Bansefi
EL BANCO QUE TE INCLUYE

| | |
|---|---|
| Nombre del Documento | **POLÍTICA DE ADMINISTRACIÓN DE LA SEGURIDAD DE LA RED** |
| No. de Control | PL-SGSI-16 |
| Versión | 1.3 |
| Vigencia a partir de | |
| Total de Páginas | 8 |
| 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 Administración de la Seguridad de la Red** | |
| **Nombre interno:** | **Política de Administración de la Seguridad de la Red** | |
| **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 ADMINISTRACIÓN DE LA SEGURIDAD DE LA RED** ..... **6**

POLÍTICAS ESPECÍFICAS ..... 6

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

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

## Consideraciones Generales

### Objetivo

Establecer los lineamientos, en materia de seguridad de la información, sobre la administración de seguridad de la red.

### Alcance

Esta política de seguridad de la información es aplicable al personal de estructura, Outsourcing, honorarios o cualquier persona que mantenga una relación laboral con el Banco y que este inmersa en las actividades de seguridad de la red.

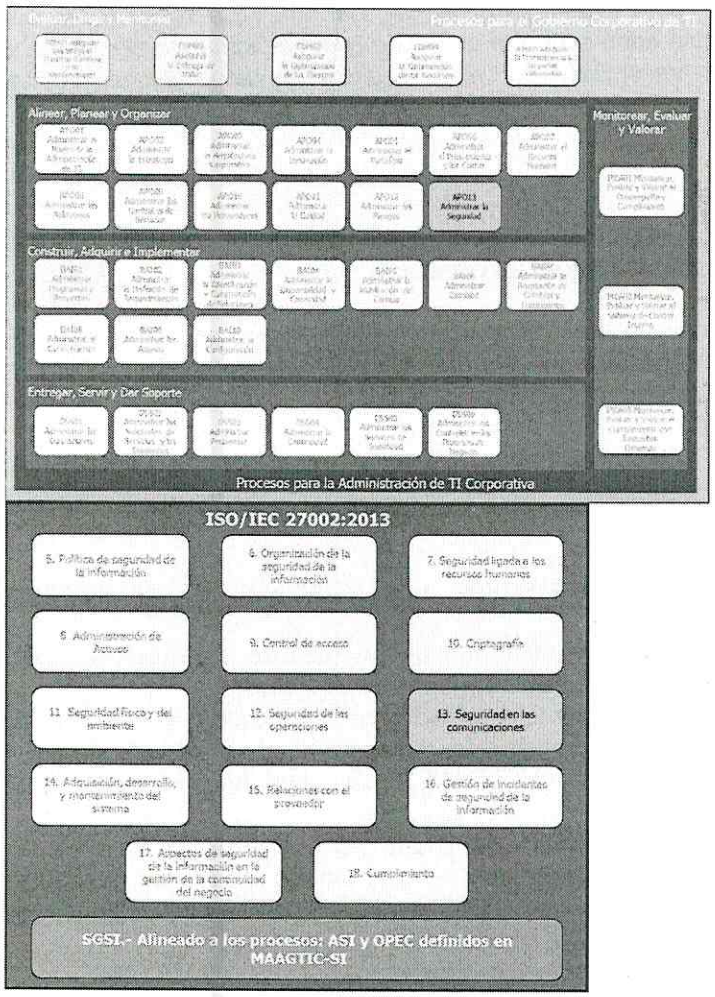
### Marco Legal de Referencia

- 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** | 13.1.1. Controles de red.<br>13.1.2. Seguridad de los servicios de red.<br>13.1.3. Separación en las redes. |

## 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 Administración de la Seguridad de la Red

Se debe proteger toda la información clasificada como reservada o confidencial que pase sobre redes que estén fuera de los límites de BANSEFI. Así mismo, se debe controlar el uso de Internet tomando en cuenta el flujo de datos, el monitoreo de la información transmitida por este medio y las implicaciones legales aplicables.

### Políticas específicas

1. La Dirección de Infraestructura y Producción debe asegurar que la operación de las redes se encuentre separada de la operación de la infraestructura de cómputo.

2. El responsable de la operación de redes debe contar con procedimientos para la administración del equipo remoto, así como controles de intercambio de información sensible sobre redes públicas y esquemas de redundancia para garantizar la disponibilidad de los servicios.

