

Migración Infraestructura On Premise a Cloud AWS

Transformación progresiva hacia una arquitectura cloud-native escalable, segura y de alto rendimiento en Amazon Web Services

Migración a AWS

Visión Ejecutiva

CLIENTE

Migración del entorno on-premise MDV a AWS, implementando una arquitectura cloud que maximice la eficiencia operativa, seguridad y escalabilidad.

La migración de las aplicaciones existentes y recursos de TI a la nube de Amazon Web Services (AWS) presenta una oportunidad para transformar el modo en que su organización hace negocios. Puede ayudarlo a una reducción de los costos, ser más ágil, desarrollar nuevas habilidades con mayor rapidez y entregar servicios fiables y disponibles a nivel global a sus clientes. Nuestro objetivo es ayudarlo a implementar su estrategia en la nube correctamente.



ALCANCE DE LA INICIATIVA

- El alcance comprende la migración del 95% de la infraestructura on-premise del banco en una primera etapa.
- Migración de aplicaciones críticas basadas en Windows y SQL Server
- Modernización de canales digitales e integraciones
- Convivencia híbrida con core AS400 a través de múltiples opciones a analizar
- La segunda instancia es el análisis, conversión y migración del entorno AS400 a un modelo adaptado para arquitectura (x86 a x64) y cloud.



OBJETIVO DE ESTA PRESENTACIÓN

- ☑ Establecer una línea base técnica del entorno actual
- ☑ Definir el mapa de arquitectura as-is / to-be
- ☑ Proponer una estrategia de migración alineada al negocio
- ☑ Identificar consideraciones clave (riesgos, dependencias, seguridad, costos)
- ☑ Presentar un roadmap de implementación estructurado por fases

Análisis de la infraestructura actual



MDV Data Center

Tráfico desde Internet a través de WAF y firewall hacia servidores internos.

Carga Windows Server 2016

E-banking, interfaz web wire/certificados, archivos corporativos e imaging, respaldos (Veeam), controladores AD, escritorio Fiserv (CSR/Teller).

Datos y Middleware

SQL central con bases críticas; Ocean Systems (Fedlink, ECS, OFAC) y dependencias entre servicios.

Core: AS400 (IBM Power 8)

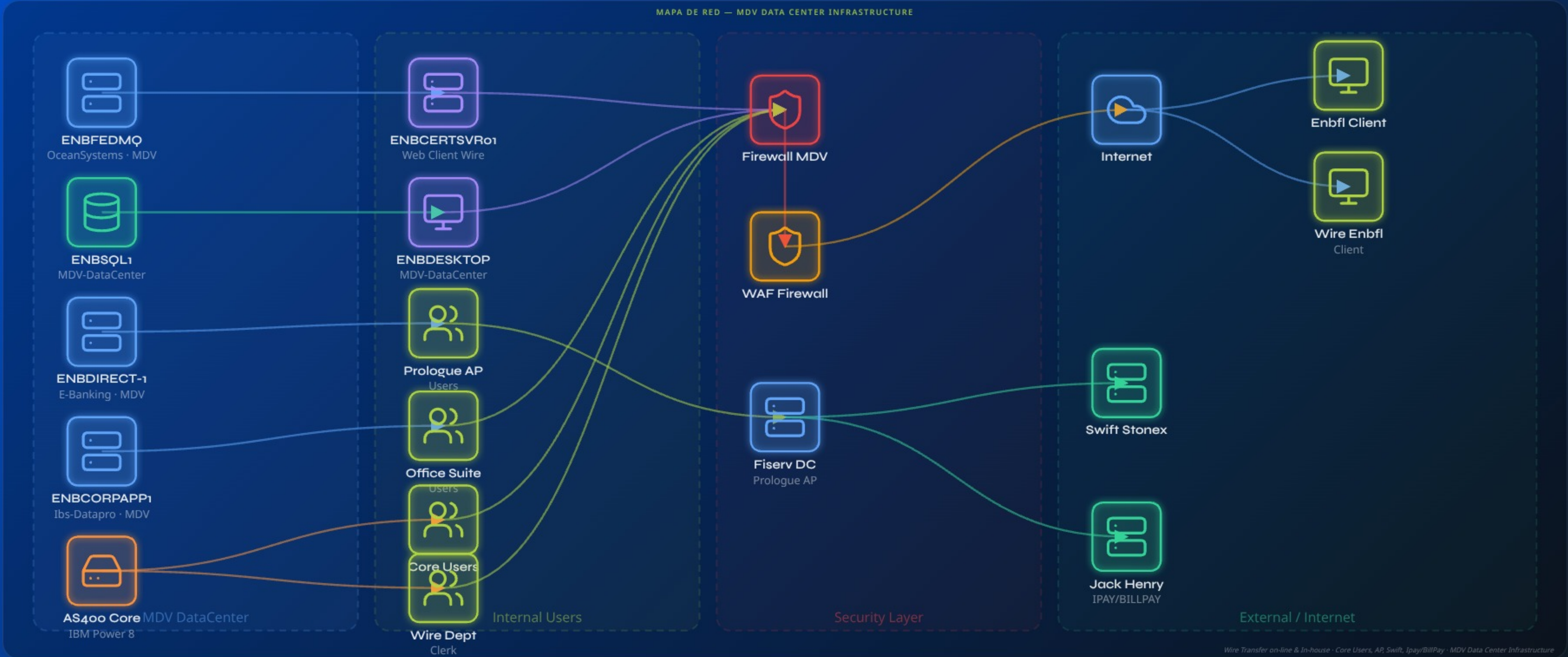
Sistema de registro y procesos core bancario.

