INEI INSTITUTO NACIONAL DE ESTADISTICA E INFORMATICA

## OFICINA TÉCNICA DE INFORMÁTICA

# POLÍTICAS

## "POLÍTICA DEL USO DE CONTROLES CRIPTOGRAFICOS DE BASE DE DATOS"

**Código: POL-006-OTIN-2018**
**Versión 1.0.0**

| POLÍTICA | | | |
|---|---|---|---|
| **NOMBRE DE LA POLÍTICA:** POLÍTICA DEL USO DE CONTROLES CRIPTOGRAFICOS DE BASE DE DATOS | | | |
| **CODIGO:** POL-006-OTIN-2018 | | | **VERSION:** 1.0.0 |
| **PROCESO AL QUE PERTENECE:** Gestión de las Seguridad | | | |
| **Elaborado por:** Unidad Funcional de Calidad, Procesos y Seguridad de la Información | **Coordinado con:** Unidad Funcional de Producción | Unidad Funcional de Infraestructura | **Aprobado por:** Director Técnico de la Oficina Técnica de Informática |
| **Nombre:** Ing. Katherine Montenegro Julcapoma | **Nombre:** Jannet Martinez Padilla | **Nombre:** Ing. Juan Padilla Padilla | **Nombre:** Ing. CIP Manuel Matos Alvarado |
| **Fecha:** 19/11/2018 | **Fecha:** 19/11/2018 | **Fecha:** 19/11/2018 | **Fecha:** 27/11/2018 |
| **Firma** | **Firma** | **Firma** | **Firma** |
| | | | Ing. CIP Manuel Amador Matos Alvarado<br>Director Técnico<br>Oficina Técnica de Informática |

# TABLA DE CONTENIDO

# "POLÍTICADEL USO DE CONTROLES CRIPTOGRAFICOS DE BASE DE DATOS"

## 1. OBJETIVO

El objetivo del presente documento es definir reglas para el uso de los controles y claves criptográficas para proteger la confidencialidad, integridad, autenticidad e inviolabilidad de la información.

## 2. FINALIDAD

Establecer los controles criptográficos para proteger la información en INEI permitiendo que la información clasificada como reservada y/o confidencial reciba un tratamiento especial en su procesamiento, a través de la aplicación mecanismos criptográficos que permitan minimizar los riesgos y lograr que la información se encuentre segura.

## 3. ALCANCE

Este documento se aplica a todos los sistemas e información encontrados dentro del alcance del SGSI. Además es aplicable a todos los colaboradores de INEI que mantengan contacto directo con la información reservada o confidencial, para el uso de algoritmos criptográficos como herramientas de control, protección de la confidencialidad e integridad de la información, así como la documentación y resguardo de estos.

## 4. REFERENCIAS

- Norma ISO/IEC 27001, capítulos A.10.1.1, A.10.1.2, A.18.1.5
- Política de seguridad de la información
- Alcance del SGSI
- Política de Clasificación de la Información
- Lista de requisitos legales, normativos, contractuales y de otra índole
- Ley de protección de datos personales. LEY Nº 29733

## 5. ABREVIATURAS Y DEFINICIONES

Las siguientes abreviaturas y definiciones son aplicables para el propósito de este procedimiento:

- **SGSI:** Sistema de Gestión de Seguridad de la Información
- **OTIN:** Oficina Técnica de Informática
- **Algoritmo:** Conjunto ordenado de operaciones sistemáticas que permite hacer un cálculo y hallar la solución de un tipo de problemas.
- **Enmascaramiento:** Es el proceso mediante el cual se cambian ciertos elementos de los datos de un almacén de datos, cambiando su información pero consiguiendo que la estructura permanezca similar, de forma que la información sensible quede protegida.

