


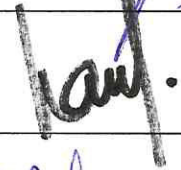

Nombre del Documento	<b>POLÍTICA DE CONTROL DE ACCESO A LA INFORMACIÓN Y APLICACIONES</b>
No. de Control	PL-SGSI-12
Versión	1.3
Vigencia a partir de	
Total de Páginas	7
Macroproceso/ Proceso principal	Administrar la Seguridad de la Información
Titular del área responsable del Proceso/ Procedimiento(responsable)	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	

**POLÍTICA DE CONTROL DE ACCESO A LA INFORMACIÓN Y APLICACIONES**
**Información General**

<b>Título:</b>	Política de Control de Acceso a la Información y Aplicaciones	
<b>Nombre interno:</b>	Política de Control de Acceso a la Información y Aplicaciones	
<b>Fecha Aprobación:</b>		
	Confidencial	
	Restringido	
<b>Nivel de confidencialidad:</b>	<b>Uso Interno</b>	✓
	Público	

**Control de cambios**

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



**POLÍTICA DE CONTROL DE ACCESO A LA INFORMACIÓN Y APLICACIONES****Contenido**

<b>CONSIDERACIONES GENERALES .....</b>	<b>4</b>
OBJETIVO .....	4
ALCANCE .....	4
MARCO LEGAL DE REFERENCIA .....	4
VIGENCIA.....	4
MARCO NORMATIVO .....	5
RESPONSABLES DE CUMPLIMIENTO .....	5
<b>POLÍTICA DE CONTROL DE ACCESO A LA INFORMACIÓN Y APLICACIONES .....</b>	<b>6</b>
POLÍTICAS ESPECÍFICAS.....	6
<i>Consideraciones de seguridad sobre la información y aplicaciones.....</i>	<i>6</i>
<i>Sobre accesos a información y aplicaciones.....</i>	<i>6</i>
<b>CONSECUENCIAS Y SANCIONES .....</b>	<b>7</b>
<b>GLOSARIO .....</b>	<b>7</b>





## Consideraciones Generales

### Objetivo

Establecer los lineamientos, en materia de seguridad de la información, sobre el acceso a la información y a las aplicaciones, a fin de que solo el personal autorizado pueda tener acceso.

### 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 cómputo propiedad de BANSEFI y/o tenga acceso a la información del Banco.

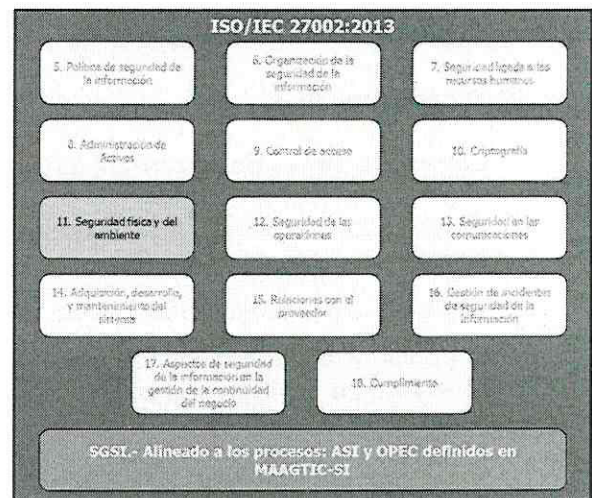
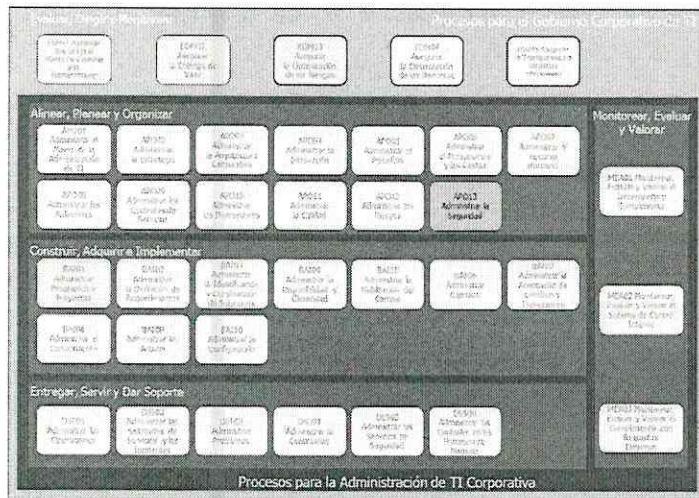
### Marco Legal de Referencia

- 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.



