ENCRIPTANDO LOS DATOS EN SQL SERVER

Wilmer Edgardo Martinez

SJO DIGITAL 2025

Primus Data

TEC | Tecnológico de Costa Rica

SJO DIGITAL 2025

AGRADECIMIENTO ESPECIAL
A NUESTROS PATROCINADORES

Primus Data

BRUNA GROUP

NESCAFÉ

TEC | Tecnológico de Costa Rica

THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

advancelearning

AGENDA

- Tipos de datos y su valor
- ¿ Qué es una amenaza ?
- Tipos de amenazas
- ¿Qué es seguridad?
- ¿Qué es encriptación? Y los tipos de encriptación
- Ejemplos de encriptación

Primus Data

TEC | Tecnológico de Costa Rica

SJO DIGITAL 2025

TIPOS DE DATOS Y SU VALOR

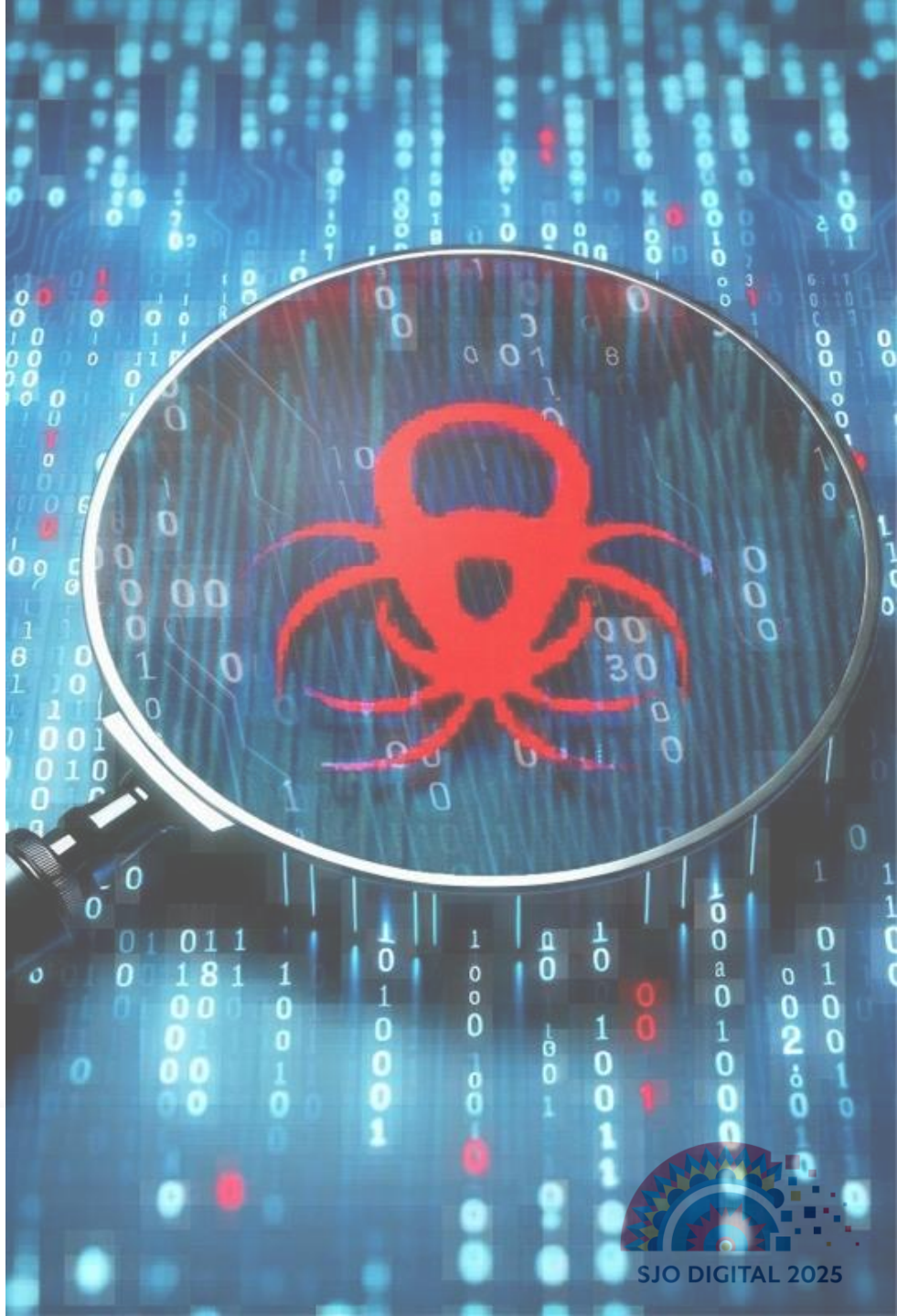
- Datos personales
- Datos Financieros
- Datos sensibles
- Datos de comportamiento
- Datos de propiedad intelectual

¿ QUÉ ES UNA AMENAZA ?

