Bansefi
EL BANCO QUE TE INCLUYE

Nombre del Documento	**POLÍTICA DE SEGURIDAD DE LOS RECURSOS TECNOLÓGICOS**
No. de Control	PL-SGSI-05
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 Seguridad de los Recursos Tecnológicos**	
Nombre interno:	**Política de Seguridad de los Recursos Tecnológicos**	
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 SEGURIDAD DEL EQUIPO **6**

POLÍTICAS ESPECÍFICAS 6
Sobre los equipos de escritorio y portátiles: *6*
Sobre los suministros de energía eléctrica *6*
Sobre la seguridad en el cableado *6*
Mantenimiento de los recursos tecnológicos *7*
Consideraciones de seguridad en el Centro de Datos *7*
Sobre la reutilización de equipos de escritorio y portátiles *7*

CONSECUENCIAS Y SANCIONES **8**

GLOSARIO **8**

Consideraciones Generales

Objetivo

Establecer lineamientos, en materia de seguridad de la información, para prevenir pérdidas, daños, hurtos o el compromiso de los recursos tecnológicos, así como para la seguridad y protección de los equipos de escritorio y portátiles contra amenazas físicas y lógicas.

Alcance

Esta política, de seguridad de la información, es aplicable al personal de estructura, sucursales, Outsourcing, honorarios o cualquier persona que le sea asignado o haga uso o tenga algún contacto con equipos de escritorio, portátiles, centro de datos, servidores y demás recursos tecnológicos de BANSEFI.

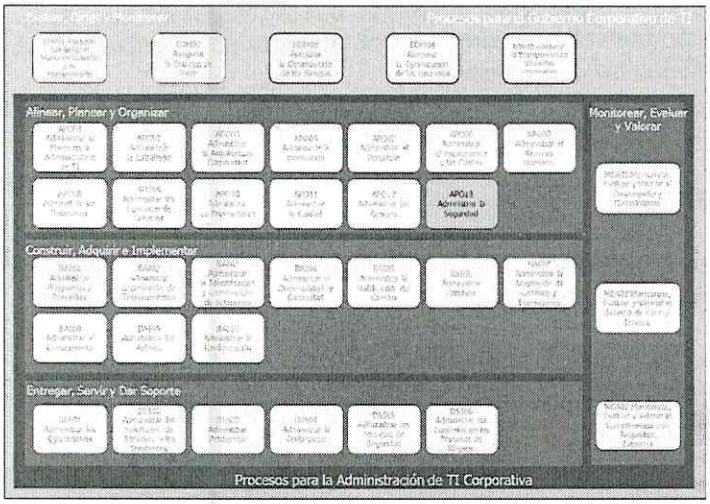
Marco Legal de Referencia

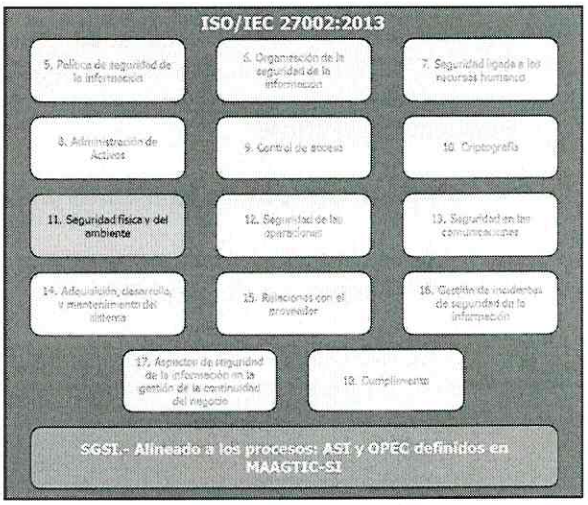
- Ley Orgánica del Banco del Ahorro Nacional y Servicios Financieros.
- Ley de Instituciones de Crédito.
- Ley Orgánica de la Administración Pública Federal
- Ley Federal de las Entidades Paraestatales.
- Ley Federal de Transparencia y Acceso a la Información Pública.
- Reglamento Orgánico del Banco 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	11.2.1 Ubicación y protección del equipamiento. 11.2.2 Elementos de soporte. 11.2.3 Seguridad en el cableado. 11.2.4 Mantenimiento del equipamiento. 11.2.5 Retiro de activos. 11.2.6 Seguridad del equipamiento y los activos fuera de las instalaciones. 11.2.7 Seguridad en la reutilización o descarte de equipos.

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 Seguridad del Equipo

Los recursos tecnológicos del Banco deben situarse o protegerse de forma que se reduzcan los riesgos derivados de las amenazas y peligros de origen ambiental, así como de los accesos no autorizados para preservar la confidencialidad, integridad y disponibilidad de la información.

Políticas específicas

Sobre los equipos de escritorio y portátiles:

1. Todos los equipos, tanto de escritorio como portátiles, deben permanecer bloqueados cuando no sean utilizados por el colaborador o administrador responsable.

2. Los colaboradores que les sean asignado o usen equipos portátiles del Banco (propios o arrendados) deben asegurar que estos cuenten con mecanismos de seguridad física en todo momento; ejemplo: chapas, candados, entre otros.