**POLÍTICA DE CONTROL DE ACCESO A LA INFORMACIÓN Y APLICACIONES**
**Marco Normativo**


Código	Descripción
<b>ISO/IEC 27001:2013</b>	9.1.1 Política de Control de Acceso 9.1.2 Acceso a las redes y servicios de 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,

*[Firma manuscrita]*



**Política de Control de Acceso a la Información y Aplicaciones**

Se debe restringir el acceso lógico a la información y a las aplicaciones, a fin de que sólo el personal autorizado pueda tener acceso a los mismo.

**Políticas específicas****Consideraciones de seguridad sobre la información y aplicaciones**

1. Todos los colaboradores, incluso terceros deberán tener acceso sólo a la información necesaria para el desarrollo legítimo de sus funciones y actividades en BANSEFI.
2. Todas las contraseñas o claves de acceso a los sistemas se consideran información confidencial.
3. El acceso a la información, sistemas y aplicaciones debe estar restringido a los colaboradores de acuerdo a los privilegios de acceso y al control de acceso aprobados por el dueño o propietario de la información.
4. El dueño o propietario de la información, a través de la Gerencia de Control Operacional y Seguridad de la Información, se reserva el derecho de suspender o cancelar facultades de acceso a cualquier persona que represente un riesgo a la confidencialidad, integridad o disponibilidad de la información.
5. Las reglas y derechos de acceso para cada usuario o grupo de usuarios deberán estar claramente definidas, documentadas y comunicadas.
6. Los siguientes controles deben ser observados:
  - a. Los requerimientos de seguridad de cada aplicación deben ser definidos por el dueño o propietario de la aplicación (nivel de confidencialidad, integridad y disponibilidad requerida)
  - b. Toda la información que utiliza cada sistema o aplicación de BANSEFI debe estar identificada y documentada.
  - c. La distribución de la información solamente podrá hacerse bajo la autorización del dueño de la misma y de conformidad con las normas de seguridad de la información institucionales.

**Sobre accesos a información y aplicaciones**

7. Cualquier intento de acceso no autorizado a los equipos, sistemas e información de BANSEFI debe ser reportado a la Dirección de Infraestructura y Producción, así como a la Dirección de Contraloría Interna.
8. La Gerencia de Control Operacional y Seguridad de la Información establecerá el procedimiento formal para la asignación de identidades y facultades en los sistemas, de tal forma que establezca un control efectivo desde el registro inicial de la cuenta hasta el momento en que requiera ser modificada, revocada o eliminada.
9. La Gerencia de Control Operacional y Seguridad de la Información es el área facultada para administrar las cuentas de usuarios de conformidad con los perfiles y roles establecidos por el dueño de la información o aplicación.
10. Las cuentas de administración deben ser notificadas a la Gerencia de Control Operacional y Seguridad de la Información indicando el colaborador(es) responsable(s) y el servicio o sistema a su cargo.
11. Las cuentas de administración deben ser renovadas como máximo cada 30 días.
12. Las cuentas de administración deben ser conocidas por el menor número de personas, por lo que el



administrador en casa de sospechar que esta ha sido comprometida, debe cambiarla inmediatamente y notificar el incidente a la Gerencia de Control Operacional y Seguridad de la Información.

### 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
<b>BANSEFI</b>	Banco del Ahorro Nacional y Servicios Financieros S.N.C.
<b>Colaboradores</b>	Personal que mantiene una relación laboral con BANSEFI dentro de los siguientes esquemas: estructura, por honorarios y Outsourcing
<b>Seguridad de la información</b>	Preservación de la confidencialidad, integridad y disponibilidad de la información
<b>Sistema</b>	Programa informático que permite a un usuario utilizar una computadora con un fin específico
<b>Terceros</b>	Personal que mantiene una relación laboral con BANSEFI, pero que no es considerado parte de ellos; ejemplo: consultores, despachos, entre otros
<b>Visitantes</b>	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

