

POLÍTICA DE POLÍTICA DE ANONIMIZACIÓN Y SEUDONIMIZACIÓN	PRO-14
	Revisión 00

REV.	FECHA	DESCRIPCIÓN

ELABORADO POR:	REVISADO Y APROBADO POR:
	DIRECCIÓN
FECHA: 08/05/2018	

POLÍTICA DE POLÍTICA DE ANONIMIZACIÓN Y SEUDONIMIZACIÓN	PRO-14
	Revisión 00

ÍNDICE

- 1.-OBJETO
- 2.-ALCANCE
- 3.-RESPONSABILIDADES
- 4.-DESCRIPCIÓN
- 5.-ARCHIVO Y CODIFICACIÓN DE REGISTROS
- 6.-DIAGRAMA DE FLUJOS
- 7.-ANEXO
- ANEXO 1.-

1.-OBJETO

POLÍTICA DE POLÍTICA DE ANONIMIZACIÓN Y SEUDONIMIZACIÓN	PRO-14
	Revisión 00

El propósito de este documento es proporcionar una guía a la empresa para el establecimiento y mantenimiento de la seudonimización y la anonimización de los datos personales.

Los usuarios de estos documentos son el delegado de protección de datos, el responsable de seguridad TI, y los representantes de las unidades de negocio responsables del tratamiento de datos personales

2.-ALCANCE

Este procedimiento es aplicable a todo el personal de la empresa.

3.-DEFINICIONES

“**Pseudonymization**” es el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

“**Anonymization**” es el tratamiento de datos personales con el objetivo de prevenir de manera irreversible la identificación de la persona física con quien se relacionan. Los datos pueden considerarse anonimizados cuando no permite la identificación de las personas físicas con las que se relacionan, y cuando no es posible identificar a una persona física a partir de los datos mediante un tratamiento posterior de esos mismos datos, o mediante el tratamiento de esos datos junto con otros datos que están disponibles o que probablemente estén disponibles. Para la mayoría de las empresas, la anonimización completa no es factible

4.-DESCRIPCIÓN

Seudonimización y anonimización de datos personales

Responsable de Seguridad debe decidir si las técnicas de seudonimización y la anonimización son apropiadas para determinadas actividades de tratamientos de datos. Responsable de Seguridad es responsable de elegir la tecnología más apropiada para la implementación de estas técnicas.

POLÍTICA DE POLÍTICA DE ANONIMIZACIÓN Y SEUDONIMIZACIÓN	PRO-14
	Revisión 00

Más abajo se encuentra una lista no exhaustiva de las técnicas de anonimización y seudonimización.

4.1. Anonimización

El objetivo de la anonimización de los datos personales es imposibilitar la identificación de una persona física en el conjunto de datos anonimizados, incluso con la ayuda de los datos originales, por lo que los datos anonimizados no se consideran datos personales. Es importante señalar que no existe un estándar prescriptivo para la anonimización dentro de los marcos legales de la UE, por lo que la elección de utilizar métodos de anonimización apropiados recae sobre el delegado de protección de datos o responsable de seguridad.

La Empresa utilizará los siguientes métodos teniendo en cuenta el grado de riesgo y el uso previsto de los datos.

- Sustitución de directorio: modificación del nombre de las personas físicas integradas en los datos, manteniendo la coherencia entre los valores, como "código postal + ciudad", "edad + sexo".
- Codificación: Implica una mezcla u ofuscación de letras. El proceso a veces puede ser reversible.

Por ejemplo: Robert podría convertirse en Betrör.

- Enmascaramiento: permite que una parte de los datos se oculte con caracteres aleatorios u otros datos.
- Borrosidad: una aproximación de los valores de los datos para volver obsoleto su significado y o imposibilitar la identificación de los individuos.
- Privacidad diferencial: este método se puede usar siempre que la empresa le brinde a un tercero acceso a un conjunto de datos anónimos. Una copia de los datos originales permanece en la Empresa, y el destinatario externo solo recibe un conjunto de datos anónimos.
- Agregación: un interesado se agrupa con varios otros interesados que comparten algunos o todos los datos personales.

4.2. Seudonimización

POLÍTICA DE POLÍTICA DE ANONIMIZACIÓN Y SEUDONIMIZACIÓN	PRO-14
	Revisión 00

La seudonimización pretende mejorar la privacidad mediante la sustitución de los campos de identificación dentro de un registro de datos por uno o más identificadores artificiales o seudónimos. Como tal, la seudonimización reduce, pero no elimina por completo, la capacidad de vincular un conjunto de datos con la identidad de un interesado.

El delegado de protección de datos junto con el Responsable de Seguridad establecerá los métodos apropiados de seudonimización tales como:

- **Encriptado (utilizando una clave secreta):** Los datos son encriptados con el uso de una clave secreta. El titular de la clave secreta puede volver a identificar fácilmente a los interesados desenscriptando el conjunto de datos.
- **Funciones hash:** Se utilizan para asignar datos de cualquier tamaño a códigos de un tamaño fijo (tenga en cuenta que existen técnicas de hash múltiples (por ejemplo, hashes salados, hashes con clave, etc.).
- **Tokenización:** es el proceso de sustitución de un elemento de datos confidenciales por un equivalente no sensible, denominado token. El token es una referencia (ej. un identificador) que se correlaciona con los datos sensibles a través de un sistema de tokenización. El sistema de tokenización proporciona a las aplicaciones de tratamiento de datos la autoridad y las interfaces para solicitar tokens o destokenizar a los datos sensibles

5.-ARCHIVO Y CODIFICACIÓN DE REGISTROS

No aplica