Bansefi
EL BANCO QUE TE INCLUYE

Nombre del Documento	**POLÍTICA DE CONTROL DE ACCESO A USUARIOS**
No. de Control	PL-SGSI-03
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 Usuarios**	
Nombre interno:	**Política de Control de Acceso a Usuarios**	
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 DEL CUMPLIMIENTO 5

POLÍTICA DE CONTROL DE ACCESO A USUARIOS **6**

POLÍTICAS ESPECÍFICAS 6
Sobre las cuentas de usuario: *6*
Sobre el control y registro de las cuentas de acceso: *6*
Consideraciones de seguridad en los sistemas y servicios: *7*

CONSECUENCIAS Y SANCIONES **8**

GLOSARIO **8**

Consideraciones Generales

Objetivo

Establecer los lineamientos, en materia de seguridad de la información, de acceso a los sistemas de información y servicios de BANSEFI.

Alcance

Esta política de seguridad de la información es aplicable al personal de estructura, sucursales, Outsourcing, honorarios o cualquier persona que haga uso de los servicios y sistemas de información del Banco.

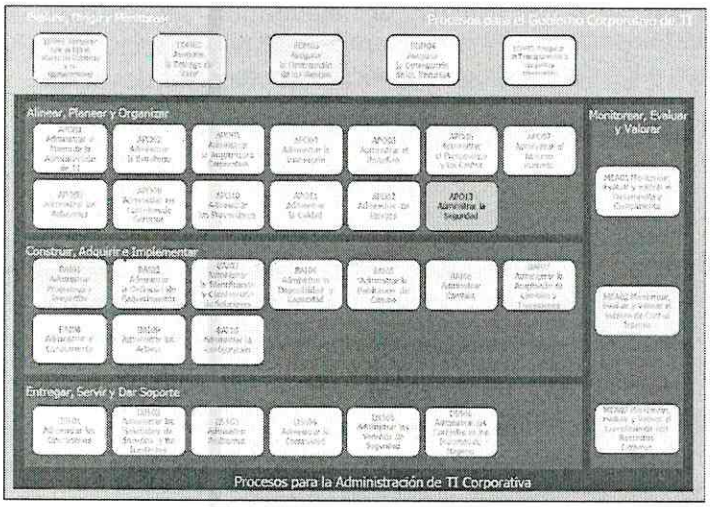
Marco Legal de Referencia

- 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.

Marco Normativo



Código	Descripción
ISO/IEC 27001:2013	9.2.1 Registro y cancelación de registro de usuario. 9.2.2 Asignación de acceso de usuario. 9.2.3 Gestión de derechos de acceso privilegiados. 9.2.4 Gestión de información secreta de autenticación de usuarios. 9.3.1 Uso de información de autenticación secreta.

Responsables del 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 Usuarios

La autorización formal de los requerimientos de acceso a los sistemas de información y/o servicios de BANSEFI debe realizarse cubriendo todo el ciclo del mismo, desde el registro de nuevos usuarios, hasta la baja del mismo, derivado de ya no requerir el acceso a los sistemas de información y/o servicios del Banco.

Políticas específicas

Sobre las cuentas de usuario:

1. La Gerencia De Control Operacional y Seguridad de la Información es la única área facultada para administrar y autorizar, previa verificación de una relación laboral con el Banco, los accesos a los sistemas y/o servicios con los que cuente BANSEFI y que se requieran para el desempeño de las funciones de los colaboradores.

2. Es responsabilidad de los colaboradores el buen uso de las cuentas de usuario, para el acceso a los sistemas y/o servicios de información del Banco, que les sean asignadas; haciendo hincapié en que estas son individuales e intransferibles y todo mal uso es responsabilidad de ellos.

3. Las contraseñas iniciales deben de ser solamente utilizadas para efecto de la creación del usuario. El colaborador, antes de realizar cualquier otra actividad, debe cambiar la contraseña al momento de ingresar por primera vez al sistema y/o servicio del Banco.

4. El acceso de visitantes o terceros a los sistemas y/o servicios institucionales será gestionado por la Gerencia de Control Operacional y Seguridad de la Información, posterior a la firma de un acuerdo de confidencialidad y justificación correspondiente por parte del Director del Área o superior inmediato solicitante y aceptación de las políticas del Banco.

5. El acceso a los sistemas y/o servicios institucionales fuera del territorio nacional, debe ser autorizado por la Dirección de Contraloría Interna con independencia de la autorización del Director del Área solicitante.

Sobre el control y registro de las cuentas de acceso:

6. El dueño o responsable del sistema y/o servicio debe definir y asignar claramente los derechos o privilegios de acceso para cada usuario o grupo de usuarios en cada sistema y/o servicio del Banco.

7. La creación de cuentas de usuario, incluyendo los privilegios asociados a cada uno de los colaboradores a su cargo, solo se realizará previa autorización del Director de área o superior inmediato.

8. La Subdirección de Recursos Humanos debe notificar quincenalmente las altas, bajas o cambios de adscripción o puesto de los colaboradores a la Gerencia de Control Operacional y Seguridad de la Información.

9. La Gerencia de Control Operacional y Seguridad de la Información debe llevar un registro actualizado de todas las cuentas de usuario y privilegios asignados a los colaboradores por cada uno de los sistemas y/o servicios.

10. La Gerencia de Control Operacional y Seguridad de la Información en conjunto con los dueños o responsables de los sistemas y/o servicios del Banco, deben revisar las cuentas de acceso al menos, cada 6 meses, a fin de depurar las cuentas inactivas y/o actualizar los privilegios de acceso de cada colaborador.

11. Los equipos de escritorio y portátiles que por necesidades del área o para cumplir las funciones, deban ser utilizados por más de un colaborador, deben contar con usuarios del sistema operativo personalizados para cada uno de ellos.

12. Los colaboradores deben realizar el cambio de su(s) contraseña(s), por lo menos, cada 6 meses en cada sistema y/o servicio institucional que tengan acceso.

Consideraciones de seguridad en los sistemas y servicios:

13. Los cuadros de diálogo de acceso sólo deben solicitar el ingreso de usuario y contraseña; no deben solicitar información adicional, ejemplo: datos de la Institución, sistema operativo o configuración.

14. El despliegue de las contraseñas en los cuadros de diálogo de acceso a los sistemas institucionales debe estar cifrado.

15. Los dispositivos de red (ruteadores, switches, firewalls, etc.), deben de contar con un ID único para cada usuario o área administrada.

16. Al instalar cualquier dispositivo en la red del Banco, ya sea de prueba, evaluación o producción, sin excepción, se deberá cambiar la contraseña predeterminada y esta pasará a ser administrada por la Dirección de Infraestructura y Producción.

17. Todas las contraseñas deben de cambiarse después de que un sistema se encontró comprometido o bien cuando el colaborador responsable del activo deje de prestar sus servicios a BANSEFI.

18. Todos los servicios y sistemas de BANSEFI deben tener configurado el tiempo de expiración de sesión.

19. Todos los sistemas y/o servicios deben verificar la longitud y estructura de la contraseña al momento de crearla o modificarla.

20. Es responsabilidad de la Dirección de Infraestructura y Producción que toda contraseña por omisión provista por el fabricante de cualquier hardware o sistema sea modificada.

21. Todos los sistemas y/o servicios deben limitar la aceptación de cinco intentos consecutivos de ingreso, después de los intentos fallidos, la cuenta de usuario debe quedar deshabilitada.

22. Los colaboradores que detecten cualquier usuario y/o contraseña en medios públicos debe ser informada a la Gerencia De Control Operacional y Seguridad y podrá ser motivo de sanción.

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 mantiene una relación laboral con BANSEFI dentro de los siguientes esquemas: estructura, por honorarios y Outsourcing
Cuadro de diálogo	Es un tipo de ventana que permite comunicación simple entre el usuario y el sistema informático.
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
ISO/IEC	Por sus siglas en Inglés, ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) son normas de estandarización, en diversas materias, reconocidas internacionalmente.
Servicio	Es un sistema diseñado para permitir interoperabilidad máquina a máquina en una red
Sistema	Programa informático que permite a un usuario utilizar una computadora con un fin específico
Seguridad de la información	Preservación de la confidencialidad, integridad y disponibilidad de la información
Terceros	Personal que mantiene una relación laboral con BANSEFI, pero que no es considerado parte de ellos; ejemplo: consultores, despachos, entre otros