Bansefi
EL BANCO QUE TE INCLUYE

Nombre del Documento	**POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**
No. de Control	PL-SGSI-24
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 Gestión de Incidentes de Seguridad de la Información**	
Nombre interno:	**Política de Gestión de Incidentes de Seguridad de la Información**	
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 GESTIÓN DE INCIDENTES DE SEGURIDAD 7

POLÍTICAS ESPECÍFICAS 7

CONSECUENCIAS Y SANCIONES 8

GLOSARIO 8

Consideraciones Generales

Objetivo

Establecer los lineamientos, en materia de seguridad de la información, para identificar, registrar, reportar y atender de manera oportuna los incidentes de seguridad de la información con la finalidad de mantener y preservar el correcto funcionamiento 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 y que este en contacto con los activos de TIC.

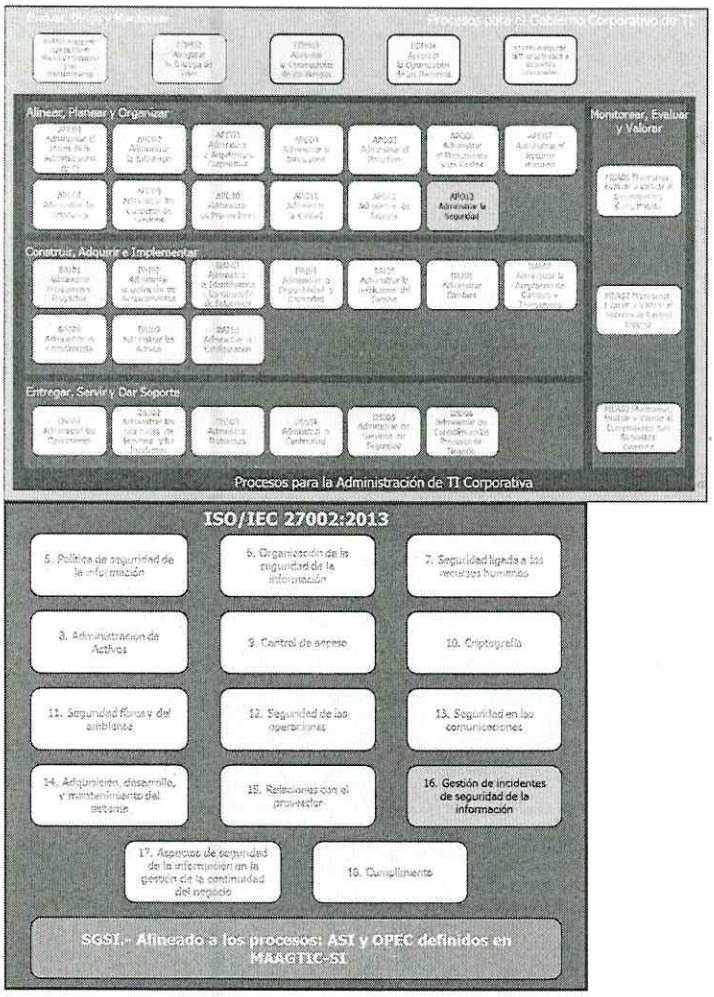
Marco Legal de Referencia

- 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	16.1.1. Responsabilidades y procedimientos. 16.1.2. Informe de eventos de seguridad de la información. 16.1.3. Informe de las debilidades de seguridad de la información. 16.1.4. Evaluación y decisión sobre los eventos de seguridad de la información. 16.1.5. Respuesta ante incidentes de seguridad de la información. 16.1.6. Aprendizaje de los incidentes de seguridad de la información. 16.1.7. Recolección de evidencia.

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 Gestión de Incidentes de Seguridad

Todos los usuarios, proveedores y terceros con alguna relación contractual con BANSEFI deben conocer los procedimientos para el reporte de los incidentes de seguridad que pudieran causar un impacto negativo a BANSEFI, por lo que todo incidente debe ser reportado de manera inmediata y oportuna aa Escritorio de Servicio de BANSEFI vía mail, telefónica o personal. Si el incidente amerita una investigación más profunda, se debe recabar toda la evidencia posible, dentro del marco legal y normativo aplicable.

