

	Política de Enmascaramiento de Datos	Código:	SGSI-A8-D6PO14
		Versión:	02
		Fecha:	11/02/2025
		Página:	Portada
		CSI:	

DigiPro, S.A. de C.V.

	Política de Enmascaramiento de Datos	Código:	SGSI-A8-D6PO14
		Versión:	02
		Fecha:	11/02/2025
		Página:	2 de 6
		CSI:	

Hoja de revisión.

Este documento fue creado conforme a los requerimientos institucionales, revisado por el área de Control y Cumplimiento y aprobado por la Dirección de Tecnologías de Información.

Estamos de acuerdo con su contenido e implementación, en caso de haber cualquier modificación o adición a este documento, es responsabilidad del área emisora indicar la modificación o adición, previa aprobación de las áreas involucradas para evitar errores, incrementar el control interno y/o mejorar la productividad de los departamentos involucrados.

Elaborado por:	Firma electrónica
Viridiana Ortega Sánchez – Gerente de Base de Datos	
Revisado por:	Firma electrónica
Carla Évora Dominguez – Analista de Control y Cumplimiento	
Aprobado por:	Firma electrónica
Mariela Corderí Castillo – Dirección de Tecnologías de Información	

Control de Cambios		
Versión	Cambios realizados	Fecha
01	Documento de nueva creación.	22/01/2025
02	Se menciona la cláusula contractual referente al enmascaramiento de datos.	11/02/2025

Tabla de contenido

Política de Enmascaramiento de Datos.4

1 Objetivo.4

2 Desarrollo.4

 2.1 Gestión del área de Base de Datos para el Enmascaramiento de Datos.....4

 2.2 Tipos de Enmascaramiento.4

 2.3 Ejemplo de enmascaramiento de datos.4

3 Consideraciones.....5

4 Documentos relacionados.6

5 Cumplimiento.6

	Política de Enmascaramiento de Datos	Código:	SGSI-A8-D6PO14
		Versión:	02
		Fecha:	11/02/2025
		Página:	4 de 6
		CSI:	

Política de Enmascaramiento de Datos.

1 Objetivo.

Establecer un tratamiento de enmascaramiento de datos sensibles, en caso de restauración de bases de datos de clientes.

2 Desarrollo.

2.1 Gestión del área de Base de Datos para el Enmascaramiento de Datos.

Objetivo
Dar a conocer el tratamiento de información confidencial cuando se recibe una solicitud de restauración de base de datos.

2.2 Tipos de Enmascaramiento.

A continuación, se muestra el tratamiento de las columnas que especifican contiene información confidencial.

Tipo de dato	Valor para enmascarar
Cadena	X
numéricos	0
Fechas	1900-01-01 00:00:00.0000000
Binarios	0

2.3 Ejemplo de enmascaramiento de datos.

Los siguientes ejemplos son definiciones básicas a tipos de datos específicos y se utilizarán, a menos que el cliente especifique un enmascaramiento diferente.

Función	Descripción	Ejemplos
Email	Método de enmascaramiento que expone la primera letra de una dirección de correo electrónico y el sufijo constante ".com", en el formato de una dirección de correo electrónico.	aXXX@XXXX.com
Fechas	Se puede enmascarar ciertos elementos de una fecha (año, mes, día, hora, minuto, etc)	1900-01-01

	Política de Enmascaramiento de Datos	Código:	SGSI-A8-D6PO14
		Versión:	02
		Fecha:	11/02/2025
		Página:	5 de 6
		CSI:	

Función	Descripción	Ejemplos
Random	Una función de enmascaramiento aleatorio que se puede usar con cualquier tipo numérico a fin de enmascarar el valor original con uno aleatorio dentro de un intervalo especificado.	MaXXX LoXXX HerXXXXXX
Teléfonos	Los teléfonos se pueden enmascarar dejando los 2 primeros números o los 4 últimos.	55XXXXXX o XXXXXX2692

3 Consideraciones.

Se deberá tener en cuenta las siguientes consideraciones para el enmascaramiento de datos:

- **Especificación de Enmascaramiento.**

Deberán indicar las Tablas y campos con información sensible, para la generación del enmascaramiento. En caso de no especificar los campos en una restauración, se tomarán como datos no sensibles y no se aplicará ninguna regla de enmascaramiento.

DIGIPRO no se hace responsable de las tablas y columnas no especificadas que no se haya hecho el tratamiento de enmascaramiento, así mismo no se hace responsable de las columnas especificadas incorrectamente por el usuario o cliente. Para más información, se puede consultar la **Cláusula contractual referente al Enmascaramiento de Datos**.

- **Permisos.**

Es importante administrar adecuadamente los permisos en la base de datos y seguir el principio de mínimos permisos requeridos. Además, se debe considerar el tener habilitada la auditoría para hacer seguimiento de todas las actividades que se realizan en la base de datos.

- **Modificación e Inserción de Datos.**

La creación de una máscara en una columna no impide que se efectúen actualizaciones en ella. De modo que, aunque los usuarios recibirán datos enmascarados cuando realicen una consulta en una columna enmascarada, ellos mismos podrán actualizar los datos si cuentan con permisos de escritura. Aun así, se debe usar una directiva de control de acceso adecuada para limitar los permisos de actualización.

El uso de SELECT INTO o INSERT INTO para copiar datos de una columna enmascarada en otra tabla da como resultado datos enmascarados en la tabla de destino (suponiendo que la exporte un usuario sin privilegios UNMASK).

	Política de Enmascaramiento de Datos	Código:	SGSI-A8-D6PO14
		Versión:	02
		Fecha:	11/02/2025
		Página:	6 de 6
		CSI:	

- Importación y Exportación.

El enmascaramiento dinámico de datos se aplica al ejecutar la importación y exportación de SQL Server. Una base de datos que contiene columnas enmascaradas da como resultado un archivo de datos exportado con datos enmascarados (suponiendo que lo exporte un usuario sin privilegios UNMASK), y la base de datos importada contendrá datos enmascarados estáticamente.

4 Documentos relacionados.

- Cláusula contractual referente al Enmascaramiento de Datos

5 Cumplimiento.

- ISO / IEC 27001:2022 / A.8 Controles tecnológicos / A.8.11 Enmascaramiento de datos.