RISK MANAGEMENT & COMPLIANCE

FINANCIAL SERVICES

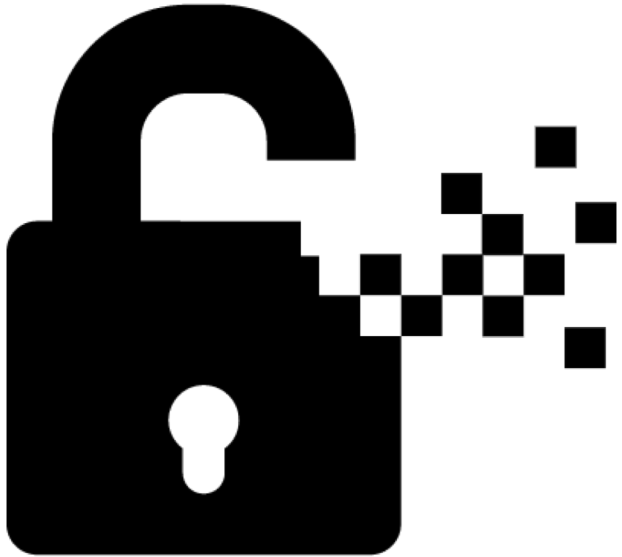
AGENDA

- Gestión del riesgo y retos del sector Enterprise Financiero
- Cumplimiento regulatorio
- Seguridad en el sector Enterprise Financiero.

HABLEMOS DE RIESGO EMPRESARIAL

INTEGRIDAD EN EL FLUJO DE LA INFORMACION

- SEGURIDAD / IT SEGURIDAD
- CYBERSECURITY
- PROTECCION DE DATOS
- RISK MANAGEMENT



RETOS DEL SECTOR FINANCIERO EN TEMAS DE SEGURIDAD

- La seguridad del sector financiero enfrenta tres retos basado en su nivel de madurez:
  1. **Cumplimiento** – Proyectos e iniciativas orientadas al cumplimiento de normas, estándares o regulaciones.
  2. **Riesgo** – Proyectos e iniciativas que ayuden a la organización a orientar los recursos a enfrentar los eventos que puedan impactar el cumplimiento de objetivos estratégicos de la organización.
  3. **Eficiencia** – Proyectos e iniciativas que ayudan a la función a ser más ágil y ligera en su operación.


FORTINET
JONES DAY
VALOR DE LA INFORMACIÓN
RIESGO EMPRESARIAL
ENFOCAR Y MONITORERAR
LOS RECURSOS EN LO MÁS IMPORTANTE.

MODELO SOLUCIONES COMO SERVICIOS

GOBIERNO, RIESGO Y CUMPLIMIENTO

Experto externo sin vicios internos corporativos permite (Persona o Empresas)

- Asignar responsabilidades puntuales y coordinar esfuerzos de acuerdo a los planes y platicas
- Comunicar e integrar la información sin concesiones.
- Publicar la Perspectiva general de los riesgos por áreas
- Identificar oportunidades locales y globales de la compañía
- Definición de mejores bases y justificaciones para toma de decisiones.

VENDER BENEFICIOS DE NEGOCIO (CORE)

