Bansefi
EL BANCO QUE TE INCLUYE

| | |
|---|---|
| Nombre del Documento | **POLÍTICA DE CONTROLES CRIPTOGRÁFICOS** |
| No. de Control | PL-SGSI-17 |
| Versión | 1.3 |
| Vigencia a partir de | |
| Total de Páginas | 7 |
| Macroproceso/ Proceso principal | Administrar la Seguridad de la Información |
| Titular del área responsable del Proceso/ Procedimiento(responsable) | Dirección General Adjunta de Tecnología y Operación |

## AUTORIZACIÓN DEL DOCUMENTO

Esta política fue documentada por personal adscrito a la Dirección General Adjunta de Tecnología y Operación. Cuenta con la opinión favorable del Grupo Estratégico de Seguridad de la Información en su sesión número GESI/01.O/16, celebrada el 01 de julio de 2016.

## AUTORIZACIÓN DEL DOCUMENTO

Autorizado y validado por:

| Nombre | Puesto | Firma |
|---|---|---|
| Guillermina Muñoz Soto | Directora General Adjunta de Tecnología y Operación | |
| Lina Nancy Martínez Ponce | Directora de Contraloría Interna | |
| Ana Laura Hernández Flores | Directora de Administración y Control Integral de Riesgos | |

## Información General

| | | |
|---|---|---|
| **Título:** | **Política de Controles Criptográficos** | |
| **Nombre interno:** | **Política de Controles Criptográficos** | |
| **Fecha Aprobación:** | | |
| **Nivel de confidencialidad:** | Confidencial | |
| | Restringido | |
| | **Uso Interno** | ✓ |
| | Público | |

## Control de cambios

| Versión | Sección | Descripción del Cambio | Fecha |
|---|---|---|---|
| 1.0 | 0 | Creación del Documento | 30-Jun-2016 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Contenido

**CONSIDERACIONES GENERALES** ..... **4**

OBJETIVO ..... 4
ALCANCE ..... 4
MARCO LEGAL DE REFERENCIA ..... 4
VIGENCIA ..... 4
MARCO NORMATIVO ..... 5
RESPONSABLES DE CUMPLIMIENTO ..... 5

**POLÍTICA DE CONTROLES CRIPTOGRÁFICOS** ..... **6**

POLÍTICAS ESPECÍFICAS ..... 6
*Sobre el servicio de no repudiación* ..... *6*
*Sobre la administración de claves criptográficas* ..... *6*

**CONSECUENCIAS Y SANCIONES** ..... **7**

**GLOSARIO** ..... **7**

## Consideraciones Generales

### Objetivo

Establecer los controles criptográficos para proteger la información en BANSEFI permitiendo asegurar que la información clasificada como reservada y/o confidencial reciba un tratamiento especial en el proceso de transportación, transmisión y almacenamiento, aplicando mecanismos criptográficos que permitan minimizar los riesgos y lograr que el almacenamiento, transportación y transmisión de la información sea segura.

### Alcance

La presente política es aplicable a todos los colaboradores de BANSEFI que mantengan contacto directo con 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 debida documentación y resguardo de éstos.

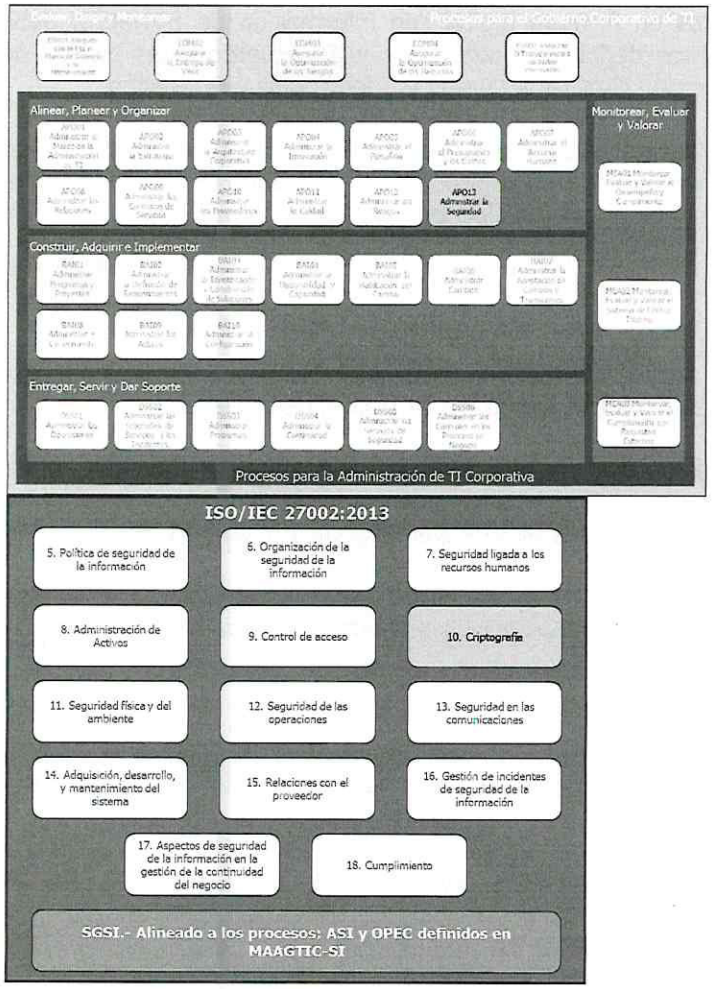
### Marco Legal de Referencia

- Ley Orgánica del Banco del Ahorro Nacional y Servicios Financieros.
- Ley de Instituciones de Crédito.
- Ley Orgánica de la Administración Pública Federal
- Ley Federal de las Entidades Paraestatales.
- Ley Federal de Transparencia y Acceso a la Información Pública.
- Reglamento Orgánico del Banco del Ahorro Nacional y Servicios Financieros, Sociedad Nacional de Crédito, Institución de Banca de Desarrollo.
- Reglamento de la Ley Federal de las Entidades Paraestatales.
- Disposiciones de Carácter General aplicables a las Instituciones de Crédito.
- Manual General de Organización del Banco del Ahorro Nacional y Servicios Financieros.
- Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información.
- Las demás Leyes, Reglamentos, Reglas, Disposiciones de carácter general, Acuerdos, Decretos, Circulares, Oficios-Circulares, Manuales, Normas, Políticas, Procedimientos, Procesos, Lineamientos, Formatos, Criterios, Metodologías, Instructivos, Directivas y cualesquiera de naturaleza análoga a las anteriores, que emita el Congreso de la Unión, la Secretaría de Hacienda y Crédito Público, la Comisión Nacional Bancaria y de Valores, el Banco de México, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, el Instituto Federal de Acceso a la Información y Protección de Datos, la Secretaría de la Función Pública, y demás autoridades u órganos competentes, aplicables a las instituciones de crédito.

### Vigencia

Esta política es vigente a partir del siguiente día hábil a su publicación en el portal de la comunidad BANSEFI.

## Marco Normativo




| Código | Descripción |
|---|---|
| **ISO/IEC 27001:2013** | 10.1.1. Política sobre el uso de controles criptográficos.<br>10.1.2. Gestión de claves. |

## Responsables de cumplimiento

Es responsabilidad de la Dirección de Contraloría Interna, a través de la Gerencia de Control Operacional y Seguridad de la Información, el vigilar el cumplimiento de la presente política. Así como de las siguientes áreas, el apegarse a esta política:

- Colaboradores de BANSEFI,
- Visitantes o terceros,

## Política de Controles Criptográficos

Todo usuario que utiliza y administra documentos en formato digital con información de BANSEFI, debe encriptar la misma de acuerdo a los requerimientos definidos, autorizados y de acuerdo a los niveles de clasificación de la información definidos por la Dirección General Adjunta de Tecnologías y Operación.

De ser necesario, la Dirección General Adjunta de Tecnologías y Operación aprobará un software criptográfico para los archivos en los sistemas de información y recursos tecnológicos que los usuarios requieran proteger de acuerdo al rol y responsabilidad que tienen sobre la información que utilizan y administran dentro de BANSEFI.

### Políticas específicas

1. Se deben utilizar herramientas de criptografía para la protección de la confidencialidad.

2. Se debe definir los algoritmos criptográficos que podrán utilizarse al interior de BANSEFI, como aplicación directa o como parte de la configuración de otros productos de seguridad comerciales, tomando en cuenta el tipo y la calidad del algoritmo criptográficos utilizado y la longitud de las claves criptográficas.

3. Sólo se deben utilizar algoritmos criptográficos, definidos por los estándares internacionales.

### Sobre el servicio de no repudiación.

1. Los servicios de no repudio deben utilizarse cuando sea necesario resolver disputas acerca de la ocurrencia o no de un evento o acción. Estos servicios están basados en el uso de técnicas criptográficas y firma digital.

2. BANSEFI establece que estos servicios estarán definidos por el uso de firma digital basada en Certificados Digitales.

### Sobre la administración de claves criptográficas

1. La administración de claves criptográficas utilizadas es responsabilidad de la Dirección General Adjunta de Tecnologías y Operación.

2. Se debe implementar un sistema de administración para respaldar el uso por parte de BANSEFI, de los dos tipos de técnicas criptográficas más usados: técnicas de clave secreta y técnicas de clave pública.

3. Las técnicas de clave pública se utilizarán para el cifrado y para generar firmas digitales.

4. Todas las claves deben ser protegidas contra divulgación, modificación y destrucción. Las claves secretas y privadas necesitan protección contra divulgación no autorizada.

5. Se debe proveer de protección física al equipamiento utilizado para generar, almacenar y archivar claves, considerando los respaldos correspondientes, el resguardo y protección de accesos a éstos.

6. Si los datos en un medio de almacenamiento se encuentran cifrados incluso en modo de respaldo, las llaves de cifrado deben ser almacenadas en otro medio de almacenamiento separado. (Cuando aplique).

7. Si se utilizan técnicas criptográficas, la información protegida debe ser transferida por un medio distinto al utilizado para transferir las llaves criptográficas.

**Consecuencias y sanciones**

La violación por acción u omisión de esta política de seguridad de la información de BANSEFI implica, actualiza y/o genera sanciones en términos de la normatividad aplicable. La supervisión de la adecuada aplicación de esta política estará a cargo de los órganos de vigilancia del Banco.

**Glosario**

| Término | Descripción |
|---|---|
| **BANSEFI** | Banco del Ahorro Nacional y Servicios Financieros S.N.C. |
| **Certificado Digital** | Es un fichero informático generado por una entidad de servicios de certificación que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet |
| **Clave criptográfica** | Es una pieza de información que controla la operación de un algoritmo de criptografía. Habitualmente, esta información es una secuencia de números o letras mediante la cual, en criptografía, se especifica la transformación del texto plano en texto cifrado, o viceversa |
| **Colaboradores** | Personal que mantiene una relación laboral con BANSEFI dentro de los siguientes esquemas: estructura, por honorarios y Outsourcing |
| **Criptografía** | Estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican |
| **No repudiación** | Concepto de prevención de la negación de un mensaje que es enviado o recibido y asegura que el que envió el mensaje no puede negar que lo envió o que el recepto niegue haberlo recibido. La propiedad de No Repudiación de un sistema de Seguridad de redes de cómputo se basa en el uso de firmas digitales |
| **Recursos tecnológicos** | Forma genérica de llamar a los equipos de tecnología y comunicaciones; como pueden ser: servidores, equipos de escritorio, equipos portátiles, equipos de telecomunicación, switch, impresoras, entre otros |
| **Seguridad de la información** | Preservación de la confidencialidad, integridad y disponibilidad de la información |
| **Terceros** | Personal que mantiene una relación laboral con BANSEFI, pero que no es considerado parte de ellos; ejemplo: consultores, despachos, entre otros |
| **Visitantes** | Personal que requiera entrar a las instalaciones del Banco, pero que no mantiene ningún tipo de relación laboral con el mismo; ejemplo: clientes, familiares de colaboradores, etc |