- Es una acción negativa o perjudicial, generalmente es un intento de infundir miedo, intimidación o coacción.
- Las amenazas pueden provenir de diversas fuentes y tomar muchas formas.

¿ QUÉ ES UNA AMENAZA ?

- Una amenaza es un fallo en la tecnología de las empresas que puede comprometer los datos.
- Una amenaza a una Base de Datos es la manipulación maliciosa de datos, sin permisos del sistema para ejercer acciones maliciosas como intento de hackeo.



Primus Data

TEC | Tecnológico de Costa Rica

SJO DIGITAL 2025

TIPOS DE AMENAZAS

- Phishing
- Malware
- Amenazas internas
- Accesos NO autorizados
- Ataque de denegación de datos (DDoS)

¿ QUÉ ES SEGURIDAD ?

- La palabra seguridad proviene del **Latín Securitas**, que significa **libre de cualquier peligro o daño**.
- En informática es el conjunto de tecnologías, procesos y practicas diseñadas para la protección de redes, dispositivos, programas y los datos en caso de ciberataque, hackeo, daño o acceso no autorizado.

Primus Data

TEC | Tecnológico de Costa Rica

SJO DIGITAL 2025

¿ QUÉ ES SEGURIDAD DE LOS DATOS?

La seguridad de los datos se refiere a las medidas de protección empleadas para proteger los datos contra accesos no autorizados y para preservar la confidencialidad, la integridad y la disponibilidad de la base de datos.

PRINCIPIOS DE SEGURIDAD DE DATOS

Confidencialidad

Integridad

Disponibilidad

Autenticación y Autorización

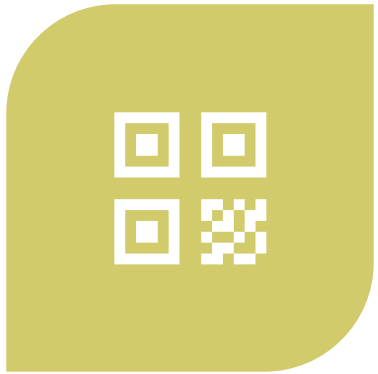
¿ QUÉ ES ENCRIPTACIÓN ?

Es un proceso de codificación mediante el cual se altera el contenido de la información haciéndola ilegible, de esta manera se consigue mantener la confidencialidad de la información mientras viaja del emisor al receptor.

TIPOS DE ENCRIPTACIÓN

TIPOS DE ENCRIPTACIÓN

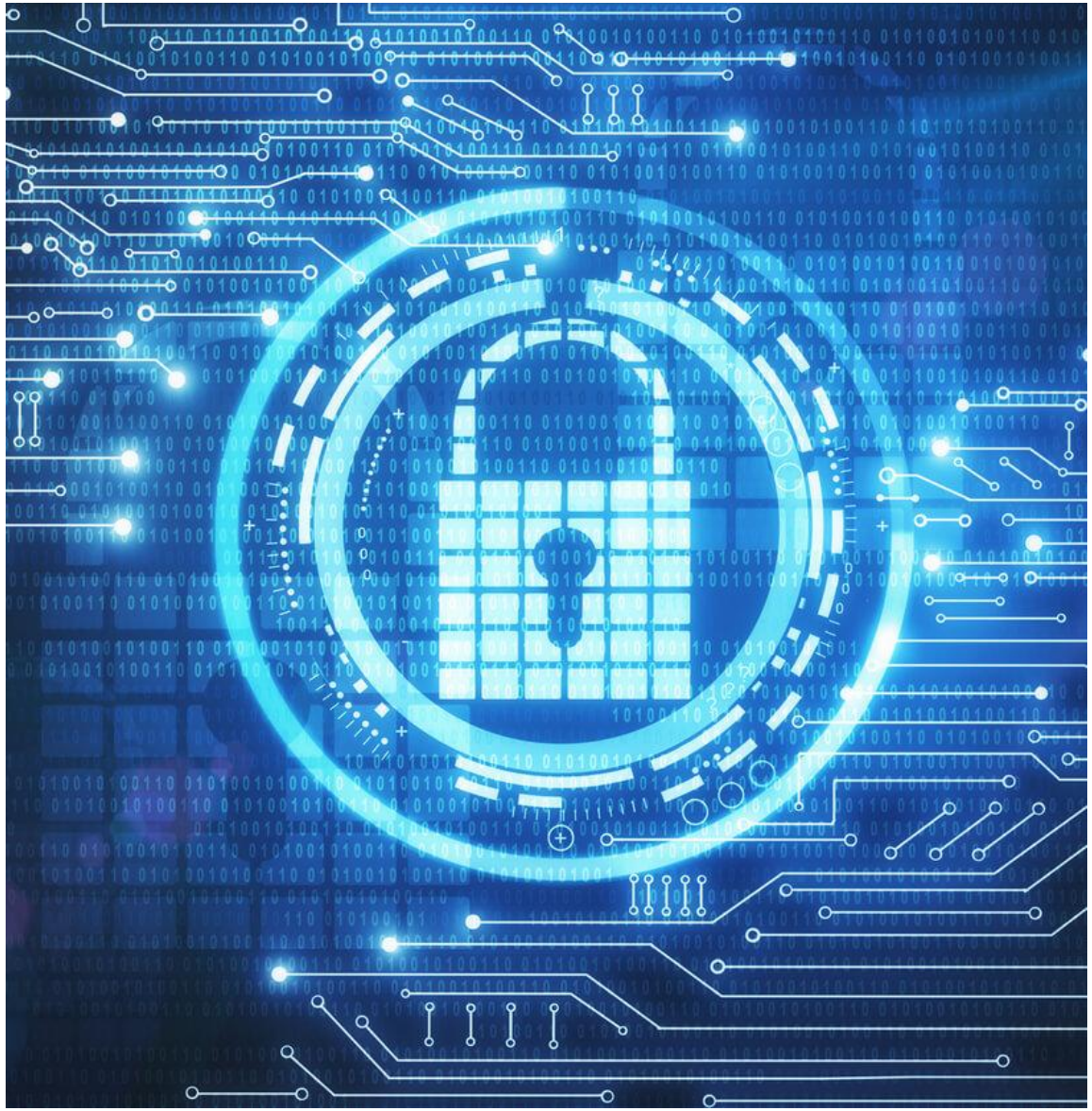
ENCRIPTACIÓN SIMÉTRICA



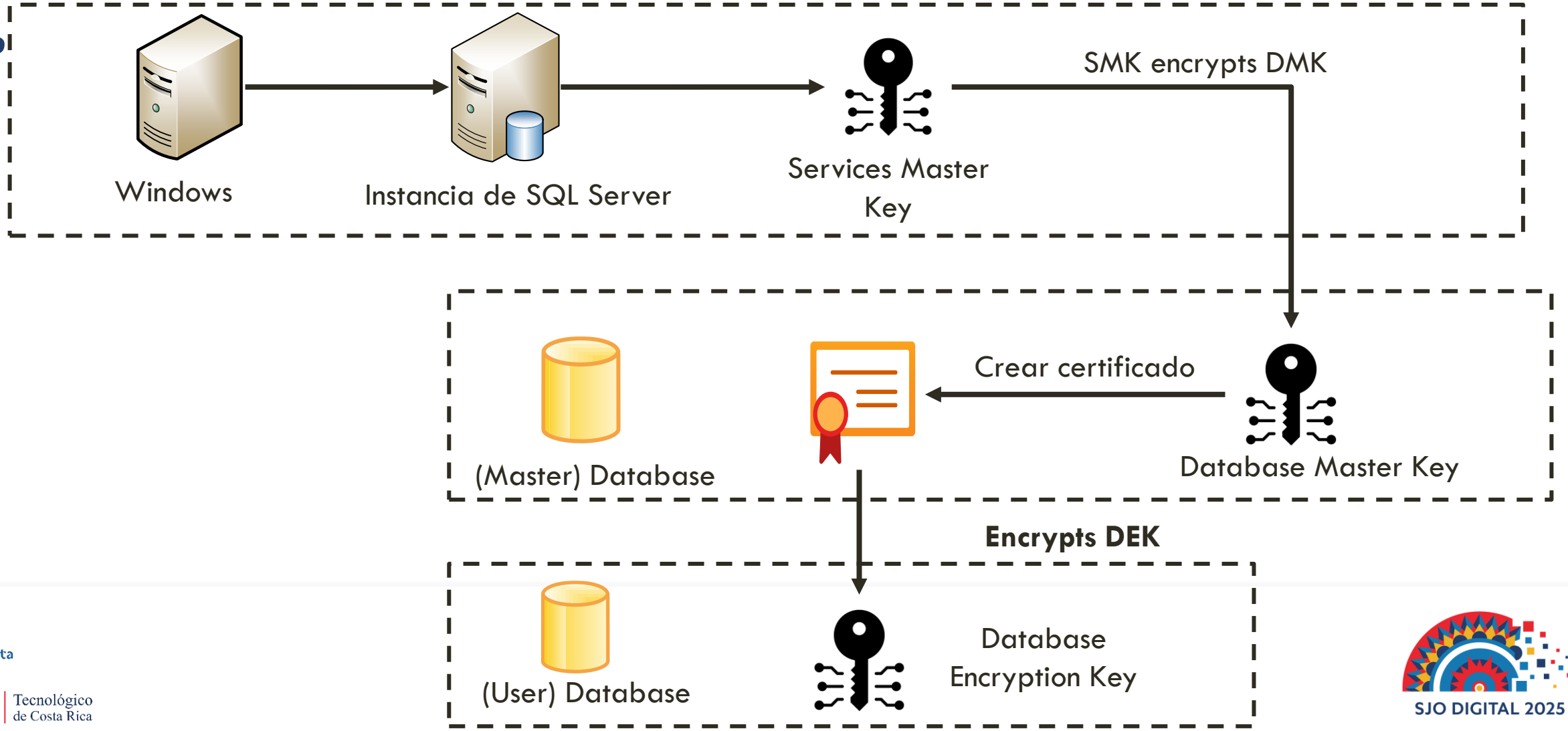
ENCRIPTACIÓN ASIMÉTRICA

ENCRIPTACIÓN POR CERTIFICADOS

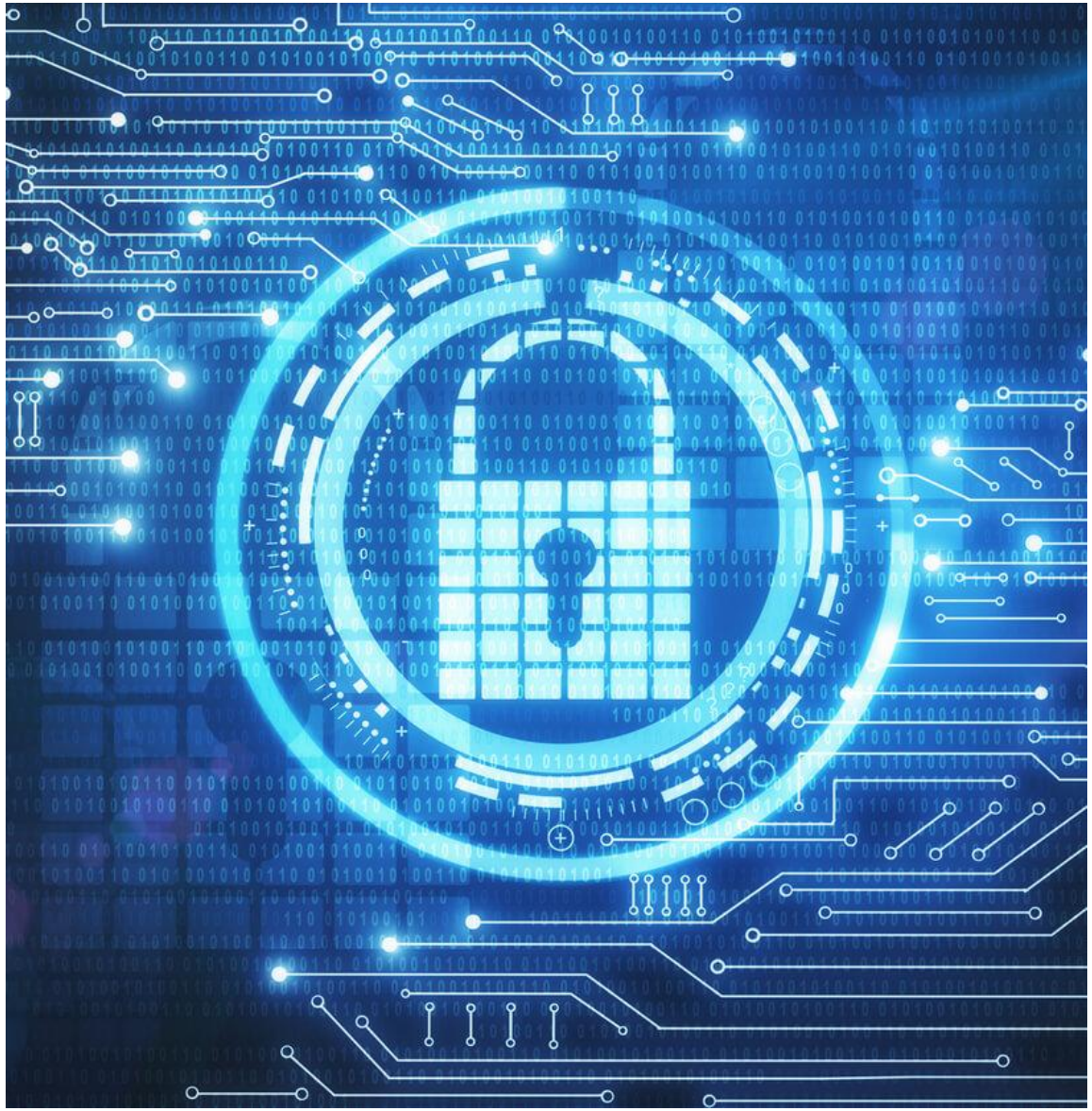
ARQUITECTURA DE ENCRIPTACIÓN



ARQUITECTURA DE ENCRIPTACIÓN DE LAS BASES DE DATOS



ENCRIPTACIÓN DE COLUMNAS



ENCRIPTAR UNA COLUMNA YA CREADA

HASHBYTES

Función de SQL utilizada para devolver el hash según el algoritmo de su entrada en SQL.