POLITICA DE RIESGO EMPRESARIAL

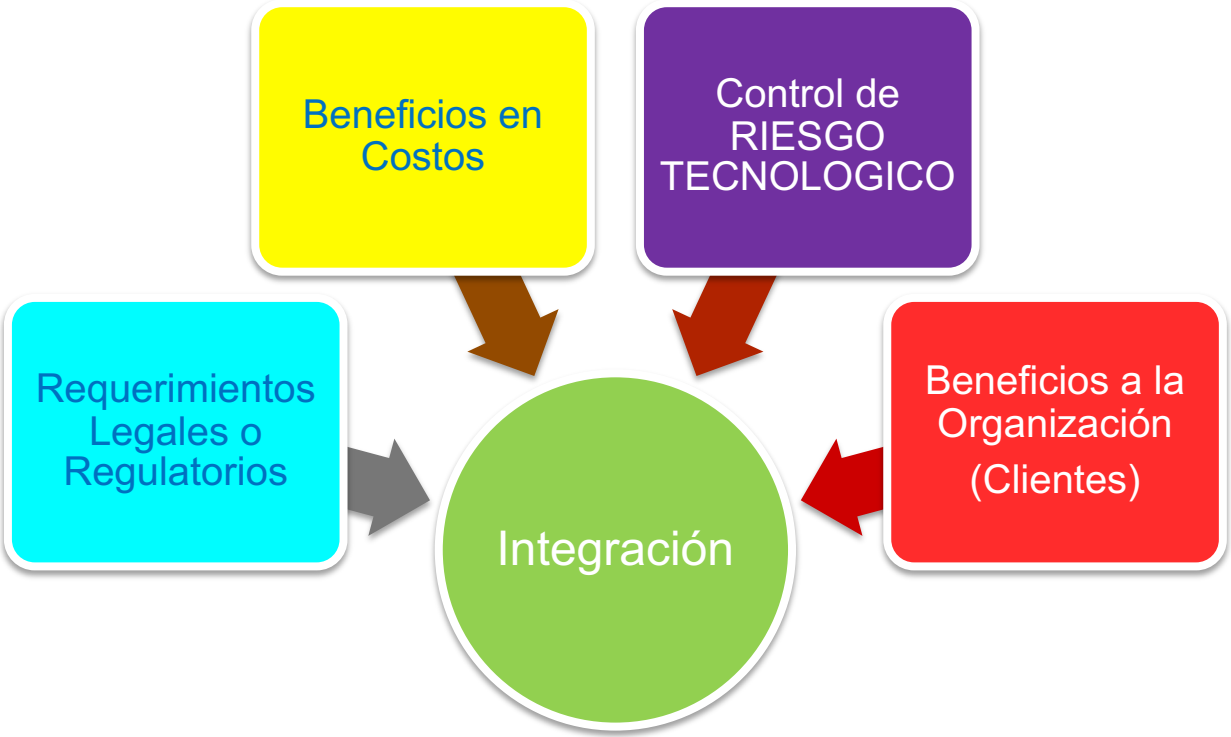
- CFO
- DIRECTOR GRAL
- CONSEJO DE AMINISTRACION
- DIRECTOR DE RIESGO EMPRESARIAL

RIESGO OPERATIVO

RIESGO TECNOLOGICO

CIO
CSO

NUESTROS DIFERENCIADORES AL NEGOCIO




FORTINET
JONES DAY
CONTROLANDO EL RIESGO
HABILITAR EL NEGOCIO PROTEGIENDO LA VENTAJA COMPETITIVA

ARQUITECTURA DE SEGURIDAD

- La función de seguridad de la información se encuentra bajo estándares a nivel global para , estandarizar y reducir costos.
- Un método para lograr estos objetivos es desarrollar e implementar una arquitectura de seguridad de la información.

ARQUITECTURA DE SEGURIDAD - VISIBILIDAD

Controles Operativos

OS Equipos y Servidores
Gestión de Identidad
SmartPhones
Procesos de Negocio
NAC
AntiSpam
Bases de Datos
Atributos de Usuario
IDS/IPS
Antivirus
Infraestructura Física
Antimalware
Análisis de Vulnerabilidades
Aplicaciones

Sistemas de Identidad
Gestión de Movilidad
Protección de Correo
Gestión de Vulnerabilidad

Visibilidad Empresarial

OS Equipos y Servidores
Gestión de Identidad
SmartPhones
Procesos de Negocio
NAC
AntiSpam
Bases de Datos
Atributos de Usuario
Antivirus
Infraestructura Física
IDS/IPS
Antimalware
Análisis de Vulnerabilidades
Aplicaciones

Arquitectura de Seguridad

REGULACIONES, CUMPLIMIENTO & FRAMEWORKS

REGULACIÓN	REQUERIMIENTOS FRENTE A LAS BASES DE DATOS
PCI	Monitoreo de acceso de datos personales en transacciones comerciales
SOX	Auditoría de transacciones financieras para garantizar la integridad de los estados financieros
Datos Personales	Auditoría de los accesos o modificaciones en los registros de clientes en las bases de datos.
Basilea	Monitoreo de la información de las cuentas que residen en las bases de datos.
CobIT	Gestión de accesos a datos sensibles.

NORMAS, LEYES Y REGULACIONES

- Normas:
  - » ISO 2700x
  - » ISO 20000
  - » SOX
  - » PCI
  - » BASILEA
- Frameworks
  - » ITIL
  - » CobIT

CNSF
COMISIÓN NACIONAL DE SEGUROS Y FIANZAS

SHCP
SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO

SAT
Servicio de Administración Tributaria

PROCESAR

BANCO DE MÉXICO

CNBV
COMISION NACIONAL BANCARIA Y DE VALORES

MODELO DE CONTROL

ISO 270001

+

SOX

+

CAP 10 CNBV

+

BAS III

+

PCI-DSS

+

→ Modelo de Gestión Propio

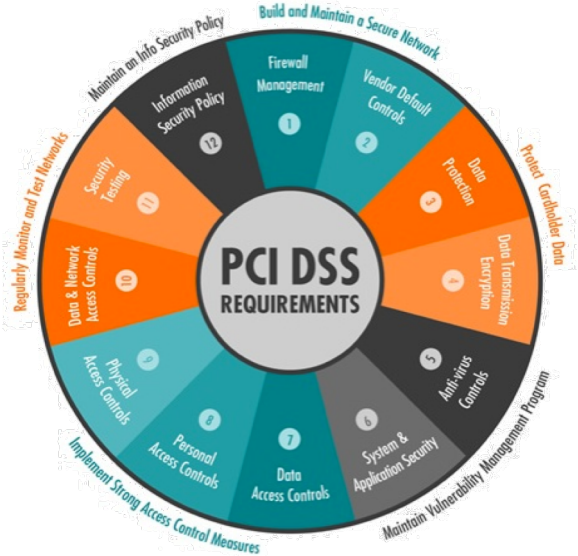
PCI-DSS

Constituido por:

Visa, MasterCard, American Express, Discovery JCB International

Conjunto de guías para el negocio con el fin de proteger la información personal durante las transacciones de pago con tarjetas:

- Adquisición
- Resguardo
- Procesamiento
- Transmisión



Minimizar el riesgo

- Brechas de seguridad
- Pérdida de patrimonio

Proteger la marca

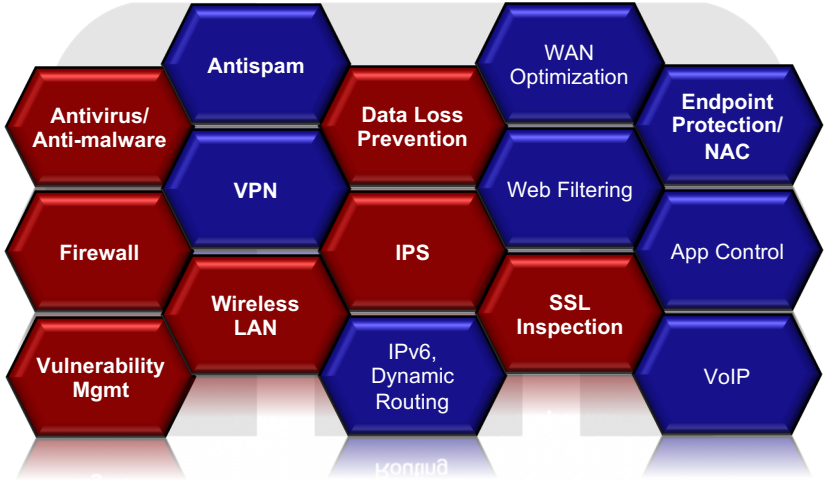
- Integridad
- Reputación

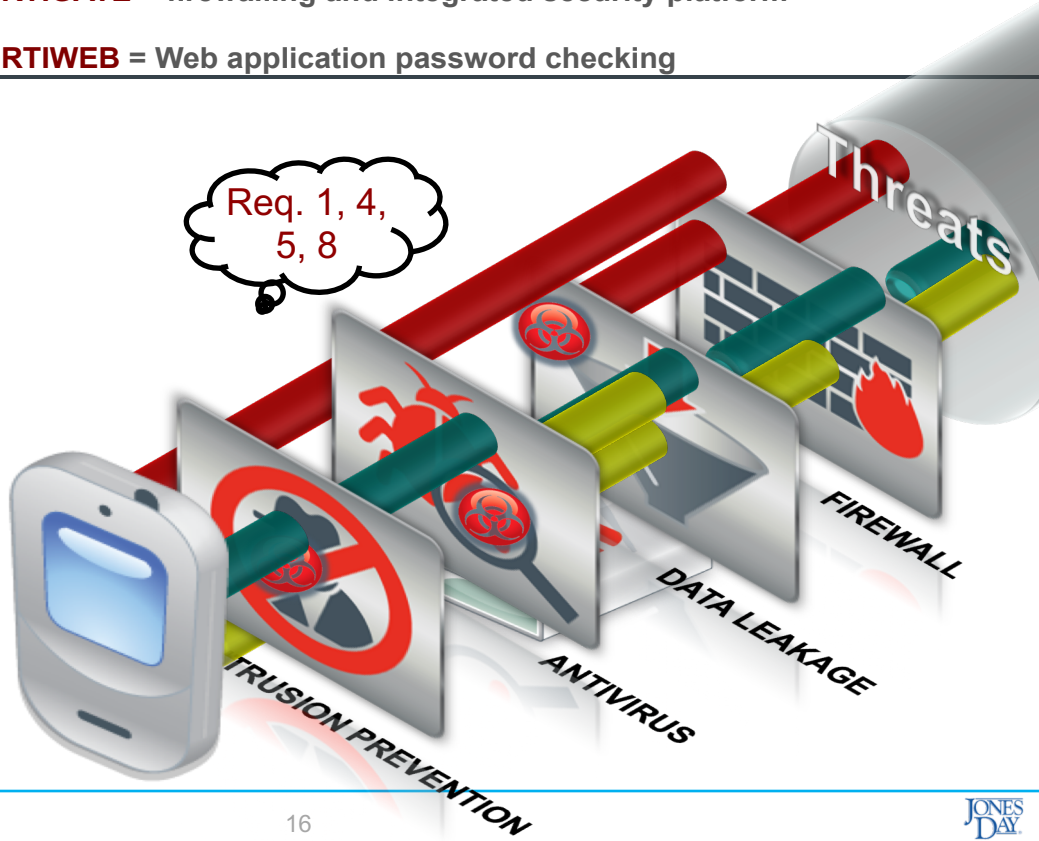
Proveer confianza

- Proteja su marca
- Proteja sus clientes

DEEP PCI STANDART #1

Build and Maintain a Secure Network	Proper firewalling policies throughout the network Integrated security Password integrity	**FORTIGATE** = firewalling and integrated security platform **FORTIWEB** = Web application password checking



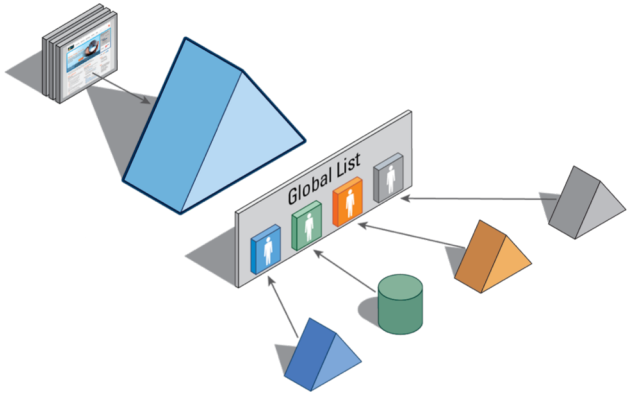


HITOS PARA PRIORIZAR LOS ESFUERZOS DE CUMPLIMIENTO DE LA PCI DSS

Desarrolle y mantenga redes y sistemas seguros	1	Instale y mantenga una configuración de firewall para proteger los datos del titular de la tarjeta.
	2	No usar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.
Proteger los datos del titular de la tarjeta.	3	Proteja los datos del titular de la tarjeta que fueron almacenados.
	4	Cifrar la transmisión de los datos del titular de la tarjeta en las redes públicas abiertas.
Mantener un programa de administración de vulnerabilidad	5	Proteger todos los sistemas contra malware y actualizar los programas o software antivirus regularmente.
	6	Desarrollar y mantener sistemas y aplicaciones seguros.
Implementar medidas sólidas de control de acceso	7	Restringir el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.
	8	Identificar y autenticar el acceso a los componentes del sistema.
	9	Restringir el acceso físico a los datos del titular de la tarjeta.
Supervisar y evaluar las redes con regularidad	10	Rastree y supervise todos los accesos a los recursos de red y a los datos del titular de la tarjeta.
	11	Probar periódicamente los sistemas y procesos de seguridad.
Mantener una política de seguridad de información	12	Mantener una política que aborde la seguridad de la información para todo el personal.

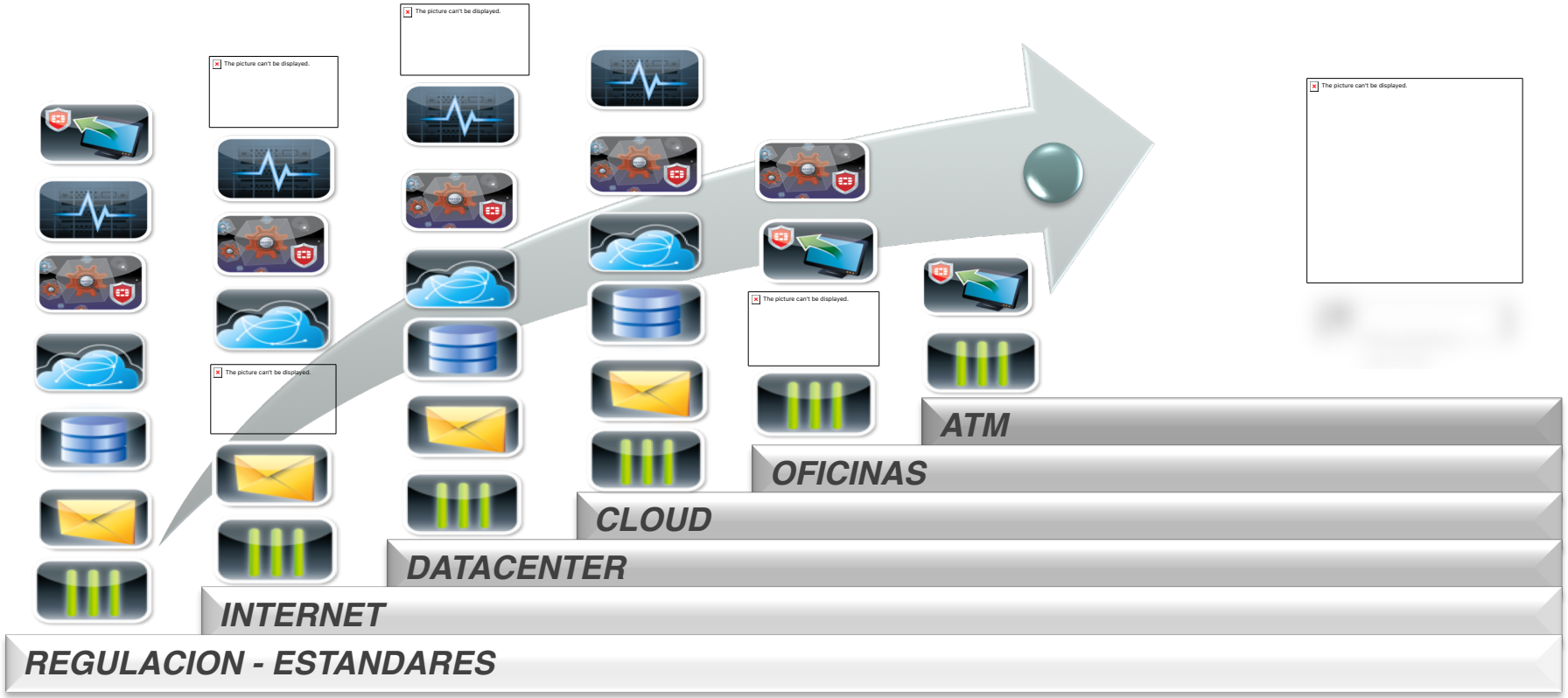
VISIBILIDAD DE DATOS CORE

- Control de cuentas privilegiadas.
- Accesos por medios no permitidos (Con permisos de Admin)
- Privilegios puente (fuera de compliance)
- Uso no restringido de recursos críticos.
- Inventario de procesos permitidos.
- Notificación a CRO o CIO en el momento de incumplimiento.
- Aplicación de políticas inmediatas enc aso de incumplimiento.

