HSM as a Services

Gestión de Claves y Servicios Criptográficos

PRESENTADA POR :

Agenda

Mensaje Introductorio

Propuesta de Valor

Ej. Casos de uso

Propuesta de Servicios

Modelo de Negocio

¿Preguntas?

Gracias por su atención!

A medida que las empresas adoptan cada vez más estrategias en la "nube”, la seguridad criptográfica se convierte en un desafío continuo que requiere un complemento que les brinde generar, acceder y proteger las claves criptográficas, independientemente de los datos confidenciales.

Recomendación

Proteger y Administrar las Claves Criptográficas de una manera segura a través del uso de Módulos de Seguridad por Hardware - HSM con certificación FIPS 140-2 nivel 3.

HSM as a Services

FIPS es acrónimo de (Federal Information Processing Standard)

Desafíos de Seguridad

Nuevos casos de uso requieren soportar estándares y elementos de seguridad mas robustos.

Cuando la clave y el activo son los mismos, cualquier persona que obtenga la clave puede monetizar y vulnerar el activo.

Los estándares de seguridad van evolucionando a medida que nacen nuevas soluciones y servicios en la industria.

La transferencia de valor malicioso puede ser instantáneo e irreversible

La administración de claves cuando la protección se mueve de centralizado a descentralizado

Transacciones de pago tradicionales, la incorporación de nuevos canales, firmas digitales, cifrado de punta a punta, PKI, blockchain, etc.

¿Gestión de Claves y Gateway de Servicios Criptográficos?

Propuesta de Valor

Un Servicio Administrado en la nube que le permite crear y controlar las claves de cifrado utilizadas por las aplicaciones, combinado con una librería de funciones criptográficas que hacen uso del HSM para obtener seguridad y continuidad en el cumplimiento del negocio.

La Solución

Hardware Security Modules

HSMs en la nube que protege y administra las claves, facilitando funciones criptográficas de cifrado, descifrado, autenticación, firmas , verificación, entre otras.

Manejo seguro de las claves cifradas para el ciclo de vida completo.

Hardware certificado (Tamper Resistant FIPS 140-2) que son sometidos a estrictas pruebas de conformidad.

Habilita funciones de Criptografía especializadas (Block TR-31, generador de números aleatorios, AES, Hashing, RSA, Elliptic Curve ECDSA, etc.).

Diseñados para admitir el más alto nivel de requisitos de RAS (Reliability, Availability, and Serviceability) verificandose en todo momento.

El HSM genera llaves bajo distintos estándares, tiene almacenamiento seguro y descarga las operaciones criptográficas de todo el sistema.

Arquitectura del Servicio

Aplicaciones y Sistemas de clientes

Comandos (entrada y salida) de Funciones del HSM

Layer interna del HSM

Criptographic Engine FIPS 140-2 nivel 3

HSM as a Service

Casos de Usos

Apoyo a las Aplicaciones de Medios de Pago

Canales

Networks

Front End
ATM, POS, P2P, e-Banking

Funciones

- Intercambio de claves KEK
- PIN Translate
- PIN Verify
- PIN Change o PIN Generate
- Generar y Verificar CVV o CVC
- Verificar ARQC y Generar ARPC - EMV
- Generación y Validación de OTPs
- Derivar Claves EMV
- Derivar Claves RKL en ATMs
- Derivar Claves DUKPT en POS
- Otras

Comandos nativos del HSM

Layer & PKCS #11

Cryptographic engine

HSM

Algortitmos Criptográficos:

• Algoritmos de clave pública PKI (asimétricos): RSA, Diffie-Hellman, ECMQV, DSA, KCDSA, ECDSA, ECDH, Edwards (X25519, Ed25519ph)

• Digital Wallet Encryption: BIP32

• Algoritmos simétricos: TDES, TR31, AES, AES-GCM, ARIA, Camelia, CAST, RIPEMD160 HMAC.

• Key Derivation: SP800-108 Counter Mode • Key Wrapping: SP800-38F

Los estándares soportados:

• Cumplimiento de seguridad: FIPS 140-2 Nivel 2 y Nivel 3

• Cumplimiento de las normas de seguridad y medioambientales: UL, CE, FCC, C-TICK, Canadá ICES, RoHS2, WEEE

• Generación de claves - AES, TDES, HMAC y PKI (ECC and RSA)

• Generación **(key-pair)** y verificación de firmas digitales utilizando el algoritmo RSA o ECDSA

• Soporte ECDSA / DH para derivación de claves.