Ecosistema Externo

Fiserv (Prologue AP), SWIFT (p. ej. Stonex), Jack Henry (iPay/BillPay).

Usuarios

Clientes externos (banca/wire), personal (core, wire, Swift, AP, Office).



Mapa del modelo: infraestructura actual vs objetivo en AWS

AS400 (core) permanece on-prem · conexión híbrida VPN o Direct Connect

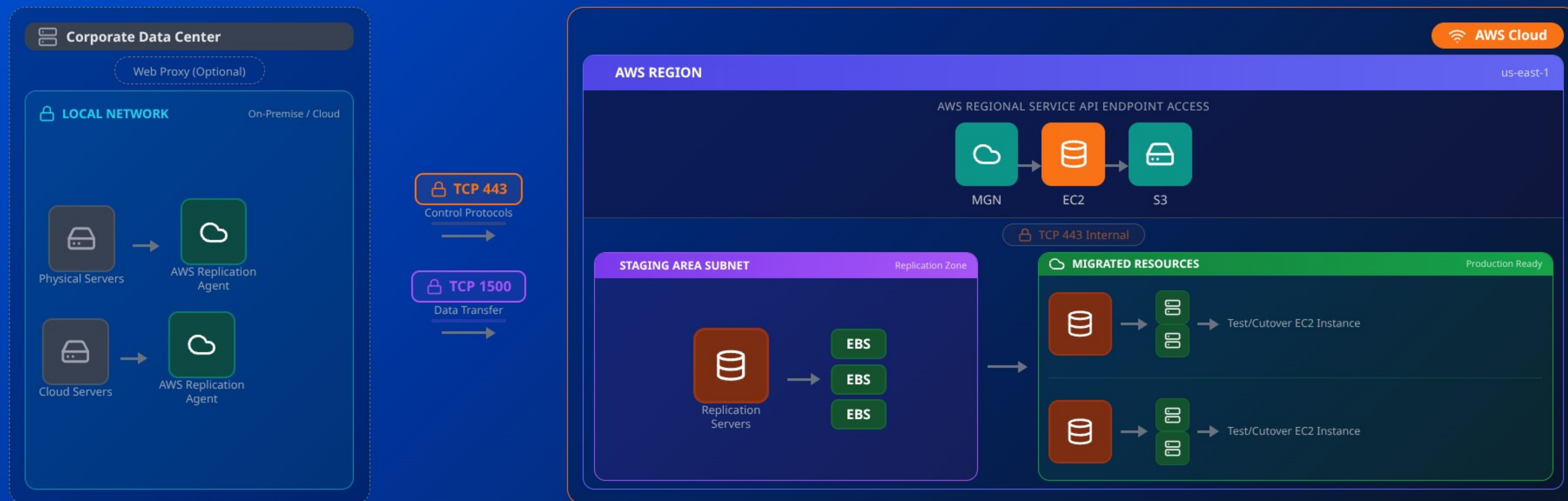


Método de Migración — AWS Application Migration Service



Lift & Shift sin downtime — Replicación continua de tráfico

> Haz clic en una flecha para ver el flujo >



☁ AWS Application Migration Service (MGN)

AWS Application Migration Service permite migrar servidores físicos, virtuales o en la nube hacia AWS de forma automatizada y con mínima interrupción. Funciona mediante la replicación continua de los servidores de origen hacia AWS a nivel de bloque, manteniendo los datos actualizados.

Durante la migración, se pueden ejecutar pruebas sin afectar el entorno productivo y, una vez validado, realizar el corte final (cutover) en una ventana controlada. Esto facilita una transición rápida, segura y consistente, sin necesidad de rediseñar las aplicaciones.

Etapa 1 - Pasos de implementación

Pasos de implementación

01 Descubrimiento y assessment

Cerrar el mapa de verdad y las decisiones que fijan diseño y etapas.

ACTIVIDADES

- Inventario de servidores y apps
- Diagrama as-is actualizado
- Talleres con negocio y vendors
- Definición de RTO/RPO y ventanas
- Revisión de licencias y certificados

ENTREGABLES

- Matriz de dependencias (app -> DB -> integración)
- Lista de riesgos y mitigaciones
- Decision Log v1 (RDS vs EC2 SQL, VPN vs DX, AD)
- Plan de etapas v0

CRITERIO DE SALIDA: *Sponsor de negocio y TI alineados en alcance por fase y prerequisites de integración.*

02 Fundaciones (Landing Zone + híbrido)

Una nube habitable con controles mínimos y conectividad probada hacia MDV/partners.

ACTIVIDADES

- Estructura de cuentas/OUs
- VPC multi-AZ y segmentación
- Baselines de IAM, KMS, CloudTrail
- IAM Identity Center
- VPN/DX y tablas de ruteo hacia AS400 y redes legacy

ENTREGABLES

- Landing zone documentada
- Entorno non-prod operativo
- Pruebas de conectividad (latencia, MTU, puertos)
- Monitoreo inicial (CloudWatch, alarmas críticas)

CRITERIO DE SALIDA: *Tráfico de prueba validado entre AWS y MDV y checklist de seguridad baseline completado.*

03 Migración por etapas y cutover

Mover cargas a producción en AWS con mínima interrupción y trazabilidad.

ACTIVIDADES

- Replicación MGN o estrategia equivalente por VM
- Migración SQL (backup/restore o DMS)
- DataSync/FSx para archivos
- Pruebas de integración en non-prod y prod por etapas

ENTREGABLES

- Runbooks de cutover y ventanas acordadas
- Conmutación DNS (Route 53)
- Hipercare 24-72 h post-cambio
- Informe de lecciones aprendidas por etapa

CRITERIO DE SALIDA: *Cargas en prod con KPIs de error/latencia dentro de umbrales y rollback no necesario o ejecutado según plan.*

04 Estabilización y operación continua

Consolidar operación BAU en la nube y preparar mejoras posteriores.

ACTIVIDADES

- Ajuste de dimensionamiento (FinOps)
- Evaluación Savings Plans / Reserved Instances
- Ejercicios de DR y rotación de secretos
- Endurecimiento continuo (Security Hub/Config)

ENTREGABLES

- Catálogo de servicios operados en AWS
- Runbooks actualizados
- Informe de optimización coste-seguridad
- Checkpoint de revisión del AS400

CRITERIO DE SALIDA: *Operación transferida a equipos con roles claros y métricas de disponibilidad/respaldo alineadas a negocio.*

Desafíos de la Transformación |

Mover el banco sin detenerlo: Superando la complejidad técnica.

VIRTUALIZACIÓN

Legacy sin Performance Loss

- ⚠ **Reto:** Desacoplar un Core diseñado para 'bare metal' sin perder performance.
- 🔧 **Estrategia:** Tuning fino sobre Red Hat Enterprise Linux (RHEL). Validación exhaustiva de IOPS antes del Go-Live.

CONECTIVIDAD

Híbrido sin Fricciones

- ⚠ **Reto:** Operar con 'un pie en cada lado' durante la migración sin latencia perceptible.
- 🔧 **Estrategia:** AWS Direct Connect + Estrategia de enrutamiento inteligente durante la fase transitoria.

INTEGRIDAD

Cero Pérdida de Datos

- ⚠ **Reto:** Mover Terabytes históricos con consistencia transaccional absoluta.
- 🔧 **Estrategia:** AWS MGN (Migration Service): Replicación en bloque a nivel disco, validación continua de checksums.

CULTURA FINOPS

Gobernar la 'Tarjeta Infinita'

- ⚠ **Reto:** Cambiar la mentalidad de 'CapEx fijo' a 'OpEx variable'. Evitar que la facilidad de aprovisionamiento dispare los costos.
- 🔧 **Estrategia:** Instaurar accountability donde cada equipo entiende el impacto económico de sus decisiones de arquitectura.

Impacto Real: 20/30% Ahorro Promedio

Más seguridad, agilidad y capacidades por la mitad del costo anterior.



OPEX REDUCTION

Impacto OPEX

Reducción directa vs. proveedor anterior, incluyendo el nuevo DRP.



RESILIENCE

Configuración DRP

Recuperación ante desastres robusta y costeable.



TIME TO MARKET

Horas

Aprovisionamiento acelerado para nuevos proyectos.



ELASTICIDAD

Auto-Scale

Recursos que crecen y decrecen según demanda real.



SECURITY BY DEFAULT

Fortinet + KMS

Cifrado nativo, IAM granular con MFA, firewall integrado.



COMPLIANCE

PCI • SOC2 • ISO

Certificaciones financieras: PCI-DSS, SOC2, ISO 27001.



OBSERVABILIDAD

360°

Métricas, logs y tracing centralizados. Alertas proactivas.



ALTA DISPONIBILIDAD

Multi-AZ

Tolerancia a fallos integrada con auto-healing.



ESTANDARIZACIÓN

IaC

Plantillas reproducibles, menos errores humanos.

Etapa 2 - Contexto y Complejidad de la Migración

AS400 a AWS



Arquitectura Origen

AS400 / IBM i

CPU RISC PowerPC 64 bits

Arquitectura propietaria, incompatible con hardware moderno.

Sistema cerrado e integrado

OS, DB2 y runtime funcionan como una única unidad inseparable.

Single-level storage

Memoria y almacenamiento unificados, complejidad oculta al desarrollador.

Lenguajes propietarios (RPG, CL, COBOL)

Baja portabilidad a otros entornos.

Modelo monolítico acoplado

Lógica, datos e infraestructura fuertemente interconectados.

Complejidad de la Migración

Incompatibilidad binaria — PowerPC no ejecuta en x86 sin transformación.

Dependencia del runtime IBM i — servicios internos inexistentes fuera del AS400.

Base de datos DB2 embebida — integrada profundamente con la lógica de negocio.

Lógica acoplada a infraestructura — sin separación clara entre app y plataforma.

Procesos batch y jobs propios — sin equivalentes directos en AWS.

Arquitectura Target

Amazon Web Services

x86/x64 y ARM

Infraestructura estándar y ampliamente compatible en la industria.

Modelo distribuido y desacoplado

Componentes independientes que se comunican vía APIs.

Servicios independientes (EC2, RDS, S3...)

Compute, base de datos y almacenamiento gestionados por separado.

Arquitectura cloud-native escalable

Escala dinámica según demanda y optimización de costos.

SERVICIOS AWS

EC2 RDS S3 Lambda ECS CloudWatch IAM VPC

ESTRATEGIA Y MODELOS DE ADAPTACIÓN

Modelos de Migración Evaluados	
Rehost (Lift & Shift)	No viable
Replatform	Limitado
Refactor	Recomendado
Re-architect	Ideal (cloud-native)

Estrategia Definida
Transformación progresiva
Separación de lógica de negocio
Desacople de base de datos
Rediseño de procesos batch

Adaptación Tecnológica	
RPG	→ Java / .NET / Python
CL	→ Step Functions, scripts, schedulers
DB2/400	→ RDS / Aurora (PostgreSQL / MySQL)

ANÁLISIS TÉCNICO: ¿POR QUÉ NO ES UN LIFT & SHIFT?

AS400 — Ecosistema monolítico integrado

Base de datos embebida en el OS — no es un componente independiente.

Single-level storage unifica memoria y almacenamiento en un único espacio lógico.

Jobs y subsistemas propios gestionan la ejecución de procesos.

Lógica de negocio ligada directamente a estructuras de datos y objetos del sistema.

AWS — Paradigma distribuido y desacoplado

Cómputo, almacenamiento y base de datos son servicios completamente separados.

Escalabilidad horizontal, no vertical — diseñada para crecer en paralelo.

Procesos batch rediseñados con herramientas de orquestación modernas.

Lógica de negocio desacoplada de la persistencia y la infraestructura.

01 Discovery

Relevamiento de programas y dependencias críticas.

- Inventario completo
- Mapeo de dependencias
- Identificación de riesgos

02 Análisis

Clasificación de lógica legacy por complejidad.

- RPG, COBOL, CL
- Lógica crítica
- Complejidad

03 Arquitectura

Diseño AWS alineado a requerimientos del negocio.

- EC2 / Lambda
- RDS / Aurora
- IAM, VPC, S3

04 Conversión

Reescritura en Java/.NET/Python, sin dependencias IBM i.

- Reescritura de código
- Rediseño batch
- Eliminación IBM i

05 Datos

Migración ETL a RDS/Aurora con validación de integridad.

- ETL desde DB2/400
- Transformación
- Validación

06 Testing

Pruebas con usuarios clave garantizando SLAs.

- Funcional
- Performance
- Regresión

07 Go-Live

Despliegue con IaC, CI/CD y plan de rollback.

- Terraform / IaC
- CI/CD
- Cutover controlado

08 Optimización

Optimización continua con observabilidad AWS.

- Costos cloud
- Performance
- CloudWatch

CONSIDERACIONES

⚠ RIESGOS PRINCIPALES

Alta complejidad técnica

Pérdida de conocimiento legacy

Errores en lógica de negocio

Impacto operativo en transición

🛡 MITIGACIÓN

Documentación exhaustiva previa

Migración por fases controladas

Testing intensivo con usuarios clave

Estrategia de rollback definida

⭐ BENEFICIOS ESPERADOS

Independencia de hardware propietario

Escalabilidad y elasticidad AWS

Reducción de costos operativos

Mayor velocidad de innovación

Integración con ecosistema cloud

📌 CONCLUSIÓN:

La migración de AS400 a AWS transforma un modelo monolítico en arquitectura distribuida moderna, habilitando escalabilidad, reducción de costos e innovación continua.

Etapa 2 - Consideraciones Clave del Proyecto



FACTORES CRÍTICOS



Gestión con Vendors CRÍTICO

- Reuniones con proveedores de software actuales
 - Validación de compatibilidad con AWS
- Confirmación de soporte en nuevas BBDD (RDS / Aurora)
 - Evaluación de licenciamiento en cloud



Base de Datos PUNTO SENSIBLE

- Validar equivalencias DB2/400 vs motores destino
- Compatibilidad de queries, stored procedures y lógica embebida
- Evaluación de necesidad de refactor o reescritura

CONSIDERACIONES ADICIONALES



Dependencias Externas

- Interfaces con otros sistemas
- Integraciones batch y online
- APIs o conectores propietarios



Gestión del Cambio

- Capacitación de equipos
- Adaptación operativa a AWS
- Nuevos modelos de soporte



Gobernanza y Seguridad

- Definición de roles (IAM)
- Políticas de seguridad y compliance
 - Auditoría y monitoreo

CONCLUSIÓN CLAVE

No es un lift & shift: implica reinterpretar, rediseñar y transformar completamente la solución.