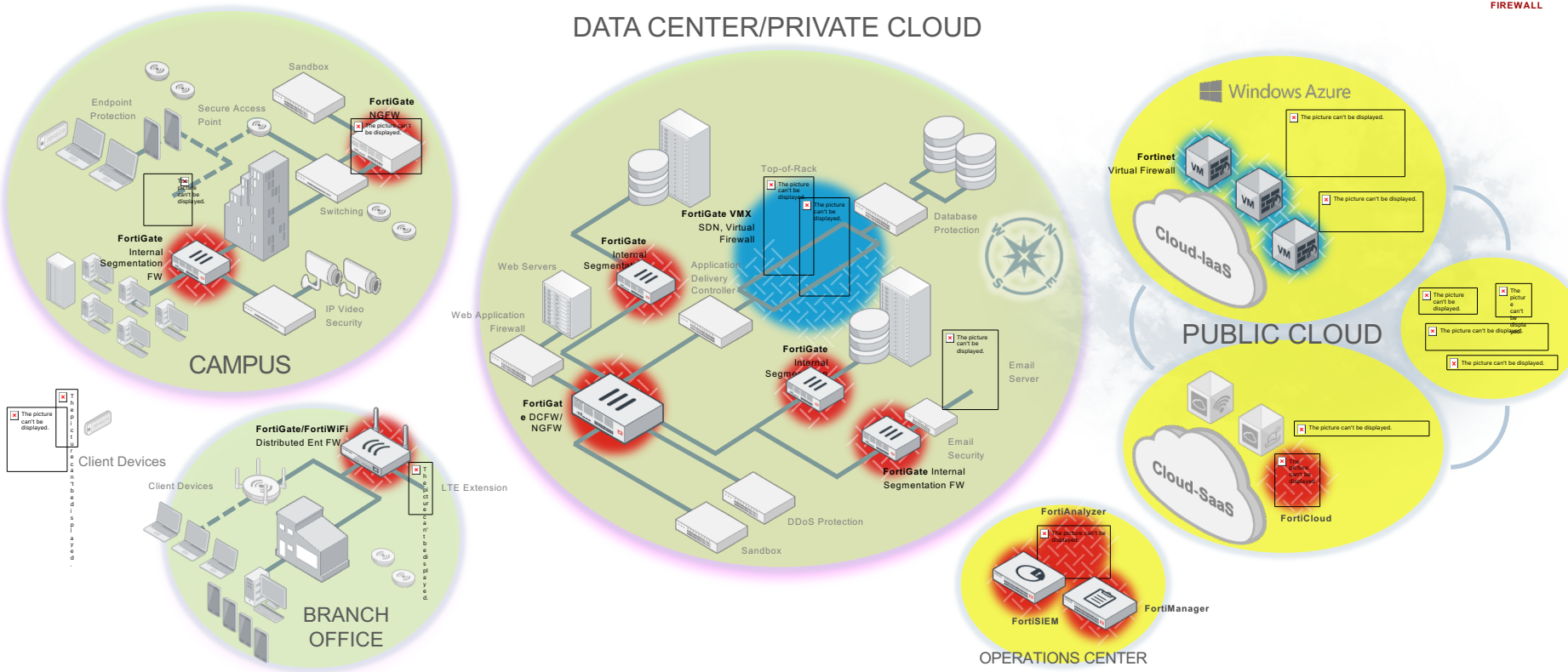


MODELO DE NEGOCIO
SERVICIOS PCI

SEGMENTO FINANCIERO SEGURIDAD Fortinet



FORTINET ENTERPRISE SECURITY FABRIC




FORTINET
JONES DAY
CONCLUSIONES