3. Se debe administrar y controlar la red de BANSEFI, a fin de protegerla contra amenazas y mantener la seguridad de los sistemas y aplicaciones que utilizan la red, incluyendo la información en tránsito, considerando al menos lo siguiente:

   a) Cada red debe proveer un nivel de seguridad acorde a la sensibilidad de los sistemas, aplicaciones y datos disponibles a través de ella
   b) Cada red debe ser diseñada y administrada de tal forma que la falla de cualquier elemento conectado con ella no permita el acceso a toda la red a usuarios no autorizados.
   c) Deben existir controles de integridad para prevenir la divulgación no autorizada o la modificación de datos mientras se encuentran en proceso de transmisión, almacenamiento o procesamiento.
   d) Las interfaces para redes externas que no pertenezcan a BANSEFI se deben autorizar tomando en cuenta la necesidad que representa para los objetivos institucionales.
   e) Los usuarios y sistemas de la red deben estar ampliamente identificados y autenticados.
   f) La comunicación entre las redes internas de BANSEFI con interne y otras redes externas deben tener sistemas de comprobación de identidad a través de un Firewall y de métodos de encriptación y protección de intrusos aprobados por el GESI.
   g) Deben registrarse los accesos válidos, no autorizados y fallidos.
   h) Se deben restringir los puertos de datos de la red sólo a dispositivos autenticados y autorizados o desactivar los puertos de red que no estén en uso.
   i) No se debe permitir la instalación de computadoras, redes o aplicaciones que comprometan la seguridad de la red.
   j) No conectar equipos que representen un puente inseguro entre una red y otra.
   k) La Gerencia de Seguridad Perimetral debe integrar una solución de antivirus perimetral y de filtrado de contenido.
   l) Las operaciones de la red interna en donde se encuentran ubicadas las estaciones de administración y monitoreo, deben ser independientes de la red de datos de usuario.

4. La información confidencial y/o reservada de BANSEFI nunca debe ser enviada a través de Internet a menos que esta haya sido cifrada por métodos previamente aprobados y autorizada por el dueño de la información. Debe existir evidencia de esta autorización.

5. El acceso a Internet es solo permitido desde estaciones personales. Todos los archivos y software descargados de Internet deben ser revisados con un programa autorizado de detección de virus antes de ser movido y/o copiados a otra computadora o abiertos o ejecutados.

6. Toda la información tomada de Internet debe ser considerada sospechosa hasta que se confirme por otra fuente confiable.

7. Los sistemas de producción, tales como servidores de aplicación, bases de datos, etc., no deben estar expuestos y conectados a Internet.

8. Dado que el servicio de Internet hace uso de los recursos de BANSEFI, la actividad de los usuarios puede ser monitoreada, sin generar alguna obligación, por lo que los usuarios no pueden esperar que se mantenga privacidad sobre el servicio.

9. Todas las conexiones hacia redes públicas o Internet deben de pasar a través del firewall.

10. El servicio de Internet es otorgado de forma personal y son los usuarios, los responsables directos de evitar accesos no autorizados a sitios de Internet que no tengan fines estrictamente laborales, así como de las actividades que bajo su cuenta se realicen.

**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 |
|---|---|
| **Antivirus** | Es un programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema |
| **BANSEFI** | Banco del Ahorro Nacional y Servicios Financieros S.N.C. |
| **Centro de datos** | Es un espacio exclusivo donde se mantienen y operan las infraestructuras de TIC que se utilizan para gestionar las actividades del negocio. |
| **Colaboradores** | Personal que mantiene una relación laboral con BANSEFI dentro de los siguientes esquemas: estructura, por honorarios y Outsourcing |
| **Firewall** | Programa informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad |
| **Infraestructura de TIC** | Hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC |
| **Logs** | Es un registro de eventos durante un rango de tiempo en particular que ocurre para un dispositivo en particular o aplicación. Entiéndase también como bitácora |
| **Monitoreo** | Acción de búsqueda de problemas causados por la sobrecarga y/o fallas en los servidores y sistemas, como también problemas de la infraestructura de red (u otros dispositivos). |
| **Network Address** | Mecanismo de mapeo (o traducción) utilizado por routers IP para |

| Término | Descripción |
|---|---|
| **Translation (NAT)** | intercambiar paquetes entre dos redes (interna y externa) que tienen rangos de dirección diferentes y por tanto incompatibles |
| | |
| **Seguridad de la información** | Preservación de la confidencialidad, integridad y disponibilidad de la información |
| **Seguridad perimetral** | Integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles |
| **Servidor** | Es un tipo de computadora, de altas prestaciones y capacidades, conectada a una red informática que contiene datos, programas, etc., que dan servicio a otras computadoras a través de esta red |
| **Terceros** | Personal que mantiene una relación laboral con BANSEFI, pero que no es considerado parte de ellos; ejemplo: consultores, despachos, entre otros |
| **Trabajo remoto** | Método de actividad laboral que se desarrolla fuera de las instalaciones de la empresa, mediante el uso de redes previamente configuradas y establecidas |
| **Topología de red** | Mapa físico o lógico de una red para intercambiar datos |
| **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 |
| **Vulnerabilidad** | Debilidad de un activo o control que puede ser explotada por una o más amenazas. |
| **Zona desmilitarizada (DMZ)** | Es un área entre Internet y la red interna que impide el acceso no autorizado a la red corporativa interna |