Por lo tanto, no es viable un enfoque de "lift & shift", ya que no existe equivalencia directa entre ambos modelos. Todo el sistema debe ser reinterpretado desde el punto de vista funcional y técnico, rediseñado para un entorno distribuido y transformado para adaptarse a estándares modernos. Este proceso requiere un entendimiento profundo del sistema original y una redefinición de su arquitectura para asegurar que funcione correctamente en el nuevo contexto.



La validación con vendors y la compatibilidad de bases de datos (DB2/400 ↔ PostgreSQL / Aurora) son los factores más críticos: impactan directamente el esfuerzo de migración y el diseño final de la arquitectura.

Presupuesto Estimativo AWS

Migración On-Premise → Cloud · Región US East (Ohio) · Estrategia: 1 año sin pago inicial

\$0

COSTO INICIAL

Reservado

\$11,775

COSTO MENSUAL

USD / mes

\$141,306

COSTO ANUAL

USD / 12 meses

17

INSTANCIAS EC2

EC2 totales

SERVICIO	DESCRIPCIÓN / SERVIDORES	TIPO DE INSTANCIA	OS / TENANCY	ALMACENAMIENTO	ESTRATEGIA DE PRECIO	COSTO MENSUAL
 Amazon EC2 Compute · 8 instancias	SRV-enbcertsrv01, SRV-enbcorpap-p2, SRV-enbcorpdesktop, SRV-enbcorpfs1, SRV-enbdirect-1, SRV-enbfedmq, SRV-VEEAM, SRV-CLOUDHOSTING	c5.2xlarge	Windows Server Dedicated	2,800 GB EBS	1yr No Upfront	\$6,341/mo 54%
 Amazon EC2 Compute · 7 instancias	SRV-enbcorpap-p1, DC1, DC2, SRV-enbcorpdesktop, SRV-enbimaging, SRV-enbsqlldr1, SRV-enbtermsrv01	m5.large	Windows Server Dedicated	2,100 GB EBS	1yr No Upfront	\$1,886/mo 16%
 Amazon EC2 Database · 1 instancia	SRV SQL — SQL Server Standard	c5.2xlarge	Windows + SQL Std Dedicated	—	1yr No Upfront	\$1,096/mo 9%
 Amazon VPC Network · 12 IPs	12 IPv4 Públicas · 2 Transit Gateway · Gateway Load Balancer (2 AZs) · 1 GWLB Endpoint · 5 GB/hr	—	—	—	On-Demand	\$2,170/mo 18%
 Amazon S3 Storage · 10 TB	Bucket Veeam Backup — S3 Standard · 1M PUT/COPY/POST/LIST · 1M GET/SELECT requests	—	—	10,240 GB	On-Demand	\$241/mo 2%
 Amazon EC2 Security · 1 instancia	EC2 Fortigate Instance — Firewall / Security Appliance	c5.large	Linux Dedicated	150 GB EBS	1yr No Upfront	\$41/mo 1%

 **LICENCIAMIENTO ANUAL**

 **Licencia Anual Veeam BKP & Replication**

El costo depende de la cantidad de cargas de trabajo, edición contratada y si se incluye DR.

EDICIÓN	PRECIO APROXIMADO
Foundation	USD 250 / workload / año
Advanced	USD 350 / workload / año
Premium (incl. Recovery Orchestrator)	USD 450 / workload / año

 **Licencia Anual Fortinet FortiGate 100F**

Licencia anual para FortiGate 100F. Bundle más utilizado en entornos corporativos: UTP.

LICENCIA	PRECIO APROXIMADO (USD/AÑO)
FortiCare Premium	USD 600
ATP Bundle	USD 1.100 – 1.300
UTP Bundle (recomendado)	USD 1.600 – 1.900
Enterprise Protection	USD 2.200 – 2.700

* Estimación AWS Pricing Calculator. Los costos reales pueden variar según el uso efectivo. No incluye impuestos aplicables.

ⓘ → Esta estimación es referencial y fue elaborada exclusivamente en base a la configuración compartida por el cliente. Puede sufrir variaciones por cambios en los costos, condiciones y políticas de AWS.

¡Gracias!

Contáctenos para más información