Bansefi
EL BANCO QUE TE INCLUYE

Nombre del Documento	**POLÍTICA DE CONTROL DE ACCESO A LA RED**
No. de Control	PL-SGSI-10
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 Control de Acceso a la Red**	
Nombre interno:	**Política de Control de Acceso a 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 CONTROL DE ACCESO A LA RED **5**

POLÍTICAS ESPECÍFICAS 5
Sobre el acceso a la red *5*
Sobre las medidas de seguridad en la red *6*
Sobre el acceso a la red en dispositivos móviles y remotamente *6*

CONSECUENCIAS Y SANCIONES **7**

GLOSARIO **7**

Consideraciones Generales

Objetivo

Establecer los lineamientos, en materia de seguridad de la información, de acceso y restricción a las redes del Banco, que permitan asegurar la confidencialidad, integridad y disponibilidad de la información que se transmite a través de estas.

Alcance

Esta política de seguridad de la información es aplicable al personal de estructura, Outsourcing, honorarios o cualquier persona que le sea asignado o haga uso de equipos de escritorio o portátiles propiedad de BANSEFI y/o tenga acceso a la red interna o externa del Banco.

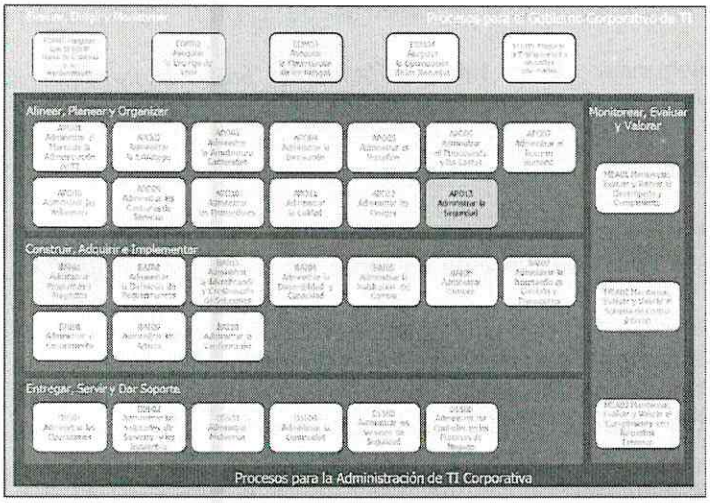
Marco Legal de Referencia

- 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	A.9.1.1 Política de control de accesos A.9.1.2 Accesos a las redes y servicios de la red.

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 Control de Acceso a la Red

El acceso a los servicios de red debe estar controlado y restringido por la Dirección General Adjunta de Tecnologías y Operación, para evitar que se haga un mal uso de los recursos y de los sistemas de información, evitando así poner en peligro la información de BANSEFI que se transmite a través de la red interna y externa del Banco.

Políticas específicas

Sobre el acceso a la red

1. El acceso a la red local y externa de BANSEFI debe ser proporcionado a usuarios autorizados y específicamente a los servicios que requieran para el cumplimiento de sus funciones, considerando en todo momento el principio de "acceso mínimo permitido".
2. La Gerencia de Telecomunicaciones debe contar con un procedimiento formal para la asignación de accesos a las redes BANSEFI, en el que se considere la aprobación de la Gerencia de Control

Operacional y Seguridad de la Información.

3. Todo cambio en los permisos de acceso deberá contar con la justificación correspondiente, así como la autorización de la Gerencia de Telecomunicaciones y la Gerencia de Control Operacional y Seguridad de la Información.
4. La Gerencia de Control Operacional y Seguridad de la Información es el área responsable de custodiar todas las autorizaciones de acceso a redes del los colaboradores y terceros autorizados.

Sobre las medidas de seguridad en la red

1. La Gerencia de Telecomunicaciones y la Gerencia de Seguridad Perimetral deben contar con la topología de red detallada y actualizada, así como un respaldo de todas las configuraciones de red del Banco.
2. La Gerencia de Telecomunicaciones y la Gerencia de Seguridad Perimetral son las áreas responsables de implementar los controles de seguridad necesarios para preservar la Confidencialidad, Integridad y Disponibilidad de la información. Así mismo, deberán asegurar la correcta segmentación de la red interna de BANSEFI y contar con segmentos seguros (DMZ o Zona Desmilitarizada) para los activos de TIC críticos.
3. La infraestructura de TIC utilizada para la administración y monitoreo de los activos de TIC, debe estar dentro de un segmento seguro (DMZ o Zona Desmilitarizada).
4. Ante una expansión de red del Banco, se deberá notificar y presentar, previo a la expansión, el correspondiente análisis de riesgos e impacto a la Gerencia de Telecomunicaciones y la Gerencia de Seguridad Perimetral para determinar los controles de seguridad requeridos.
5. El direccionamiento de red (NAT) debe ser gestionado por la Gerencia de Telecomunicaciones y la Gerencia de Seguridad Perimetral.
6. Para aquellos accesos a información sensible o crítica por medio de redes, deberá existir un control de estas conexiones y de los usuarios que las utilizan considerando los siguientes puntos:
   a) Limitar rutas de comunicaciones para evitar que los usuarios tengan accesos a servicios no autorizados.
   b) Conexión automática de puertos a sistemas específicos
   c) Limitación de opciones en menús y subménus.
   d) Prevenir la navegación ilimitada por internet e intranet.
   e) Realizar regularmente pruebas de penetración a lo largo de toda la ruta de posibles accesos a la red, coordinada por el Grupo Estratégico de Seguridad de la Información.
7. Los servidores con servicios de Internet, deben estar en una zona desmilitarizada (DMZ) y protegidos por un firewall.

Sobre el acceso a la red en dispositivos móviles y remotamente

1. En caso de usar equipos móviles se debe asegurar que la información de BANSEFI no se vea comprometida, implementando controles de seguridad física, acceso lógico, respaldos de la información contenida en el equipo de escritorio o portátil, protección contra virus y código malicioso, entre otros.
2. El uso de redes inalámbricas estará a cargo de la Gerencia de Telecomunicaciones y esta implementará los controles necesarios para evitar que cualquier persona pueda conectarse a las mismas.
3. La Gerencia de Telecomunicaciones con apoyo de la Gerencia de Seguridad Perimetral debe implementar los métodos de autenticación apropiados para controlar el acceso de usuarios remotos.
4. Se debe controlar el acceso físico y lógico a los puertos de configuración y diagnóstico remoto a fin

de evitar mantener activa la conexión remota en todo momento y que se pudieran obtener accesos no autorizados.

5. Todas las conexiones de acceso remoto deben contar con mecanismos robustos de autenticación y transmisión de datos segura. Este servicio debe estar restringido solo a usuarios autorizados y específicamente a los recursos que requieran para el cumplimiento de sus funciones, considerando en todo momento el principio de "el acceso mínimo permitido"
6. Se debe controlar el acceso físico y lógico a los puertos de configuración y diagnóstico remoto a fin de evitar mantener activa la conexión remota en todo momento y que se pudieran obtener accesos no autorizados.
7. La conexión remota a los servicios de BANSEFI se debe realizar únicamente a través de la infraestructura provista y por los servicios definidos por la Gerencia de Seguridad Perimetral. Está prohibido el uso de módems en los computadores de usuarios para para obtener acceso remoto a la red, así como cualquier medio no autorizado por la Dirección General Adjunta de Tecnologías y Operación.
8. En función del punto anterior, queda estrictamente prohibido el uso de TeamViewer.
9. La Gerencia de Telecomunicaciones debe contar con un procedimiento formal para la autorización de conexiones remotas para colaboradores y terceros, en el que considere el visto bueno del Oficial de Seguridad, justificación del servicio y autorización del Director(a) del Área Solicitante.
10. El acceso remoto a colaboradores y terceros que se ubiquen fuera del territorio nacional deberá contar adicionalmente con la autorización del Director(a) de Contraloría Interna.
11. La Gerencia de Telecomunicaciones debe establecer un procedimiento de monitoreo de conexiones remotas.
12. Como estándar se deben establecer al menos tres tipos de acceso:
    a) Acceso general – Acceso a correo institucional y portal institucional (intranet)
    b) Acceso particular – El mismo acceso general, más los permisos necesarios para ingresar al sistema o aplicaciones que se justifique o autorice.
    c) Acceso a administradores de sistemas – Acceso a los sistemas e infraestructura propia de sus funciones.

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
Activos de TIC	Aplicativos de cómputo, bienes informáticos, soluciones tecnológicas, sus componentes, las bases de datos o archivos electrónicos y la información contenida en éstos.
BANSEFI	Banco del Ahorro Nacional y Servicios Financieros S.N.C.

Colaboradores	Personal que labora en BANSEFI (Estructura, Honorarios y Outsourcing)
Equipo de escritorio	Es un tipo de computadora personal, diseñada y fabricada para ser instalada en una ubicación fija, como un escritorio o mesa
Equipo móvil	Es un tipo de computadora de tamaño pequeño, con capacidades de procesamiento, con conexión a Internet, con memoria, diseñado específicamente para una función, pero que pueden llevar a cabo otras funciones más generales; ejemplo: smartphones, tablets, agendas electrónicas, entre otros.
Equipo portátil	Es un tipo de computadora que integra todos los elementos necesarios para un correcto funcionamiento, dispuestos en una carcasa pequeña y de fácil transportación
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
Network Address Translation (NAT)	Mecanismo de mapeo (o traducción) utilizado por routers IP para 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
Topología de red	Mapa físico o lógico de una red para intercambiar datos
Zona desmilitarizada (DMZ)	Es un área entre Internet y la red interna que impide el acceso no autorizado a la red corporativa interna