• Hash/message digest: SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160

•Intercambio de claves Criptográficas (key wrapping & unwrapping) - KEK

• Cifrado /descifrado de datos y generación /verificación de MAC basado en hash (HMAC,CMAC)

• Hardware-based Digital Random Number Generator (DRNG)

Cryptography Asymmetric • Symmetric

Administración Remota

Tarjetas inteligentes para control de acceso y almacenamiento de claves por cliente.

Permite que el cliente junto con el proveedor utilicen una interfaz de navegador estándar para obtener acceso de forma remota a los HSM, donde realizaremos operaciones de administración de claves sin tener que desplazarse al centro de datos.

BENEFICIOS

- Gestión remota centralizada y fácil de usar.
- Evita viajar a centros de datos.
- Fuerte control de acceso y auditoría.
- El cliente tiene control de sus claves.

Seguridad y Auditoria en la Gestión de Administración

Beneficios de Nuestra Propuesta

Servicio integral para acceso a HSMs de pago

Ubicado en Datacenters venezolanos con redundancia

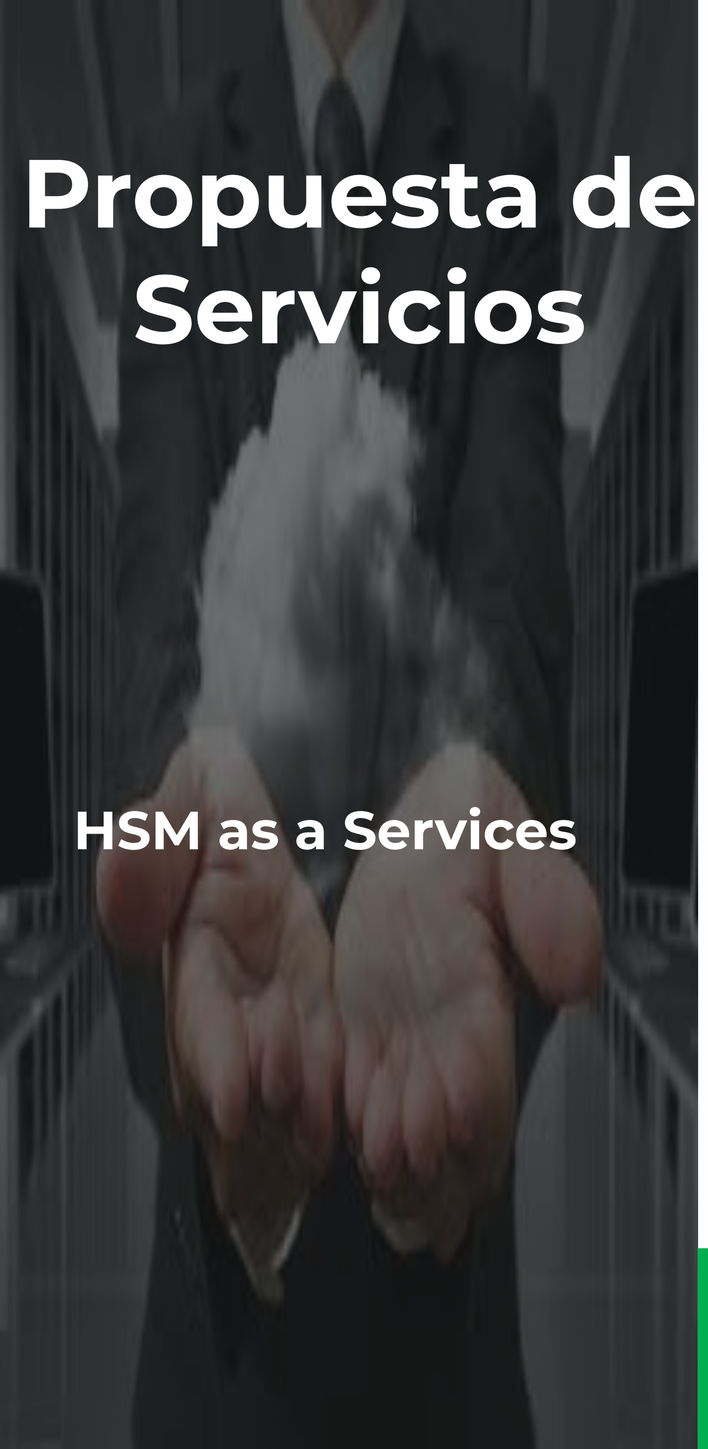
Se adapta a las necesidades del cliente (escalable)

Consultoría con especialistas de más de 35 años en el mercado

Soporte y Apoyo de Partners especializados

Balance entre costo y beneficio

Servicio de soporte flexible para apoyar distintos casos de uso.



Propuesta de Servicios

HSM as a Services

- Servicios de Consultoría (initial setup fee):

- Levantamiento de información - definición de Alcance
- Elaboración de Documento de especificaciones SOW
- Asesoría para la integración.

- Plan HSM as a Services

- Se ubica en el plan de servicios requerido (pago Mensual)
- Pago base Mensual

- Servicios de Integración y puesta en marcha:

- Configuración y ajustes
- Pruebas preliminares de integración y funcionalidad
- Pruebas de certificación/Aseguramiento de Calidad QA
- Implantación en producción
- Soporte y acompañamiento post producción

- Gerencia de proyecto
- Capacitación y documentación

Integración a la Medida

Planes de Servicios

Planes	Descripción	Precio	Enlace/Conexión
Bronce	1 HSM. Hasta 20 CPS Soporte 8x5		Publica
Plata	2 HSMs Físicos en Centros de Datos Separados Hasta 50 CPS Soporte 8x5		Publica
Oro	2 HSMs Físicos en Centros de Datos Separados Hasta 120 CPS Soporte 12x5		Publica
Diamante	2 HSMs Fisicos en Centros de Datos Separados Hasta 250 CPS Soporte 7x24		Publica
Plata Plus	2 HSMs Fisicos en Centros de Datos Separados Hasta 50 CPS Soporte 8x5		Privada
Oro Plus	2 HSMs Físicos en Centros de Datos Separados Hasta 120 CPS Soporte 12x5		Privada
Diamante Plus	2 HSMs Físicos en Centros de Datos Separados Hasta 250 CPS Soporte 7x24		Privada

Diferentes Paquetes para Diferentes Necesidades

Modelo de Negocio

Item	Precio	Frecuencia
Setup Fee		Pago único
Plan de Servicio (Ejemplo Plata)		Mensual

Alcance:

Setup fee: Consultoría para integración, capacitación, ceremonia de llaves.

Mensualidad: Conexion al (los) HSMs contratados según capacidad indicada, Soporte para 3DES, RSA, AES, DUKPT, Acceso a funciones criptográficas.

Premisas de la Oferta:

- Contrato mínimo a 3 años.

- Ajuste anual (POR DEFINIR)

- El cliente tendrá tres (3) tarjetas smart card para la gestión de su LMK.

- El cliente podrá cambiar a otros planes, informando con dos (2) meses de anticipación.

GRUPO 3000

Es un consorcio de capital privado que reúne a un grupo de 3 empresas dedicadas a la comercialización de productos y servicios en materia tecnológica.

Tecnocomputación 3000 S.A.

Fundada en 1983 en Venezuela

Dedicada a la comercialización de soluciones de **medios de pago electrónico** para sectores como el financiero, *retail* y de gobierno

Tecniservicio 3000 C.A

Rif: J-00221433-5

Fundada en 1990 en Venezuela.

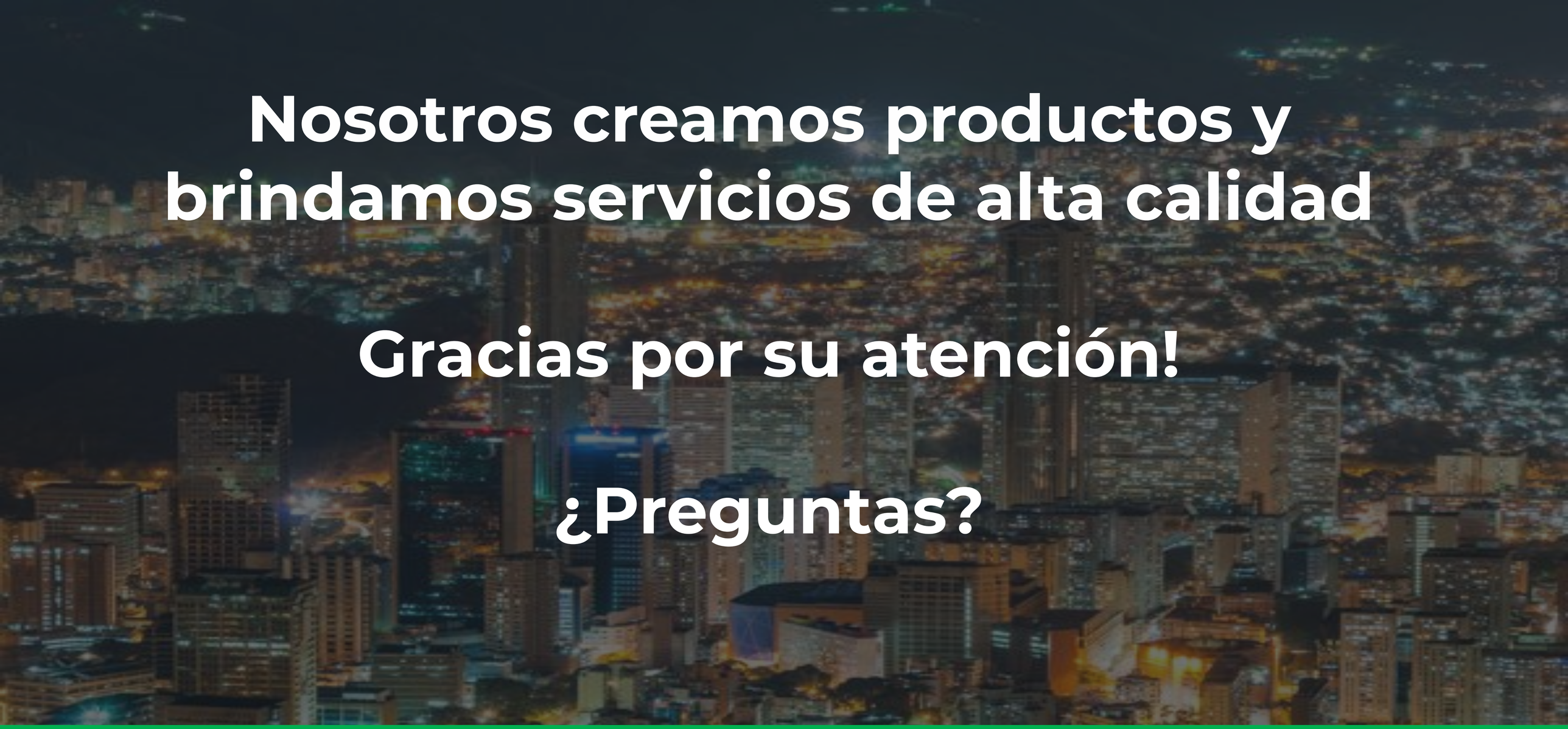
Dedicada a prestar **soporte técnico** a las soluciones que comercializan las empresas del grupo.

Identificación Plástica 3000 C.A.

Rif: J- 00223338-9

Fundada en 1985 en Venezuela.

Dedicada a la comercialización de **impresoras de carnets y sus accesorios,** para clientes finales, como asociados comerciales.



Nosotros creamos productos y brindamos servicios de alta calidad

Gracias por su atención!

¿Preguntas?

Visítanos: www.tecnocomputacion.com

Contactos

Ana María Dávila
Consultor de Negocios
Gerencia de Medios De Pago
Cel. + 58 (412) 627.3000 / + 58 (414) 905.5810
Telf. + 58 (212) 283.5366 Ext. 225
Correo: adavila@gr3000.com

Ana Fabiola Castrillón
Consultor de Negocios
Gerencia de Medios De Pago
el. +58(412) 2343000
Telf. +58(212) 283-5366 y +58(212) 284-9721.
Correo: acastrillon@gr3000.com

Orian Starke
Consultor de Negocios
Gerencia de Medios De Pago
Cel. 0412-2563000
Telf. 0212-2860065 ext. 265
Correo: ostarke@gr3000.com