HASHBYTES ('<algorithm>', { @input | 'input' })

<algorithm>::= MD2 | MD4 | MD5 | SHA | SHA1 | SHA2_256 | SHA2_512

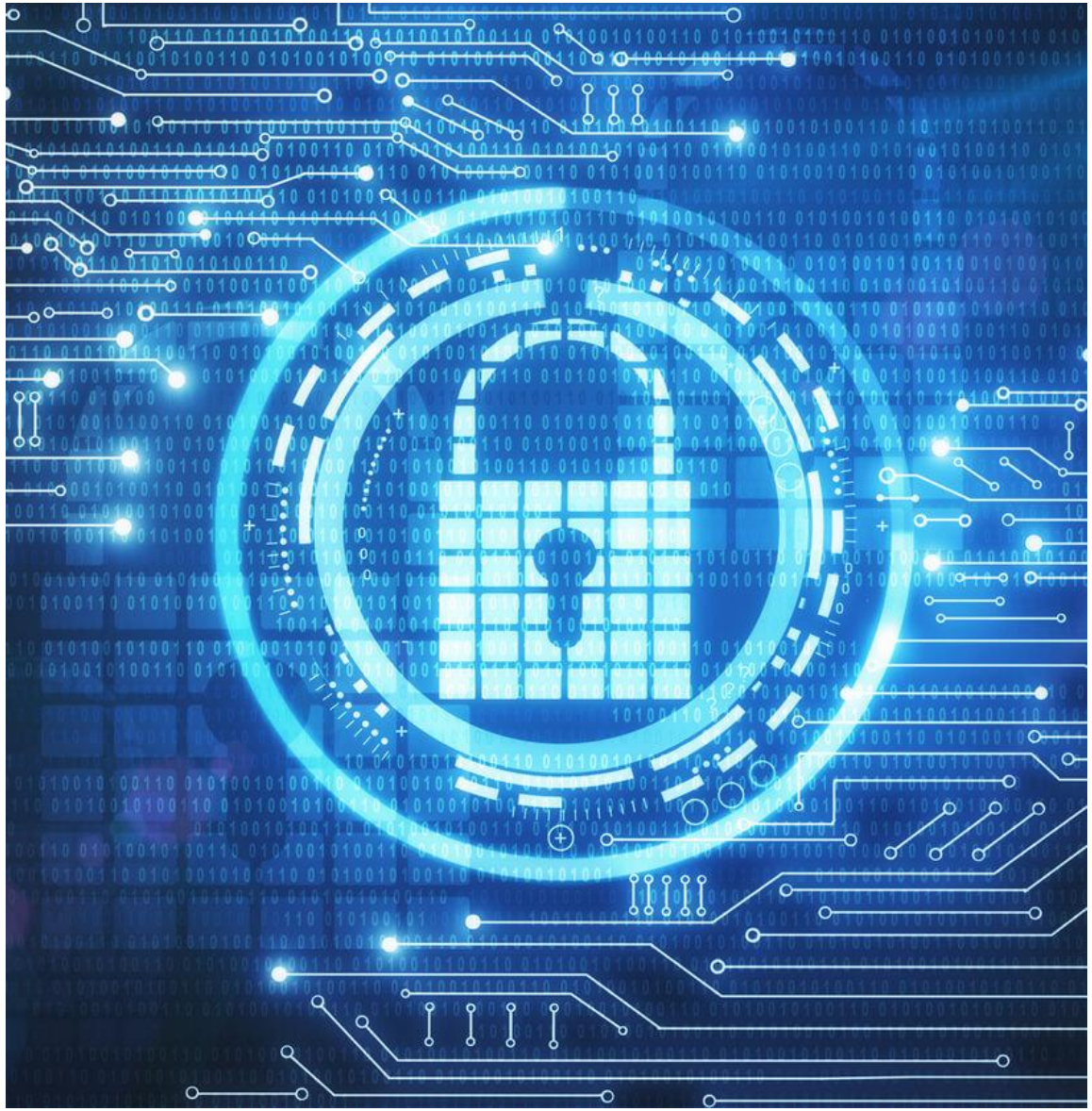

DEMO

ENCRIPTAR UNA COLUMNA YA CREADA

Caso: El nuevo auditor de la empresa identifico que la tabla de **usuarios** tiene el campo de **contraseña** a la vista y las personas con acceso a la tabla pueden ver la contraseña de los usuarios.

Solicitud: Actualizar el campo o columna de **contraseña** de la tabla **usuarios** por medio de una encriptación al registro.

ENCRIPTACIÓN DE COLUMNAS CON LLAVES SIMETRICAS



ENCRIPTAR UNA COLUMNA UTILIZANDO LLAVES SIMETRICAS

Este método es adecuado para proteger datos sensibles, como números de tarjetas de crédito, contraseñas o información confidencial. La encriptación de claves simétricas implica el uso de una misma clave para encriptar y desencriptar los datos.

