La ciberseguridad en el sector bancario nacional

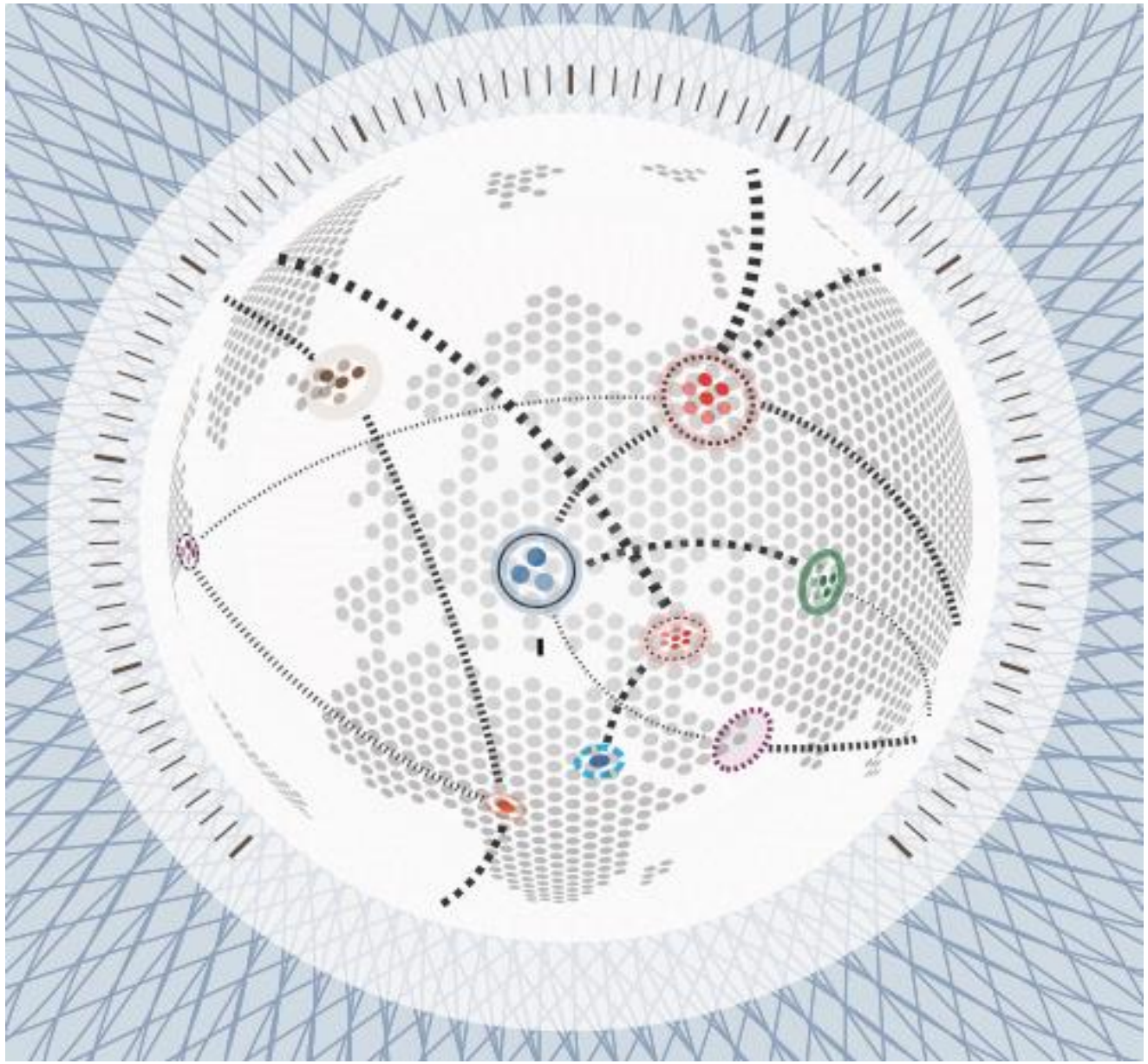
CÁMARA DE BANCOS
E INSTITUCIONES FINANCIERAS
DE COSTA RICA

Agosto, 2018

¿Qué quieren los consumidores de la banca digital?

- Un cliente o potencial cliente debe poder ser capaz de realizar cualquier operación, sea de la naturaleza que sea.
- En un tiempo mínimo, desde cualquier dispositivo.
- Debe ser sencillo y sin necesidad de presencia física en la oficina.
- Sin ningún proceso operativo de back-office que sea obligado para completar y formalizar la operación.

WORLD ECONOMIC FORUM



Cyberattacks - Data fraud or theft

TOP 5

The Global Risks

$1T

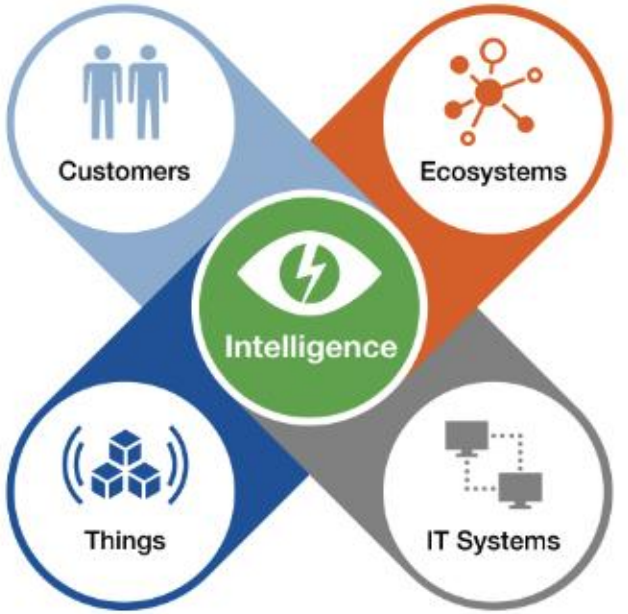
Impacto económico en el mundo

The Global Risks Report 2017

http://reports.weforum.org/global-risks-2017

WORLD ECONOMIC FORUM

Digital Business = Volume, Complexity and New Risks



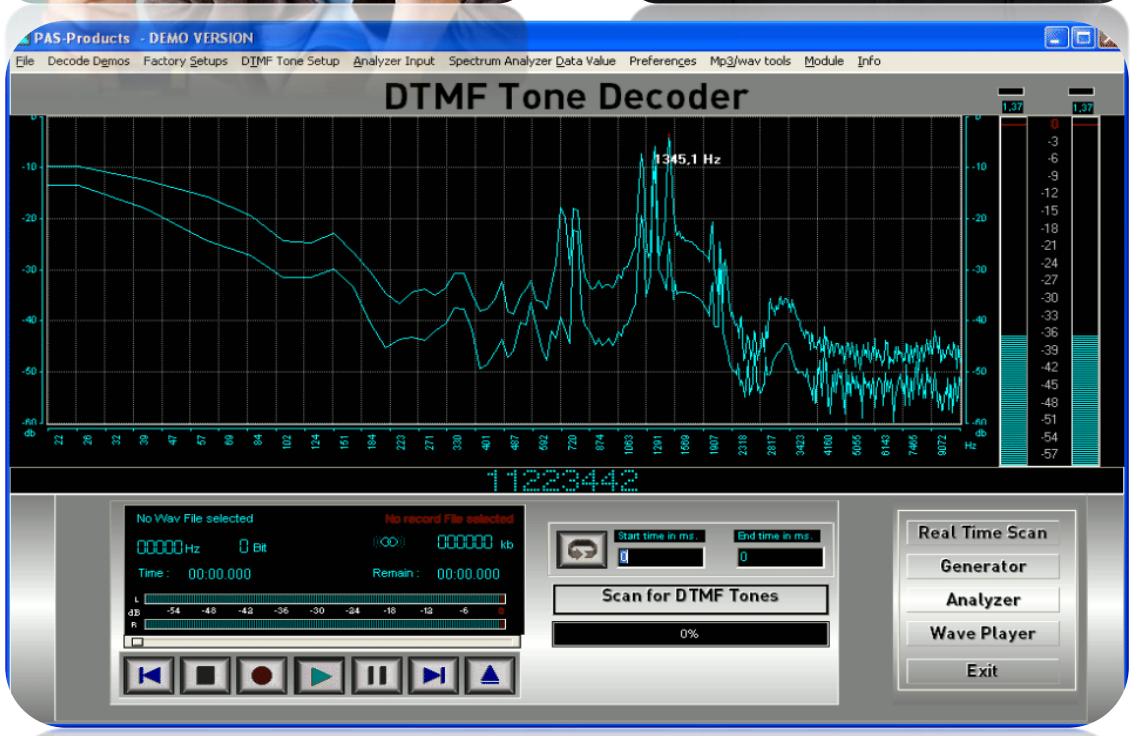
Gartner

Principales Vectores de ataques

Principales vectores de ataques

Principales vectores de ataques

- Ingeniería Social
- Obtención de información confidencial (Financiera o Personal)
- Uso de telefonía IP VoIP
- Apps para llamadas falsas



Recomendaciones de seguridad

- Nunca brinde información confidencial claves, pines, tokens, OTP
- No existan objetos extraños en el ATM
- Nunca pierda la tarjeta de vista
- Utilice tarjetas virtuales para compras o una tarjeta de $500
- Defina límites
- Revise los estados de cuenta por transacciones no autorizadas
- Firma digital
- Active las alertas por transacciones (2212-2000)

Límites de la tarjeta

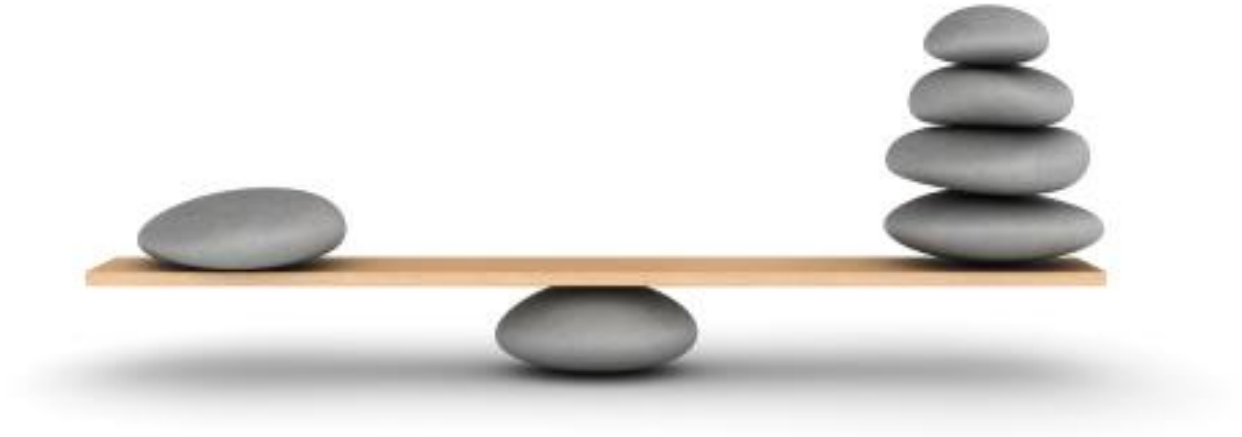
Defina un monto máximo para cada una de los siguientes servicios:

-	Límite del banco	Límite actual del cliente	Límite máximo permitido
Retiro cajeros automáticos	700,000	100,000	700,000
Transferencias cajero automático	500,000	25,000	500,000
Compra con tarjeta	2,250,000	250,000	2,250,000

¿Cuál es el riesgo apropiado?

La “protección perfecta” no existe

Alto riesgo
Bajo costo
Bajo nivel de madurez
Menos controles



Bajo Riesgo
Alto Costo
Alto nivel de madurez
Mayor controles

Modelo de Negocio

Más clientes, más canales, mayor complejidad

Nuestro objetivo es construir un programa sostenible que equilibre la necesidad de protección con las necesidades de nuestro negocio.

Evolución Bimodal

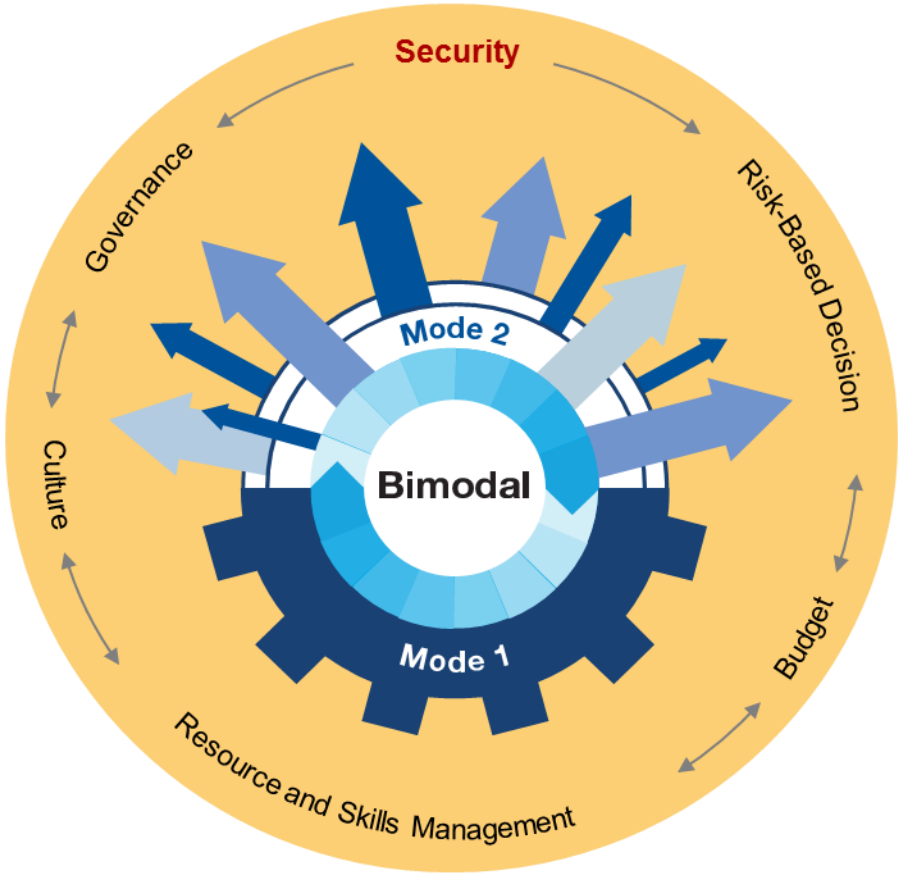
Modo 1 Proyectos grandes, en un año
Modo 2 iniciativas de corto plazo, semanas o meses

Desafío del CISO:

- Desarrollar y adaptar las prácticas de gestión de riesgos bimodal
- Mejorar la tasa de éxito del Modo 2
- Disminuir tiempo y costos

De otra manera:

- El negocio evitará el área de seguridad y riesgo
- La empresa estará expuesta a mayores riesgos



Digital business requires cybersecurity

Manage cybersecurity risk effectively — from data security solutions, cloud security and SaaS, to ecosystems and IoT.

Digital business brings new risks

Cybersecurity risks pervade every organization and aren't always under IT's direct control. Increased cyber risk is real - but so are the data security solutions. The key is to build influence across business units and ecosystems to better manage security and risk, find the right talent and ensure appropriate levels of protections.

Gartner

Áreas de acción

Postura holística
y Proactiva

Proteger información del cliente y del Banco donde esté

Asumir una brecha de Seguridad

Desarrollo de capacidades en el personal

Movilidad
Nube

Escenarios no controlados, Apps externas

Aseguramiento del software e infraestructura

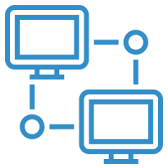
Sistemas monitoreo inteligente

Áreas de acción

Mitigar vectores y amenazas en tiempo real

Soluciones integrales, No pensar en soluciones aisladas

Desarrollar capacidades de detección y respuesta



Fintech

Análisis de datos, patrones y correlación de eventos

Muchas gracias!