Bansefi
EL BANCO QUE TE INCLUYE

| | |
|---|---|
| Nombre del Documento | **POLÍTICA DE MONITOREO** |
| No. de Control | PL-SGSI-14 |
| 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 Monitoreo** | |
| **Nombre interno:** | **Política de Monitoreo** | |
| **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 MONITOREO** ..... **6**

POLÍTICAS ESPECÍFICAS ..... 6
*Sobre el monitoreo en sistemas y aplicaciones* ..... *6*
*Sobre las bitácoras y logs de monitoreo* ..... *6*

**CONSECUENCIAS Y SANCIONES** ..... **7**

**GLOSARIO** ..... **7**

## Consideraciones Generales

### Objetivo

Establecer lineamientos, materia de seguridad de la información, para el monitoreo de la infraestructura de TI de BANSEFI.

### 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, que haga uso y/o tenga acceso a los sistemas y red del Banco y que estén inmersos en el proceso de monitoreo de la infraestructura.

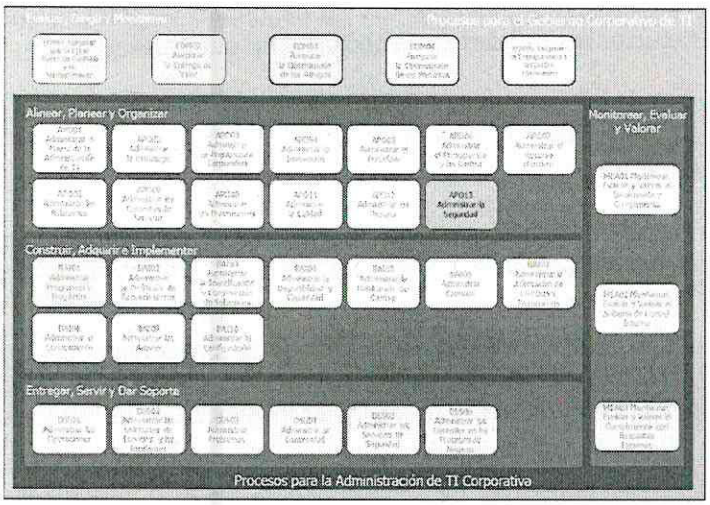
### Marco Legal de Referencia

- 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** | 12.4.1. Registro de evento.<br>12.4.2. Protección de la información de registros.<br>12.4.3. Registros del administrador y el operador.<br>12.4.4. Sincronización de relojes<br>12.7.1 Controles de auditoría de sistemas de información |

## 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 Monitoreo

Todos los activos de TIC de BANSEFI deben ser monitoreados, los eventos de seguridad de información deben ser registrados en bitácoras o logs, a fin de detectar actividades sospechosas o no autorizados.

### Políticas específicas

#### Sobre el monitoreo en sistemas y aplicaciones

1. La Dirección de Infraestructura y Producción debe asegurar que todos los sistemas y aplicaciones, así como las plataformas sobre las que operan, tengan activas las bitácoras de operación, error, transacción, registro de usuarios y de actividades
2. Las bitácoras y/o logs resultantes del punto anterior deben resguardarse y protegerse por la Dirección de Infraestructura y Producción y por la Gerencia de Control Operacional y Seguridad de la Información, toda vez que servirán como pistas de auditoría para cualquier investigación de eventos o incidentes.
3. La Dirección de Infraestructura y Producción debe monitorear de manera periódica el uso y acceso de las instalaciones, mecanismos de procesamiento de información, sistemas, aplicaciones y servicios del Banco.

#### Sobre las bitácoras y logs de monitoreo

4. La Dirección de Infraestructura y Producción y la Gerencia de Control Operacional y Seguridad de la Información deben respaldar las bitácoras (logs) de manera regular, las cuales deben estar salvaguardadas y protegidas contra desactivaciones, modificaciones y accesos no autorizados.
5. Las bitácoras (logs) de los sistemas o aplicaciones deben ser a nivel transacción, con el fin de mantener el control de la información que es consultada, actualizada o borrada.
6. Las bitácoras (logs) podrán ser depuradas con el propósito de liberar recursos en la plataforma sobre la que operen los sistemas o aplicaciones de BANSEFI, siempre y cuando se garantice que, como resultado de los procedimientos de respaldo y recuperación de la información, se podrá contar con bitácoras continuas o sin pérdida de registro alguno.
7. El tiempo de retención de las bitácoras y/o log debe ser de 3 meses para sistemas críticos y de 1 mes para sistemas no críticos. Los dueños de la información podrán solicitar ampliar este periodo en función de sus propios requerimientos.
8. Las bitácoras (logs) de los sistemas o aplicaciones deben ser manejadas y revisadas periódicamente a fin de poder detectar cualquier registro o falta de él, que sea indicio de alguna actividad anormal o maliciosa.
9. La Dirección de Infraestructura y Producción debe asegurar que toda la infraestructura de TIC de BANSEFI este sincronizada a la hora oficial para los Estados Unidos Mexicanos generada por el Centro Nacional de Metrología, en los husos horarios establecidos en la Ley del Sistema de Horario en los Estados Unidos Mexicanos, para lo cual hará uso del servicio que dicho centro proporciona de manera gratuita.

10. Las bitácoras y logs deben contener, como mínimo, los siguientes campos:
    a. Identificación de la terminal o equipo del usuario (Mac Address e IP)
    b. Fecha y hora de todos los intentos de acceso exitosos y fallidos.
    c. Fecha y hora de todas las transacciones críticas
    d. Fecha y hora de cierre de sesión
    e. Toda la actividad realizada por los usuarios con privilegios de administrador.

**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 |
| **Infraestructura de TIC** | Hardware, software, redes e instalaciones requeridas para desarrollar, probar, proveer, monitorear, controlar y soportar los servicios de TIC |
| **Logs** | Es un registro de eventos durante un rango de tiempo en particular que ocurre para un dispositivo en particular o aplicación. Entiéndase también como bitácora |
| **Monitoreo** | Acción de búsqueda de problemas causados por la sobrecarga y/o fallas en los servidores y sistemas, como también problemas de la infraestructura de red (u otros dispositivos). |
| **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 |
| **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 |