ENCRIPTAR UNA COLUMNA UTILIZANDO LLAVES SIMETRICAS

- Método de encriptación de columnas de las bases de datos:

1. Crear una llave simétrica (**CREATE SYMMETRIC KEY** <Nombre Llave>).
2. Apertura la llave simétrica (**OPEN SYMMETRIC KEY** <Nombre Llave> **DECRYPTION BY PASSWORD** <Contraseña>)
3. Encriptar los valores a trabajar (**ENCRYPTBYKEY(KEY_GUID**(<Nombre Llave>), <Valor insertar o actualizar>)
4. O desencriptar los valores a trabajar **DECRYPTBYKEY**(<columna a Desencriptar>))
5. Cerrar la llave simétrica (**CLOSE SYMMETRIC KEY** <Nombre Llave>)

ENCRIPTAR UNA COLUMNA UTILIZANDO LLAVES SIMETRICAS

Consideraciones:

1. Proteger la clave maestra y el certificado, ya que comprometerlos podría exponer todos los datos encriptados.
2. La encriptación y desencriptación tiene un impacto en el rendimiento, espacialmente si se procesan grandes volúmenes de datos.
3. Considerar el diseño de la tabla, ya que utiliza campos tipo datos binarios (**VARBINARY**) para almacenar datos encriptados

Primus Data

TEC | Tecnológico de Costa Rica

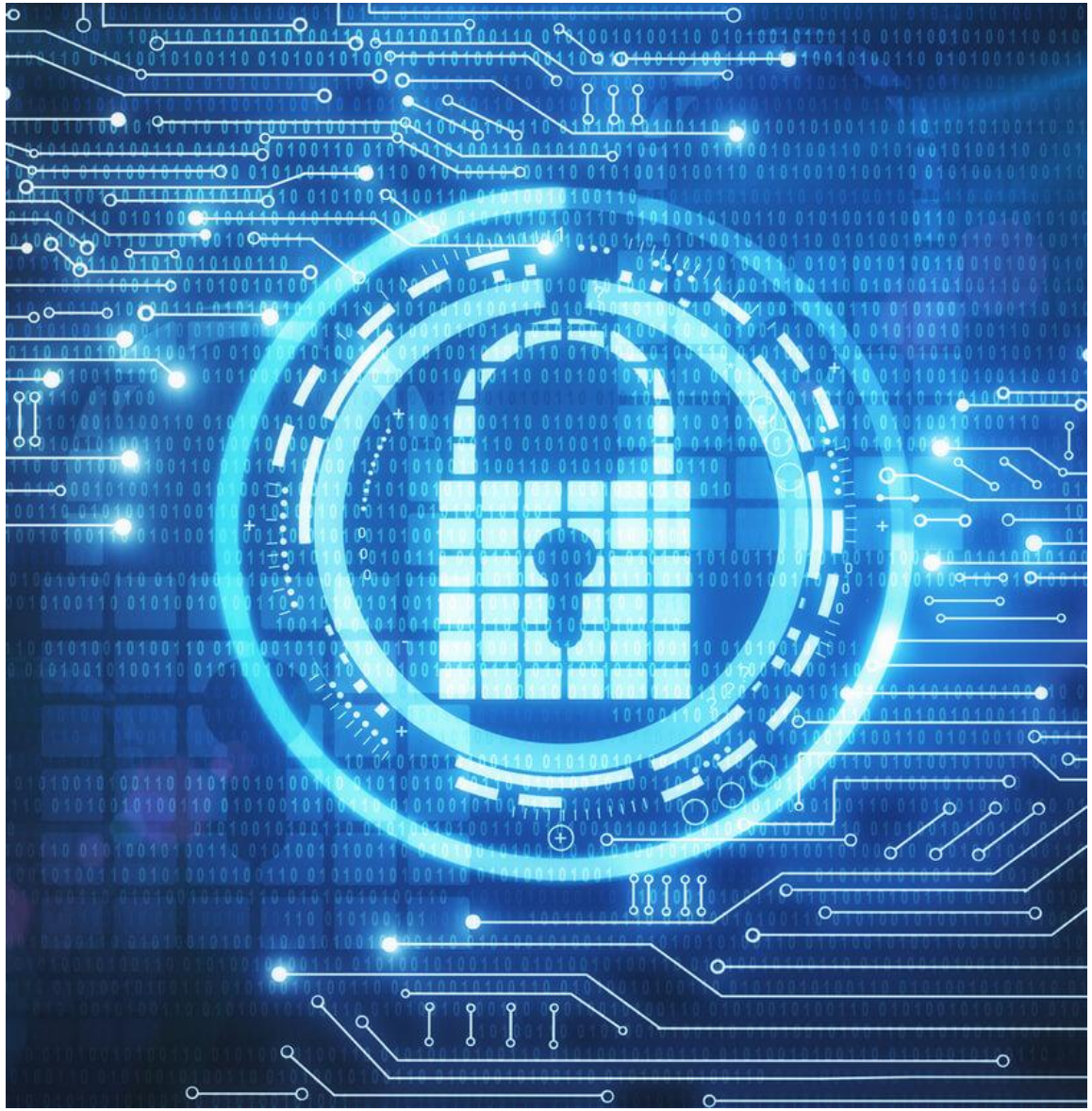
SJO DIGITAL 2025

ENCRIPTAR UNA COLUMNA UTILIZANDO LLAVES SIMETRICAS

Caso: El gerente de recursos humanos de la empresa, solicito a la gerencia de IT, buscar un medio para que los registros de **salario de los colaboradores** de la empresa solo puedan verse por **recursos humanos**.

Solicitud: Crear una llave simétrica para poder insertar, visualizar y actualizar los registros de salarios de los colaboradores.

ENCRIPTACIÓN CON LLAVES SIMETRICAS Y CERTIFICADOS



ENCRIPTAR COLUMNAS CON LLAVE SIMÉTRICAS Y CERTIFICADO

Consideraciones:

1. Proteger la clave maestra y el certificado, ya que comprometerlos podría exponer todos los datos encriptados.
2. La encriptación y desencriptación tiene un impacto en el rendimiento, espacialmente si se procesan grandes volúmenes de datos.
3. Considerar el diseño de la tabla, ya que utiliza campos tipo datos binarios (**VARBINARY**) para almacenar datos encriptados

ENCRIPTAR COLUMNAS CON LLAVE SIMÉTRICAS Y CERTIFICADO

Método de encriptación de columnas con certificado:

1. Crear la **Master Key de encriptación (**`CREATE MASTER KEY ENCRYPTION BY PASSWORD = <Contraseña>`**).**
2. Crear el **certificado de encriptación** (`CREATE CERTIFICATE <Nombre Certificado> WITH SUBJECT = <Descripción Certificado>`).
3. Crear una llave simétrica (**CREATE SYMMETRIC KEY** <Nombre Llave> **WITH ALGORITHM =** <Algoritmo encriptación> **ENCRIPTION BY CERTIFICATE** <Nombre Certificado>).
4. Abrir la llave simétrica (**OPEN SYMMETRIC KEY** <Nombre Llave Simétrica> **DECRYPTION BY CERTIFICATE** <Nombre Certificado>);

ENCRIPTAR COLUMNAS CON LLAVE SIMÉTRICAS Y CERTIFICADO

Método de encriptación de columnas con certificado:

5. Encriptar los valores a trabajar (**ENCRYPTBYKEY(KEY_GUID**(<Nombre Llave>), <Valor insertar o actualizar>)
6. O desencriptar los valores a trabajar **DECRYPTBYKEY**(<columna a Desencriptar>))
7. Cerrar la llave simétrica (**CLOSE SYMMETRIC KEY** <Nombre Llave>)

ENCRIPTAR COLUMNAS CON LLAVE SIMÉTRICAS Y CERTIFICADO

Consideraciones:

1. Proteger la clave maestra y el certificado, ya que perderlos hará que los datos encriptados sean inaccesibles.
2. La encriptación y desencriptación tiene un impacto en el rendimiento, utilizar solo en las columnas que realmente necesitan protección.
3. Considerar el diseño de la tabla, ya que utiliza campos tipo datos binarios (VARBINARY) para almacenar datos cifrados.

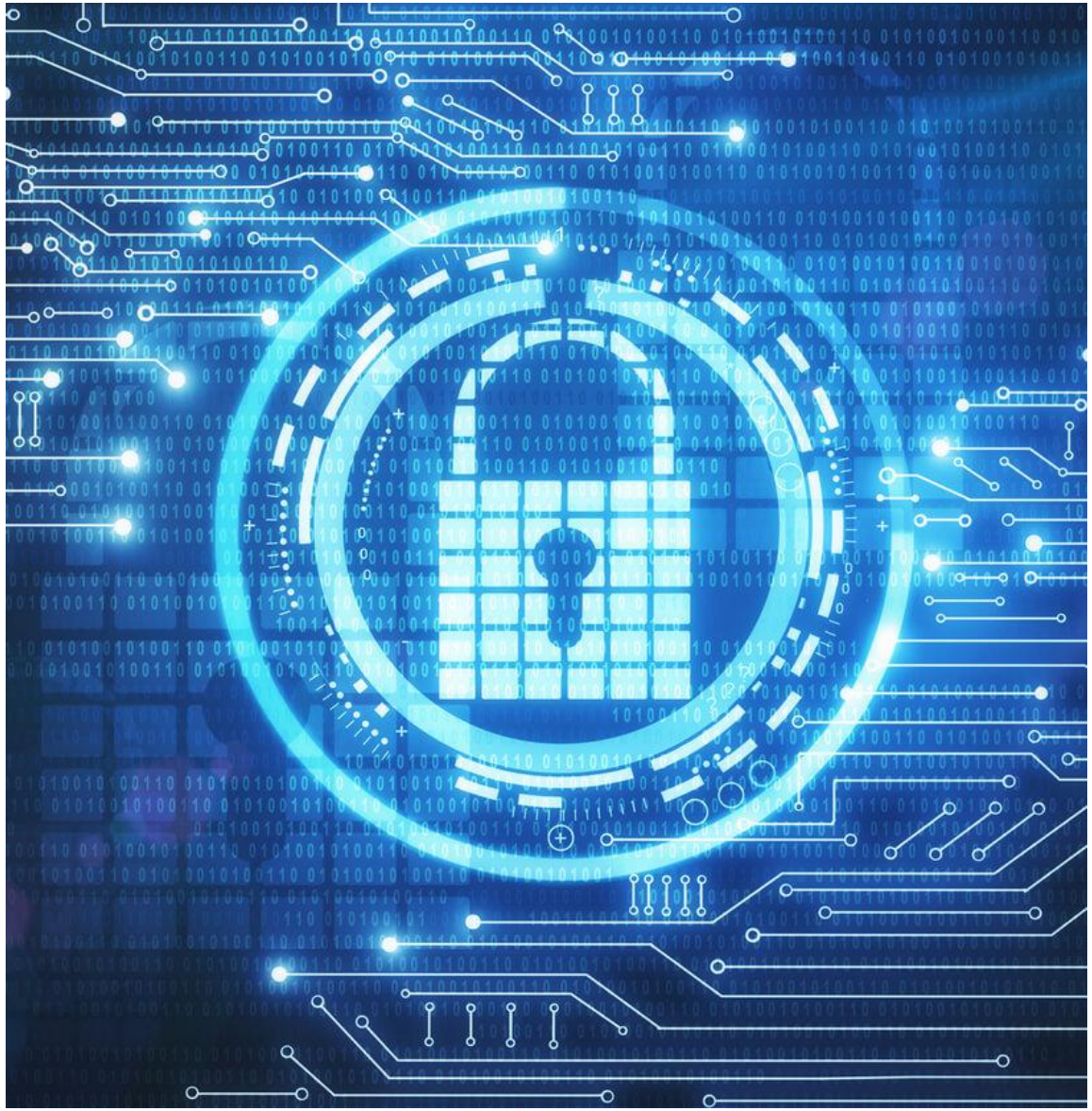

DEMO

ENCRIPTAR COLUMNAS CON LLAVE SIMÉTRICAS Y CERTIFICADO

Caso: El gerente financiero de la empresa, solicito al personal de IT buscar un medio para que los registros de cuentas bancarias o números de tarjeta de crédito de los clientes solo puedan verse por el personal correspondiente.

Solicitud: Crear una llave simétrica por medio de certificado para poder insertar, visualizar y actualizar los registros de cuentas bancarias de los clientes.

ENCRIPTACIÓN DE LAS BASES DE DATOS



ENCRIPTAR LOS ARCHIVOS FÍSICOS DE BASE DE DATOS

Para tener seguridad en los archivos físicos de las bases de datos, es necesario definir un proceso de encriptación de las bases de datos importantes para la empresa.

ENCRIPTAR LOS ARCHIVOS FÍSICOS DE BASE DE DATOS

Método de encriptación de las bases de datos:

1. Crear la Master Key de encriptación **CREATE MASTER KEY ENCRYPTION** .
2. Crear el certificado de encriptación **CREATE CERTIFICATE** .
3. Crear la encriptación en cada una de las Bases de Datos de usuario utilizando el certificado (**CREATE DATABASE ENCRYPTION KEY, ENCRYPTION BY SERVER CERTIFICATE**).
4. Respaldar llaves y certificados.

Primus Data

TEC | Tecnológico de Costa Rica

SJO DIGITAL 2025

ENCRIPTAR LOS ARCHIVOS FÍSICOS DE BASE DE DATOS

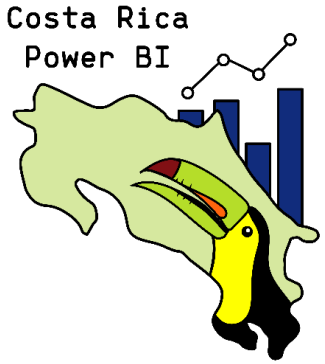
Caso: El auditor en sistema de la empresa, identifico que los archivos físicos de las bases de datos pueden estar expuestos en caso de robo, se solicita al DBA buscar los medios necesarios para reforzar la seguridad de estos archivos de base de datos.

Solicitud: Crear una llave de encriptación y aplicarle esta encriptación a cada una de las bases de datos de la Instancia de SQL Server.

RECURSOS

- **Hashbytes** https://learn.microsoft.com/es-es/sql/t-sql/functions/hashbytes-transact-sql?view=sql-server-ver16
- **Master Key Encription** https://learn.microsoft.com/es-es/sql/t-sql/statements/create-master-key-transact-sql?view=sql-server-ver16
- **Create Certificate** https://learn.microsoft.com/es-es/sql/t-sql/statements/create-certificate-transact-sql?view=sql-server-ver16
- **Create database encryption key** https://learn.microsoft.com/es-mx/sql/t-sql/statements/create-database-encryption-key-transact-sql?view=sql-server-ver16

CON EL APOYO DE



Primus Data

TEC | Tecnológico de Costa Rica

SJO DIGITAL 2025

ENCRIPTANDO LOS DATOS EN SQL SERVER

Wilmer Edgardo Martinez

SJO DIGITAL 2025

Primus Data

TEC | Tecnológico de Costa Rica

www.linkedin.com/in/wilmer-edgardo-martinez-1a00833a

SJO DIGITAL 2025