Bansefi
EL BANCO QUE TE INCLUYE

Nombre del Documento	**POLÍTICA DE DESARROLLO Y MANTENIMIENTO DE SISTEMAS**
No. de Control	PL-SGSI-22
Versión	1.3
Vigencia a partir de	
Total de Páginas	9
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 Desarrollo y Mantenimiento de Sistemas**	
Nombre interno:	**Política de Desarrollo y Mantenimiento de Sistemas**	
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 6

POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS **7**

POLÍTICAS ESPECÍFICAS 7

CONSECUENCIAS Y SANCIONES **9**

GLOSARIO **9**

Consideraciones Generales

Objetivo

Establecer los lineamientos, en materia de seguridad de la información, para mantener la seguridad de la información durante la adquisición, desarrollo y mantenimiento de sistemas.

Alcance

Esta política de seguridad de la información es aplicable al personal de estructura, Outsourcing, honorarios o cualquier persona que mantenga una relación laboral con el Banco y que este inmerso en las actividades de adquisición, desarrollo y mantenimiento de aplicaciones y sistemas.

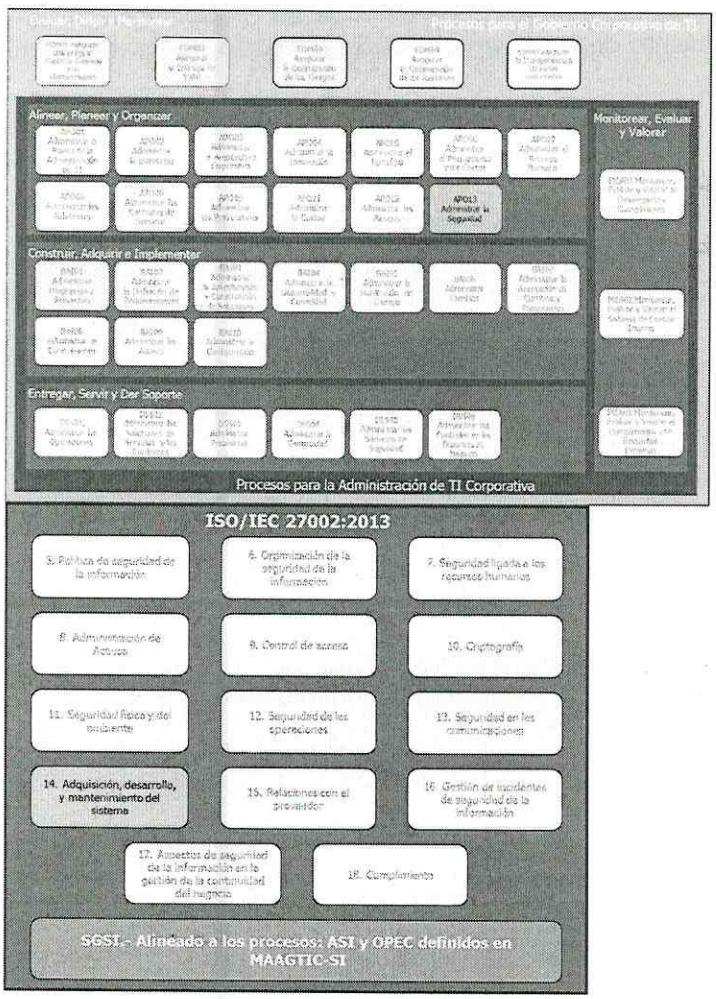
Marco Legal de Referencia

- 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	14.2.1. Política de desarrollo seguro. 14.2.2. Procedimientos de control de cambios del sistema. 14.2.3. Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación. 14.2.4. Restricciones en los cambios a los paquetes de software. 14.2.5. Principios de ingeniería de sistema seguro. 14.2.6. Entorno de desarrollo seguro. 14.2.7. Desarrollo tercerizado. 14.2.8. Prueba de seguridad del sistema. 14.2.9. Prueba de aprobación del sistema.

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 Adquisición, Desarrollo y Mantenimiento de Sistemas

Se debe incluir requerimientos de seguridad de la información a lo largo del ciclo de desarrollo de sistemas.

Políticas específicas

1. Todos los requerimientos de seguridad de la información, incluyendo las necesidades de procesamiento de información sensible o crítica, comunicaciones, de alta disponibilidad y de respaldo deben estar claramente identificados en la fase de inicio del proyecto
2. La Dirección General Adjunta de Tecnología y Operación, en conjunto con la Dirección de Desarrollo y Mantenimiento de Sistemas deben tomar en cuenta las mismas políticas cuando se trate de la evaluación de software o aplicaciones para BANSEFI.
3. Durante el desarrollo de los sistemas o aplicaciones se debe mantener la segregación de funciones evitando que una sola persona tenga el control total sobre el ciclo de vida del desarrollo de sistemas (la misma persona que desarrolla no puede ser la que pruebe y la que libere el sistema a producción).
4. Los ambientes de Desarrollo, Pruebas y Producción deben estar separado con el fin de evaluar las consecuencias de cambios en la infraestructura y aplicaciones antes de aplicarlos al ambiente de producción.
5. La configuración de los equipos debe garantizar que la ejecución de código móvil autorizado opere de acuerdo a las políticas de seguridad definidas.
6. El área que solicita el desarrollo de un nuevo sistema de información debe establecer en conjunto con el área que se encargará del desarrollo, el entendimiento común de los requerimientos del sistema considerando de manera enunciativa más no limitativa los siguientes puntos:
   - Los requerimientos funcionales, de datos, de control interno y de seguridad deben estar documentados
   - Identificar el tipo de información que manejara el sistema de conformidad con la clasificación vigente.
   - Desarrollar una matriz de roles y perfiles para el control de accesos, en donde se defina claramente los diferentes niveles de acceso de los usuarios y administradores.
   - Identificar y documentar el origen de los datos de entrada-salida y establecer la relación con otros sistemas
   - La información que sea considerada como crítica deberá ser cifrada para asegurar su confidencialidad.
   - Definir la criticidad de la aplicación, así como el tiempo máximo permitido para la recuperación.
   - Definir esquemas de respaldo para los datos, código fuente y todo el entorno de la aplicación.
   - Definir necesidades de auditoría para el registro de accesos y transacciones.
7. Se debe realizar pruebas funcionales y de integración para validar las entradas, salidas, la integridad de mensajes y el correcto procesamiento interno de los componentes o servicios ofrecidos por la aplicación.
8. Se deben establecer claramente los criterios de aceptación de sistemas y aplicaciones.
9. La Dirección de Desarrollo y Mantenimiento de Sistema debe contar con un mecanismo para llevar u

estricto control de librerías, código fuente y versiones de cada sistema o aplicación.

10. El uso de información real o sensible de BANSEFI, para la ejecución de pruebas en el desarrollo de sistema no está autorizado, salvo aquellos casos en que exista autorización expresa por parte del dueño o propietario de la información.
11. Una vez terminada la prueba y que no se necesiten más los datos de prueba, éstos deben eliminarse de manera segura, a fin de no comprometer la seguridad de la información, para lo cual se debe contar con la evidencia de borrado seguro correspondiente.
12. Cualquier cambio o actualización a las aplicaciones deben ser documentados, evaluados, autorizados y probados antes de entrar en ambientes de producción. En el caso de aquellos que se deben realizar a aplicaciones comerciales, deben contar con el consentimiento del fabricante.
13. Las herramientas y aplicaciones utilizadas para el desarrollo de sistemas y/o aplicaciones sólo pueden ser accedidas por personal autorizado dedicado al desarrollo de sistemas, por lo cual ningún otro equipo de cómputo puede tener instaladas dichas herramientas.
14. Está prohibido copiar el código fuente de los sistemas o aplicaciones en desarrollo o en operación.
15. Las actualizaciones al sistema operativo y aplicación de parches a las aplicaciones deben ser probadas en un ambiente controlado antes de liberarlas al ambiente de producción a fin de evitar problemas operacionales con las aplicaciones que se tienen instaladas. Después de cualquier cambio en aplicaciones en producción se debe correr un protocolo de pruebas para asegurar su correcto funcionamiento.
16. En el proceso de desarrollo de sistemas no está permitido el utilizar puertas traseras, canales encubiertos o configuraciones que comprometan la seguridad de la información.
17. Dentro del desarrollo de sistemas se deben tomar medidas para identificar y asegurar que, ni a través del sistema ni como parte del sistema en forma automatizada, se pueda hacer un mal uso del sistema y/o de los datos con el fin de provocar fraudes o comprometer la seguridad de la información de BANSEFI.
18. Cuando el desarrollo sea delegado a un tercero, se deberá establecer un contrato de servicios que estipule que:
    - La propiedad intelectual y la propiedad del código es de BANSEFI
    - La calidad del producto final será verificada por el dueño de la aplicación.
    - El dueño de la aplicación firmará una carta de aceptación.
    - BANSEFI tiene derecho a auditar las actividades del desarrollador externo.
19. Todo desarrollo realizado por un tercero debe ser supervisado y monitoreado por el personal designado por la Dirección de Desarrollo y Mantenimiento de Sistemas, a fin de garantizar que se cumplan con los requisitos de seguridad de información establecidos.
20. Cuando se cambie de proveedor es necesario tomar en consideración los siguientes puntos:
    - Riesgo de incorporar nuevos controles y procesos con los terceros.
    - Proyección del tercero a futuro.
    - Impacto de los costos de mantenimiento futuros, los cambios en procesos de mantenimiento y el control de versiones.

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
Acuerdo de Nivel de Servicios (SLA)	Consiste en un contrato en el que se estipulan los niveles de un servicio en función de una serie de parámetros objetivos, establecidos de mutuo acuerdo entre ambas partes, así, refleja contractualmente el nivel operativo de funcionamiento, penalizaciones por caída de servicio, limitación de responsabilidad por no servicio, etc
Ambiente de desarrollo	Ambiente independiente del de producción donde se desarrollan las modificaciones de workbench o customizing y las mismas luego de ser probadas son impactadas al ambiente de producción.
Ambiente de producción	Ambiente donde se encuentran los datos operativos y donde los usuarios finales transacciones. La información sensible de la organización se encuentra almacenada en el mismo.
Ambiente de pruebas	Es un entorno que aísla los cambios en el código, fruto de la experimentación, del propio entorno de producción o entorno de edición
BANSEFI	Banco del Ahorro Nacional y Servicios Financieros
Centro de datos	Es un espacio exclusivo donde se mantienen y operan las infraestructuras de TIC que se utilizan para gestionar las actividades del negocio.
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	Programa informático que permite a un usuario utilizar una computadora con un fin específico
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
Terceros	Personal que mantiene una relación laboral con BANSEFI, pero que no es considerado parte de ellos; ejemplo: consultores, despachos, entre otros
Visitantes	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
Zona desmilitarizada (DMZ)	Es un área entre Internet y la red interna que impide el acceso no autorizado a la red corporativa interna