- **Encriptación de datos:** es el proceso mediante el cual cierta información o texto sin formato es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación.
- **Claves criptográficas:** Es una secuencia de números o letras mediante la cual, en criptografía, se especifica la transformación del texto plano en texto cifrado, o viceversa.
- **Cifrado de clave pública:** El cifrado de clave pública utiliza un par de claves relacionadas matemáticamente. Un mensaje cifrado con la primera clave debe descifrarse con la segunda clave y un mensaje cifrado con la segunda clave debe descifrarse con la primera clave. Cada participante en un sistema de claves públicas dispone de un par de claves. Una clave se designa como clave privada y se mantiene secreta. La otra clave se distribuye a quien lo desee; esta clave es la clave pública. Cualquier usuario puede cifrar un mensaje utilizando su clave pública, pero sólo el propietario de la clave privada puede leerlo. Cuando recibe el mensaje, lo descifra utilizando la clave privada.
- **Cifrado de clave privada:** Los sistemas de cifrado de clave privada utilizan una sola clave que comparten el remitente y el destinatario. Ambos deben poseer la clave; el remitente cifra el mensaje mediante la clave y el destinatario descifra el mensaje con la misma clave. Para poder establecer una comunicación privada, tanto el remitente como el destinatario deben mantener la clave en secreto.

## 6. POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

El Administrador de Base de datos en coordinación con los programadores y el Jefe del proyecto, deben encargarse de la encriptación de los datos e información confidencial, sensible o de carácter personal del INEI que se encuentre en formato digital, de acuerdo a los requerimientos definidos y autorizados, a los niveles de clasificación de la información definidos y a la normatividad vigente.

De acuerdo a la información de cada Proyecto del INEI, el Jefe de Proyecto en coordinación con el Oficial de Seguridad de la Información del INEI podrá aprobar la aplicación de un software criptográfico para los archivos en los sistemas de información y recursos tecnológicos que los usuarios requieran proteger de acuerdo a su rol, función y responsabilidad que tienen sobre la información que utilizan y administran dentro del INEI.

## 7. POLÍTICAS ESPECÍFICAS

- Se deben emplear herramientas de criptografía para la protección de la información clasificada como confidencial de conformidad a la Ley Nº 29733.
- El administrador de Base de datos deberá definir los algoritmos criptográficos que se podrán emplear al interior del INEI, considerando el tipo y la calidad del algoritmo criptográfico utilizado así como también la longitud de las claves criptográficas.
- Se utilizarán controles criptográficos en los siguientes casos:
  - ✓ Para la protección de claves de acceso a los sistemas, datos, información y servicios.
  - ✓ Para la transmisión de información que contenga datos de carácter sensible, confidencial o datos personales, dentro y fuera de la institución.

- ✓ En la protección de la información a resguardar cuando alguna Dirección Nacional o Técnica o el propietario de la información lo requiera, o cuando lo establezca el Comité de Gestión de Seguridad de la Información del INEI.

### 7.1. ADMINISTRACIÓN DE LAS CLAVES CRIPTOGRÁFICAS

- La unidad Funcional de Infraestructura Tecnológica bajo la supervisión del Oficial de Seguridad de la Información del INEI es la única responsable de la administración de las claves criptográficas utilizadas.
- Para el cifrado y la generación de firmas digitales, se debe emplear alguna técnica para el cifrado de clave. Se sugiere: técnicas de clave secreta y técnicas de clave pública por ser las más empleadas.
- Todas las claves criptográficas deben ser protegidas contra pérdida, divulgación, modificación y destrucción. En el caso de olvido, pérdida, corrupción o destrucción, debe existir un método de recuperación establecido por la Unidad Funcional de Infraestructura Tecnológica.
- De corresponder, si los datos que se encuentran en algún medio de almacenamiento se encuentran cifrados (incluso en modo de respaldo), las claves de cifrado deben ubicarse en otro medio de almacenamiento por separado.
- El Administrador de BD es el responsable de establecer las siguientes reglas sobre la gestión de claves en las bases de datos:
  - ✓ Activación y distribución de claves criptográficas.
  - ✓ Definición del plazo para el uso de las claves y de su actualización periódica (de acuerdo con la evaluación de riesgos).
  - ✓ Archivo de claves inactivas que son necesarias para archivos electrónicos encriptados.
  - ✓ Destrucción de claves.
- Las claves son administradas por sus propietarios, en conformidad con las reglas mencionadas precedentemente.

## 8. BUENAS PRÁCTICAS PARA EL USO DE CONTROLES CRIPTOGRAFICOS

### 8.1. ENMASCARAMIENTO DE DATOS:

- El jefe o el analista del proyecto debe identificar y catalogar los diversos tipos de datos que pueden ser confidenciales elaborando una lista completa de los elementos de datos de cada Proyecto de la Institución.
- Una vez identificados los datos, se requiere determinar si existe información confidencial, la ubicación de los datos y la técnica ideal de enmascaramiento de datos de acuerdo a la Ley de Protección de datos personales.
- Para la implementación del enmascaramiento se debe tener en cuenta la arquitectura, la planificación adecuada y una mirada a las necesidades futuras de la institución.
- Debe existir un equipo encargado de las pruebas de enmascaramiento de datos para garantizar que las configuraciones de enmascaramiento produzcan los resultados deseados. Si no lo hacen, entonces el DBA restaurará la base

de datos al estado inicial, ajustará los algoritmos de enmascaramiento y completará el proceso de enmascaramiento de datos una vez más.

## 8.2. ENCRIPTACION DE BASE DE DATOS:

- Siempre se debe realizar una copia de seguridad de las bases de datos antes de cifrarlas.
- Las claves de cifrado deben encontrarse almacenadas de forma segura, ya que serán necesarias para eliminar el cifrado. Si ocurre un desastre y se necesitara restaurar la base de datos a otro servidor desde un archivo de copia de seguridad, la copia de seguridad será inútil sin el certificado y la clave privada.
- La máquina física que aloje una base de datos se debe encontrar en un entorno seguro, bloqueado y supervisado para evitar la entrada de personal no autorizado, el acceso o el robo.
- Los registros de auditoria podrán ser revisados regularmente por personas informadas e independientes designadas por el propietario de los datos junto con el Oficial de Seguridad de la Información del INEI para cumplir con los requisitos del propietario de los datos. Estos requisitos y el proceso de revisión deberán estar documentados.

## 8.3. CONTROLES PARA LA ENCRIPTACIÓN DE BASE DE DATOS

De acuerdo con las obligaciones legales y contractuales, la institución debe proteger a los sistemas individuales y a la información, para ello debe hacer uso de los siguientes controles criptográficos, según corresponda:

- **Enmascaramiento (Oracle):** Oculta filas y datos según las concesiones de acceso del usuario.
- **Enmascaramiento (SQL Server):** Enmascara la totalidad o parte de datos confidenciales, como números de identificación nacional, números de tarjetas de crédito, fechas de nacimiento, números de teléfono u otros tipos de información.
- **Encriptación de base de datos/cifrado de datos transparentes (TDE SQL Server):** Realiza el cifrado de E / S en tiempo real y el descifrado de los datos y archivos de registro.
- **Encriptación de base de datos/cifrado de datos transparentes (TDE Oracle):** Función que permite cifrar las columnas de la base de datos y administrar las claves de cifrado.
- **Claves criptográficas:** Proporcionan mecanismos de autenticación y cifrado para aplicaciones y usuarios.

El Administrador de Base de datos es el responsable de redactar instrucciones detalladas sobre el uso de las mencionadas herramientas criptográficas cuando sean aplicables.

# 9. ANEXOS

## 9.1. ANEXO 01: BITÁCORA DE DATOS ENCRIPTADOS

| | | | | Ubicación de datos cifrados | | | | |
|---|---|---|---|---|---|---|---|---|
| N° | Fecha | Responsable | Nombre del Proyecto | Instancia | Esquema | Tabla | Campo | Observaciones |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

## 9.2. ANEXO 02: BITÁCORA DE DATOS ENMASCARADOS

| | | | | Ubicación de datos cifrados | | | | |
|---|---|---|---|---|---|---|---|---|
| N° | Fecha | Responsable | Nombre del Proyecto | Instancia | Esquema | Tabla | Campo | Observaciones |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |