo de una industria de la Ciberseguridad, que sirva a sus objetivos estratégicos

**Objetivo
principal
Política
Nacional**

Promover un
ciberespacio
libre, abierto,
seguro y
resiliente

Las normas SBIF asociadas a Ciberseguridad



Norma SBIF 1-13

Actualizada 24 de enero de 2018

Evaluación de la gestión de los bancos en la administración de sus **riesgos operacionales**



Se exige un adecuado control de Ciberseguridad en el BANCO, con estructuras e inversiones dedicadas a la mitigación de estos riesgos



Norma SBIF 20-8

Actualizada 24 de enero de 2018

Reporte inmediato de **incidentes** de ciberseguridad



Se exige reportar incidentes que afecten la seguridad de la información, continuidad del negocio o la imagen de la Institución



Norma SBIF 20-7

Actualizada 27 de diciembre de 2017

Prerrequisitos para la externalización de **servicios a terceros**



Se profundiza la responsabilidad del BANCO en que sus proveedores cuenten con lo necesario para proteger la integridad de los activos de información y la infraestructura de TI

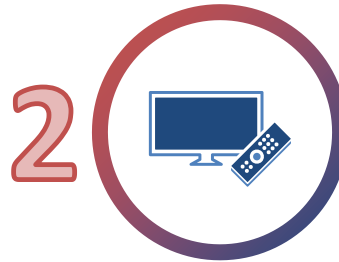
Agenda

1. Situación internacional de la CiberSeguridad y su influencia en la región.
2. Marco normativo de la CiberSeguridad en el país.
3. Dar una perspectiva del posicionamiento de BancoEstado en CiberSeguridad y los desafíos que nuestra posición nos impone.

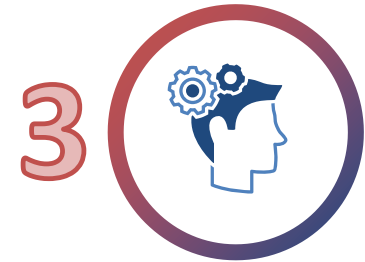
Nuestros principales desafíos



Organización



Tecnología para
nosotros y los clientes



Cultura de
Seguridad

Hemos potenciado como pilar fundamental...



1 Organización

- Contamos con instancias de gobierno de seguridad: Directorio, Comités de Riesgos, Procesos y Tecnología, Mesas Directivas.
- Contamos con protocolos de crisis y un equipo de respuesta ante incidentes de ciberseguridad (ERIC símil CSIRT).
- Contamos con un esquema de Políticas y Normas Específicas de Riesgo y Seguridad de la Información, aprobadas en el Comité de Riesgos y el Directorio.
- Utilizamos un marco metodológico para el control y gestión (ISO 27001/27002).
- Instancias de coordinación entre bancos para temas de ciberseguridad (miembro permanente del Virtual Task Force - VTF).

Hemos potenciado como pilar fundamental...



2

Tecnología para nosotros y los clientes

- Diversos mecanismos para resguardo de información sensible (2da y 3ra Clave, Chip en tarjetas, entre otros).
- Infraestructura tecnológica para la protección de activos de información críticos expuestos al ciberespacio.
- Adicional a lo anterior, contamos con Planes de Continuidad Tecnológicos (DRP) y Operacionales (BCP), para enfrentar diversos escenarios de indisponibilidad tecnológica de servicios.

Hemos potenciado como pilar fundamental...



3

Cultura de Seguridad

Clientes

- Programa de concienciación hacia los trabajadores del Banco enfocado en su interacción con clientes.
- Educación digital y de seguridad.

Personal del Banco

- Capacitaciones especializadas en Seguridad de la Información y Ciberseguridad.
- Simulaciones de ingeniería social (ej.phishing falso, USB abandonados).
- Medición nivel de adherencia cultural en ciberseguridad en BancoEstado.

En síntesis ...



... la aceleración digital que habilita la masificación y sofisticación de los clientes de la banca debe ir acompañada de un modelo de desarrollo y operación de la ciberseguridad que se esté visitando regularmente.

Esto debe ser un acto constante, nuestros clientes lo demandan, y el país lo necesita.



BancoEstado®



CON TODOS
DE TODOS
PARA TODOS.