Políticas específicas

1. Toda sospecha de incidente, violación y problema de seguridad que comprometa la integridad, disponibilidad y/o confidencialidad de los sistemas y servicios institucionales debe ser reportada tan rápido como sea posible al Responsable de Seguridad de la Información de la Institución (RSII) y a la Dirección de Contraloría Interna (DCI)
2. Los medios oficiales para reportar incidentes de seguridad son a través del Escritorio de Servicio y los medios institucionales que para el efecto dispongan el RSII y/o la DCI, quienes canalizarán el incidente de acuerdo con la Guía Técnica de Atención de Incidentes vigente.
3. El Responsable de Seguridad de la Información de la Institución y la Dirección de Infraestructura y Producción establecerán la Guía Técnica de Atención de Incidentes y establecerán el Equipo de Respuesta a Incidentes de Seguridad de TIC (ERISC).
4. El ERISC debe priorizar las acciones correspondientes a fin de garantizar en todo momento la continuidad de la operación del Banco y aislar o contener el incidente detectado.
5. Se debe mantener un registro auditable y detallado de todos los incidentes y eventos de seguridad de la información reportados, incluyendo los documentos mencionados en la Guía Técnica de Atención de Incidentes, los cuales se debe almacenar por al menos tres años, posterior al cierre del incidente.
6. Toda la documentación de los incidentes de seguridad de la información registrados debe estar clasificados como confidenciales y ser custodiados por la Gerencia de Control Operacional y de Seguridad de la Información.
7. Durante las reuniones del ERISC se deben llevar a cabo sesiones de lecciones aprendidas con los colaboradores involucrados en el manejo de incidentes, con base a los incidentes de seguridad de información presentados.
8. Los colaboradores involucrados en el manejo y solución de los incidentes de seguridad de la información deben estar capacitados en el uso de herramientas que se utilicen en la investigación y respuesta de los mismos.
9. Ningún usuario no autorizado debe intentar probar o corregir la debilidad que dio origen al incidente de seguridad de la información detectado.
10. Se debe evitar el uso de activos de información o mecanismos comprometidos por el incidente de seguridad de información.
11. En el caso de documentos físicos afectados, se debe conservar el original como evidencia del incidente ocurrido.
12. En caso de que a causa del incidente se vean afectados sistemas de cómputo se debe crear un respaldo de los mismos, con el objetivo de analizar el respaldo y dejar intacto el sistema comprometido para que pueda servir como evidencia en caso necesario.
13. Se deben cambiar de inmediato contraseñas o mecanismos de acceso a los sistemas afectados por el incidente.
14. En caso de que equipo de cómputo haya sido comprometido, se debe evitar utilizarlo para intercambio de información, incluso se debe desconectar el equipo de la red.
15. Se deben evitar acciones reactivas del intruso, mediante el uso de herramientas tecnológicas.
16. Se debe identificar la fuente del incidente a través de bitácoras y logs, considerando el uso de herramientas de análisis forense o de correlación de eventos.

17. Se debe preservar la escena (asegurar el área afectada por el incidente) y proteger la evidencia con el objetivo de preservar su admisibilidad y valor en caso de que sea necesario entablar una acción legal, para lo cual se deben tener en consideración las siguientes acciones:
    - Tomar fotografías, asegurar las bitácoras, tomar notas el estado del sistema, etc.
    - Identificar cada parte de la evidencia por medio de etiquetas, fechas, firmas, etc.
    - Usar acuses de recibo cuando la evidencia sea transferida a otra persona para su manejo, considerando la participación de dos testigos.
    - Controlar el acceso a la evidencia.
    - Definir quien tiene acceso a la evidencia.
    - Recolecta toda la información posible a cerca del incidente.
    - Evitar durante la cadena de custodia de la evidencia, que esta salga de territorio nacional.
18. Siempre que se autorice por parte del Grupo Estratégico de Seguridad de la Información se puede solicitar apoyo de proveedores externos para la solución del incidente de seguridad de la información.
19. Cuando se tenga evidencia de que el incidente de seguridad de la información fue provocado por colaboradores de BANSEFI, se deben tomar las acciones legales y disciplinarias conducentes.
20. En caso de que el incidente haya puesto en riesgo datos personales o bancarios de clientes y/o proveedores, el RSII debe informar el incidente y acciones correspondientes al Grupo de Dirección de TIC, a la Dirección de Contraloría Interna y según sea el caso a la Comisión Nacional Bancaria y de Valores, al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales o a las Instancias de Seguridad Nacional.

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
Incidente de seguridad	Como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a las Políticas de Seguridad de la Información del Banco
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
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada por una o más amenazas.