Bansefi
EL BANCO QUE TE INCLUYE

Nombre del Documento	**POLÍTICA DE PROTECCIÓN CONTRA CÓDIGO MALICIOSO**
No. de Control	PL-SGSI-07
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 Protección contra Código Malicioso**	
Nombre interno:	**Política de Protección contra Código Malicioso**	
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
MARCO NORMATIVO 5
VIGENCIA 5
RESPONSABLES DE CUMPLIMIENTO 5

POLÍTICA DE PROTECCIÓN CONTRA CÓDIGO MALICIOSO **6**

POLÍTICAS ESPECÍFICAS 6
Consideraciones contra el código malicioso *6*
Consideraciones del antivirus institucional *6*

CONSECUENCIAS Y SANCIONES **6**

GLOSARIO **7**

Consideraciones Generales

Objetivo

Establecer los lineamientos, en materia de seguridad de la información, que permitan preservar la integridad del software, sistemas de información y de las redes que procesen, almacenen o transmitan información de BANSEFI.

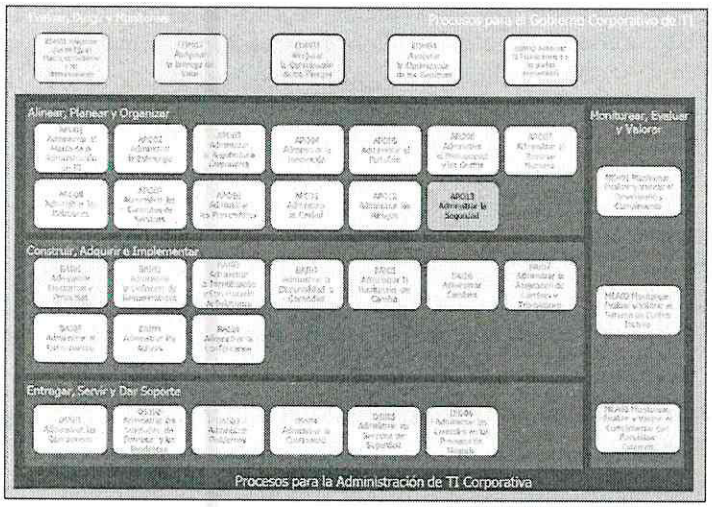
Alcance

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.

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.

Marco Normativo



Código	Descripción
ISO/IEC 27001:2013	12.2.1 Controles contra código malicioso.

Vigencia

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

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 Protección contra Código Malicioso

Para protegerse de ataques derivados de código malicioso que puedan afectar la integridad del software, sistemas de información y de las redes que procesan, almacenan o transmiten información de BANSEFI, se deben tomar las precauciones necesarias para prevenir y detectar la introducción de código malicioso (virus, gusanos, bombas lógicas, caballos de Troya, etc.).

Políticas específicas

Consideraciones contra el código malicioso

1. En caso de observar anomalías o sospechar sobre presencia de código malicioso en cualquier recurso tecnológico de BANSEFI, el colaborador debe desconectarlo de la red y reportarlo a través del Escritorio de Servicios.
2. Los colaboradores tienen prohibido descargar e instalar software diferente al que viene instalado en la imagen ISO Institucional del equipo asignado.
3. Los colaboradores tienen prohibido descargar archivos de música, video, imágenes, entre otros; que no se encuentren plenamente justificado en las funciones de su puesto.
4. Los colaboradores no deben de manejar, escribir, generar, compilar, recolectar, ejecutar o intentar introducir cualquier código malicioso diseñado para su replicación o daño en los equipos de BANSEFI.
5. El colaborador debe abstenerse de utilizar el servicio de Internet para difundir código malicioso y/o ataques desarrollados por él mismo.
6. La Dirección de Contraloría Interna deberá conducir revisiones periódicas para detectar el uso de software no autorizado y aplicar las medidas correspondientes.

Consideraciones del antivirus institucional

7. Todos los recursos tecnológicos del Banco deben tener instalado el antivirus aprobado por la Dirección de Infraestructura y Producción.
8. El antivirus debe estar habilitado y actualizado en todos los recursos tecnológicos de BANSEFI, los colaboradores no deben contar con permisos para cancelar este proceso.
9. Todos los dispositivos de almacenamiento interno o externo previo a su utilización deben ser revisados con el antivirus institucional.

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.
Código malicioso	Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.
Colaboradores	Personal que mantiene una relación laboral con BANSEFI dentro de los siguientes esquemas: estructura, por 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 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.
Imagen ISO	Tipo de archivos en donde se guardan todos los datos de un CD, un DVD, un disco duro, etc. para hacer una copia de seguridad, para clonarlos o para facilitar su transporte, etc. Se guardan en formatos como ISO, BIN, etc
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.