3. Es responsabilidad del colaborador el no separarse por un tiempo prolongado de su equipo y/o dejarlo resguardado en un lugar seguro.

Sobre los suministros de energía eléctrica

1. La Dirección Infraestructura y Producción debe asegurar que los recursos tecnológicos de BANSEFI estén protegidos contra fallas del suministro de energía eléctrica.

2. La Dirección Infraestructura y Producción debe asegurar que los recursos tecnológicos clasificados como esenciales o críticos, para la operación, cuenten con generadores de energía y sistemas de alimentación interrumpidas (UPS) con el fin de garantizar el suministro de energía eléctrica de manera continua.

3. La Dirección Infraestructura y Producción debe probar y revisar los UPS´s y plantas de energía periódicamente y de acuerdo a las especificaciones del fabricante.

4. El uso de UPS´s es exclusivo para los recursos tecnológicos institucionales. Los colaboradores no deben conectar radios, teléfonos celulares, cafeteras, enfriadores de agua, ventiladores, entre otros.

Sobre la seguridad en el cableado

1. La Dirección General Adjunta de Tecnologías y Operación es la responsable de verificar que los cables de telecomunicaciones (voz y datos), y energía eléctrica que transporten datos o soporten los Activos de TIC, esten protegidos contra intercepción y daño físico.

2. Los cables de electricidad deben separarse forzosamente de aquellos de comunicaciones a fin de evitar interferencias.

3. LA Dirección de Infraestructura y Producción debe asegurar que las líneas de energía eléctrica y comunicaciones dentro del centro de datos estén instaladas de acuerdo a estándares internacionales; ejemplo: debajo del piso, sobre rieles, canaletas o conductos y sujeto a medidas de protección adicionales.

Mantenimiento de los recursos tecnológicos

1. Todos recursos tecnológicos deben contar con mantenimientos preventivos y correctivos de forma periódica, de acuerdo a los requerimientos del fabricante y personal calificado, siendo la Dirección de Infraestructura y Producción la encargada de autorizar y revisar estas tareas, así mismo se deben conservar los registros o reportes de dichos mantenimientos.

2. La Dirección de Infraestructura y Producción proporcionará el mantenimiento preventivo y correctivo solo a aquellos equipos registrados en el inventario Institucional, estableciendo los mecanismos de control y seguimiento a los servicios de mantenimiento contratados.

3. El equipo de soporte (aire acondicionado, UPS, sistema contra incendios, etc.) debe recibir mantenimiento preventivo de acuerdo con las especificaciones del fabricante y con una periodicidad de al menos una vez al año.

4. El personal externo que acuda a dar soporte o mantenimiento a los recursos tecnológicos del banco debe estar acompañado en todo momento por un colaborador autorizado de la Dirección de Infraestructura y Producción.

5. Los recursos tecnológicos que se retiren de su sitio original para efectos de mantenimiento o manipulación por terceros, deben pasar por un control previo de seguridad y aprobación de la Dirección de Infraestructura y Producción y de la Gerencia de Control Operacional y Seguridad de la Información.

Consideraciones de seguridad en el Centro de Datos

1. Los cables eléctricos, switches y toma de energía se deben localizar fuera del alcance de posibles derrames líquidos.

2. No se permite el ingreso de alimentos y bebidas al centro de datos.

3. Se deben mantener y monitorear las condiciones de temperatura y humedad del centro de datos.

4. Ningún colaborador está autorizado a llevar consigo o trasladar recursos tecnológicos del centro de datos, salvo con previa autorización de la Dirección de Infraestructura y Producción y de la Gerencia de Control Operacional y Seguridad de la Información, para este caso, quedan exentos los equipos portátiles y sus accesorios.

5. Los servidores deben ubicarse en un rack y sólo colaboradores autorizados tendrá acceso al mismo.

Sobre la reutilización de equipos de escritorio y portátiles

1. Previo a la reasignación de equipos a colaboradores, la Dirección de Infraestructura y Producción debe realizar un formateo, de los mismos, a bajo nivel, lo anterior previa autorización del superior inmediato del colaborador responsable de su guarda y custodia.

2. La Dirección de Infraestructura y Producción debe llevar un registro formal de los equipos reasignados y de los que son dados de baja donde se indique que se eliminó la información contenida en dicho equipo.

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.
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 mantiene una relación laboral con BANSEFI dentro de los siguientes esquemas: estructura, por honorarios y Outsourcing
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
Formatear	Proceso que permite el correcto vaciado o borrado de la información de un disco duro o medio de almacenamiento
Rack	Es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones
Recursos tecnológicos	Forma genérica de llamar a los equipos de tecnología y comunicaciones; como pueden ser: servidores, equipos de escritorio, equipos portátiles, equipos de telecomunicación, switch, impresoras, entre otros
Servidor	Es un tipo de computadora, de altas prestaciones y capacidades, conectada a una red informática que contiene datos, programas, etc., que dan servicio a otras computadoras a través de esta red
Sistema de alimentación ininterrumpida (UPS)	Por sus siglas en inglés uninterruptible power supply (UPS) es una fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica