Bansefi
EL BANCO QUE TE INCLUYE

Nombre del Documento	**POLÍTICA DE CONTROL DE ACCESO A SISTEMAS OPERATIVOS**
No. de Control	PL-SGSI-11
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 Control de Acceso a Sistemas Operativos**	
Nombre interno:	**Política de Control de Acceso a Sistemas Operativos**	
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 SISTEMAS OPERATIVOS **6**

POLÍTICAS ESPECÍFICAS´ 6
Consideraciones de seguridad y control de acceso a sistemas operativos *6*
Sobre los equipos de escritorio y portátiles *6*

CONSECUENCIAS Y SANCIONES **7**

GLOSARIO **7**

Consideraciones Generales

Objetivo

Establecer los lineamientos, en materia de seguridad de la información, para el adecuado acceso a los sistemas operativos.

Alcance

Esta política de seguridad de la información es aplicable al personal de estructura, Outsourcing, honorarios o cualquier persona que, de acuerdo a sus funciones, deba tener acceso a los sistemas operativos de BANSEFI.

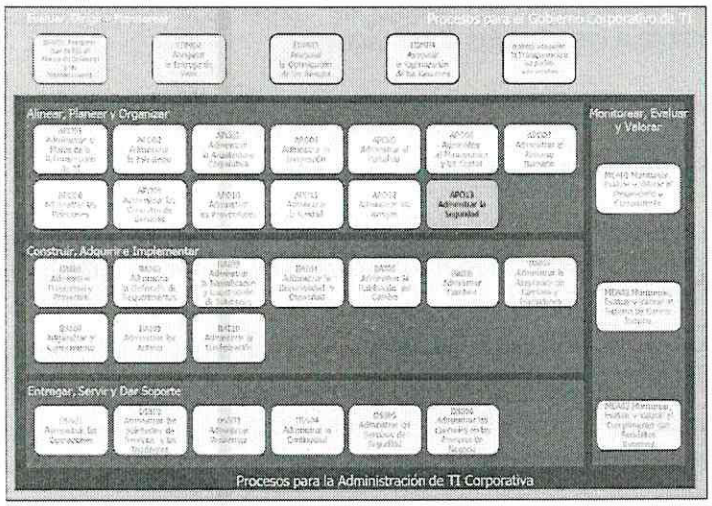
Marco Legal de Referencia

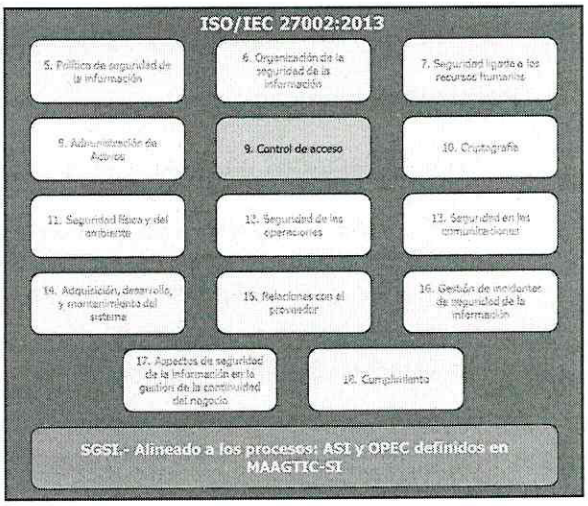
- Ley Orgánica del Banco del Ahorro Nacional y Servicios Financieros.
- Ley de Instituciones de Crédito.
- Ley Orgánica de la Administración Pública Federal
- Ley Federal de las Entidades Paraestatales.
- Ley Federal de Transparencia y Acceso a la Información Pública.
- Reglamento Orgánico del Banco 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.

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	9.3.1 Uso de información de autenticación secreta. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos de inicio de sesión seguro 9.4.3 Sistema de gestión de contraseñas 9.4.4 Uso de programas utilitarios privilegiados 9.4.5 Control de acceso al código fuente de los programas

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 Sistemas Operativos

Los mecanismos de procesamiento de información, aplicaciones y sistemas de información deben usarse restringiendo el acceso al sistema operativo únicamente a los usuarios autorizados.

Políticas específicas´

Consideraciones de seguridad y control de acceso a sistemas operativos

1. La Gerencia de Control Operacional y Seguridad de la Información debe limitar el acceso a los sistemas operativos solo a los colaboradores autorizados mediante la verificación de la identidad de los mismos y del equipo de escritorio o portátil que utilizan.
2. La Dirección de Infraestructura y Producción debe monitorear todos los accesos exitosos y fallidos a los sistemas operativos, así como llevar un correcto registro de los mismos.
3. El acceso al sistema operativo debe ser controlado a través de un procedimiento de registro seguro a fin de minimizar la oportunidad de obtener un acceso no autorizado al sistema, por lo tanto se debe considerar lo siguiente:
   a. No se deben mostrar identificadores de sistema o de aplicación hasta que el registro sea exitoso.
   b. Desplegar una advertencia que el sistema sólo podrá ser utilizado por usuarios autorizados.
   c. No mostrar mensajes de ayuda durante el proceso de registro.
   d. Limitar el número de intentos a tres oportunidades, registrando los intentos fallidos, forzando un periodo de atraso antes del siguiente intento, terminando cualquier conexión de datos e incluso bloqueando la cuenta del usuario.
   e. No indicar ningún mensaje de error o parte del registro incorrecta.
   f. Desconectar y no permitir el acceso después del rechazo.
   g. Limitar el tiempo mínimo y máximo que debe durar el proceso de login.
   h. Desplegar fecha y hora del último login exitoso.
4. Todo personal con acceso autorizado a los sistemas operativos debe tener un identificador de usuario único con el propósito que sus actividades puedan ser debidamente identificadas y/o rastreadas. Este identificador es intransferible.
5. El uso de cuentas de administrador debe estar limitado solo al personal que administra el equipo y su uso deberá ser controlado, de forma que se tenga un registro de quien lo utilizó y que realizó.
6. El uso de las librerías de cada sistema operativo debe ser limitado a los colaboradores plenamente autorizados, conservando un registro de las actividades de cada usuario.
7. La Dirección de Infraestructura y Producción debe conservar un registro de todas las librerías de cada sistema operativo de los recursos tecnológicos, y es responsable de remover aquellas herramientas o utilerías que no seas necesarias o represente un riesgo de seguridad en el sistema.

Sobre los equipos de escritorio y portátiles

8. Está prohibido instalar o configurar software y/o hardware por los colaboradores; todo el software que sea necesario instalar en los equipos debe ser autorizado por la Dirección de Infraestructura y Producción.
9. Está expresamente prohibido bajar software de Internet para instalarlo en los equipos de cómputo. No está autorizado bajar contenido de Internet que no haya sido autorizado por la Dirección de Infraestructura y Producción.

10. Los colaboradores no están autorizados para el uso de herramientas que les permita modificar la configuración de un equipo (cambio de direcciones IP, alta y baja de dispositivos, etc.).
11. Si no ha habido actividad en el equipo de escritorio o portátil durante un lapso de tiempo determinado, el sistema debe bloquearse automáticamente activándose el protector de pantalla y se debe re-establecer cuando el usuario introduzca la contraseña adecuada.

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
Colaboradores	Personal que labora en BANSEFI (Estructura, Honorarios y Outsourcing)
Hardware	Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático
Seguridad de la información	Preservación de la confidencialidad, integridad y disponibilidad de la información
Sistema Operativo	Conjunto de órdenes y programas que controlan los procesos básicos de una computadora y permiten el funcionamiento de otros programas
Software	Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas