NUVOL
Cybersecurity services

CASO DE ÉXITO

Banca de Confianza: 7 años construyendo una cultura de ciberseguridad sostenible

Sector Bancario | LATAM

Uno de los bancos más importantes de LATAM confió en Nuvol Cybersecurity para transformar su postura de seguridad durante 7 años consecutivos. Lo que inició como una iniciativa puntual de concientización se convirtió en una alianza estratégica integral que abarca desde la gestión de identidades hasta el soporte operativo de infraestructura.

7+
Años de Colaboración
Relación continua y en expansión

6
Capas de Seguridad
Servicios activos en simultáneo

Banca
Sectores cubiertos
Uno de los + importantes en LATAM

El Desafío

El banco operaba en un entorno regulatorio exigente con una superficie de ataque en expansión. Sus principales retos al iniciar la alianza con Nuvol:

- Alto riesgo humano: colaboradores con baja cultura de ciberseguridad, vulnerables a phishing y ingeniería social.
- Gestión de identidades dispersa: sin una estrategia unificada de acceso, autenticación y protección de credenciales.
- Protección de información no estructurada: datos sensibles sin clasificación ni etiquetado consistente en el entorno Microsoft 365.
- Brechas operativas en infraestructura: parches de seguridad en servidores Linux y Windows con ejecución irregular y sin visibilidad centralizada.
- Dependencia de talento externo especializado: necesidad de personal técnico de soporte sin la capacidad de contratarlo internamente a escala.

La solución

Nuvol diseñó e implementó una arquitectura de seguridad en capas, alineada al contexto regulatorio y a las prioridades operativas del banco. La solución integra seis componentes clave:

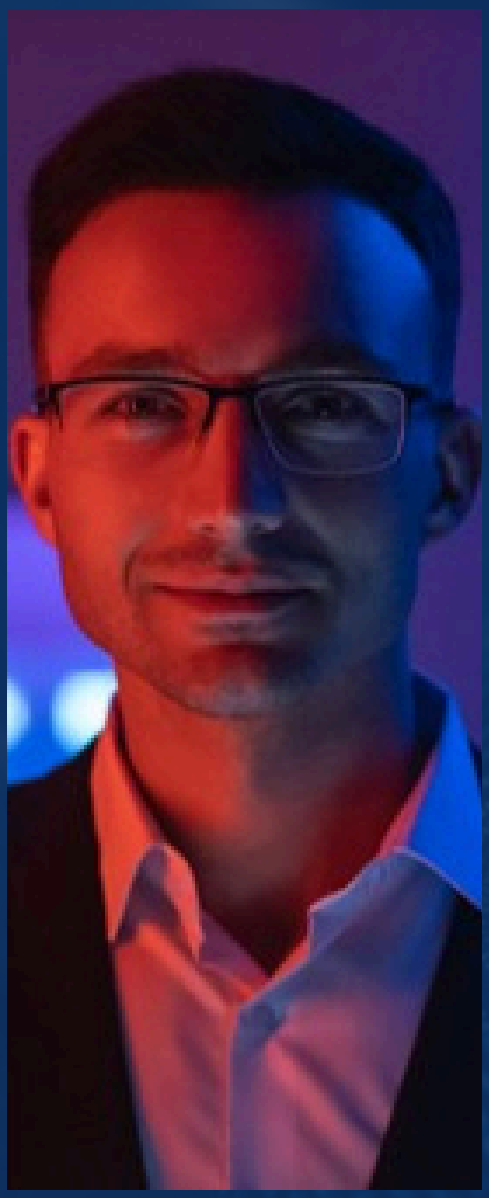
Capa	Tecnología / Servicio	Valor entregado
Concientización	KnowBe4 Security Awareness Training	Reducción del riesgo humano con simulaciones de phishing, campañas continuas y métricas de mejora conductual por área.
Identidad y Acceso	Microsoft Entra ID	Gestión centralizada de identidades, políticas de acceso condicional y control de usuarios privilegiados bajo Zero Trust.
Autenticación	Windows Hello for Business	Eliminación de contraseñas en endpoints: autenticación biométrica y por PIN seguro, reduciendo drásticamente el riesgo de robo de credenciales.
Gestión de Dispositivos	Microsoft Intune	Políticas de cumplimiento, gestión de dispositivos corporativos y protección de datos en endpoints bajo control centralizado.
Protección de Datos	Microsoft Purview (Etiquetado y Clasificación)	Clasificación automática y manual de información sensible. Políticas de prevención de pérdida de datos (DLP)
Operaciones IT	IT Outsourcing: Soporte Técnico + Parchado de Seguridad	Personal especializado de Nuvol integrado al equipo del banco para soporte de usuarios y gestión de parches en servidores Linux y Windows.

Resultados e impacto

Cultura de Seguridad

- Adopción sostenida del programa KnowBe4 por más de 7 años, uno de los indicadores más sólidos de madurez cultural en ciberseguridad.
- Reducción progresiva en la tasa de clics en simulaciones de phishing, con mejoras medibles por área y nivel jerárquico.
- El banco cuenta hoy con métricas de riesgo humano (Human Risk Score) como parte de sus KPIs de seguridad ante reguladores.

NUVOL
Cybersecurity services



Identidad y Acceso sin contraseñas

- Implementación exitosa de Windows Hello for Business: autenticación biométrica y por PIN eliminando el uso de contraseñas en estaciones de trabajo.
- Entra ID como eje de gestión de identidades: acceso condicional activo y políticas de Zero Trust aplicadas a todo el directorio corporativo.
- Reducción del riesgo asociado a reutilización y robo de contraseñas, un vector crítico en el sector bancario.

Protección de Datos e Información

- Clasificación y etiquetado de información sensible implementado sobre Microsoft 365, alineado a normativas.
- Intune como plataforma de gestión de cumplimiento de dispositivos, garantizando que solo endpoints sanos accedan a activos críticos.

Operaciones y Continuidad

- Soporte técnico operativo continuo integrado al equipo del banco — con personal de Nuvol actuando como extensión del equipo interno.
- Gestión sistemática de parches de seguridad en servidores Linux y Windows, reduciendo la ventana de exposición ante vulnerabilidades críticas.
- Ejecución predecible y auditada del ciclo de parchado, alineada a políticas de gestión de riesgo tecnológico del banco.

Porque Nuvol

- Mismo equipo técnico senior durante 7 años
- Visión integral: estrategia + operación
- Especialistas en seguridad Zero Trust en Microsoft
- CSM dedicados en los proyectos
- Respuesta rápida y acceso directo al experto

"Nuvol no es un proveedor. Es el equipo técnico de ciberseguridad que no teníamos internamente — y que siempre estuvo cuando lo necesitamos, su acompañamiento marca la diferencia"
CISO

Conversemos sobre cómo Nuvol puede ser su aliado estratégico de ciberseguridad.

info@cybernuvol.com México - Panamá - Colombia +(52) 55 9124 0158