



POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN



Propiedad del Banco Nacional de Obras y Servicios Públicos, S.N.C.


Av. Javier Barros Sierra No. 515

Col. Lomas de Santa Fe, Delegación Álvaro Obregón

Ciudad de México, C.P. 01219

Tel. 52-70-12-00

La reproducción total o parcial de este documento podrá efectuarse mediante la autorización expresa de la Dirección de Contraloría Interna, otorgándole el crédito correspondiente.

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN			Vigente a partir de:		
				Día	Mes	Año
				23	03	2018

Hoja de Autorización

Elaboró

Elaboró

Dr. Gustavo Martínez Romero Subgerente de Seguridad de la Información 1	Rúbrica	Ing. Israel Rojas Luna Subgerente de Seguridad de la Información 2	Rúbrica
---	---------	--	---------

Elaboró

Ing. Juan Carlos Rodríguez Rodríguez Gerente de Seguridad de la Información	Rúbrica
---	---------

Autorizó

Lic. Saúl Olivares Ortega Director de Contraloría Interna y Responsable de la Seguridad de la Información en la Institución	Rúbrica
---	---------

Visto Bueno

Grupo Estratégico de Seguridad de la Información

Acuerdo número

GESI/SO.23.03.2018/02

MNOI50000113 Página 1 de 47	Aprobado/Autorizado					Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año			
	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					Día	Mes	Año
Elaboró JCRR/GMR/IRL						17	11	2017
Revisó SOO								

Sección de Control de Cambios


Revisión	Página (s) Modificada (s)	Descripción del Cambio	Fecha de Emisión
01	Todas	Se modificó todo el documento ya que hubo cambios en el estándar que se utiliza como guía para la generación de las Políticas General de Seguridad de la Información ISO/IEC 27001:2005 a ISO/IEC 27001:2013.	07/09/2017
02	Todas	Las modificaciones efectuadas se precisan en FAC No. MNO50000113-1.	07/11/2017
03	13	Directrices de clasificación: se actualizaron los artículos para información reservada e información confidencial. Se modificó el párrafo, en el cual se incluye el enlace en materia de transparencia por cada DGA, de acuerdo a la Ley.	18/01/2018
03	14	Protección de datos personales: se generó un lineamiento que da cumplimiento a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.	18/01/2018
03	14	Manejo de los medios de almacenamiento: Se fortaleció la política de gestión de medios extraíbles, señalando la inhabilitación de los puertos USB.	18/01/2018
03	18	Política de uso de los controles criptográficos: se consideró la red externa y cómputo en la nube.	18/01/2018
03	20	Salida de activos: se condieraron los equipos de cómputo externos.	18/01/2018
03	27	Gestión de seguridad de red: se fortaleció considerando la creación de perfiles de navegación, conforme a las necesidades de las áreas.	18/01/2018

MNOI50000113 Página 2 de 47	Aprobado/Autorizado					Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año			
Elaboró JCRR/GMR/IRL	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					Día	Mes	Año
Revisó SOO						17	11	2017

Contenido

Hoja de Autorización	1
Sección de Control de Cambios	2
Sección I Visión General	4
I.1. Objetivo	4
I.2. Alcance	4
I.3. Responsabilidades respecto del Manual	5
I.4. Marco jurídico y normativo	6
I.5. Instancias de autorización	6
Sección II. Políticas	7
II.1. Política General de Seguridad de Información	7
II.2. Organización para la seguridad de la información	8
II.3. Seguridad en los Recursos Humanos	10
II.4. Gestión de activos	11
II.5. Control de accesos	15
II.6. Cifrado	18
II.7. Seguridad física y ambiental	18
II.8. Políticas de seguridad en las operaciones	22
II.9. Seguridad de las comunicaciones	27
II.10. Adquisición, desarrollo y mantenimiento de los sistemas de información	32
II.11. Relación con proveedores	35
II.12. Gestión de incidentes en la seguridad de la información	37
II.13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio	39
II.14. Cumplimiento	40
Sección III. Infracciones a la Política de Seguridad	42
Anexo 1	45

MNOI50000113 Página 3 de 47 Elaboró JCRR/GMR/IRL Revisó SOO	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN						Vigente a partir de:		
							Día	Mes	Año
							23	03	2018

Sección I Visión General

I.1. Objetivo

El presente documento, tiene como propósito establecer las políticas generales de seguridad de la información de Banobras, tomando como guía el estándar ISO/IEC 27001:2013, mismas que deberán cumplirse con la finalidad de preservar la confidencialidad, integridad y disponibilidad de la información de la Institución.

I.2. Alcance

Las políticas contenidas en este documento, aplican para todo el personal que labore o preste servicios en la Institución; así como, para cualquier persona que utilice las tecnologías de la información y comunicaciones de la Institución.

Los lineamientos, procedimientos, directrices y guías desarrolladas a partir de estas políticas, deben aplicarse en todas las fases del ciclo de vida de la información: generación, distribución, almacenamiento, procesamiento, transporte, acceso, consulta y destrucción; para todos los sistemas, infraestructuras tecnológicas y las instalaciones que los soportan.

MNOI50000113 Página 4 de 47 Elaboró JCRR/GMR/IRL Revisó SOO	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						17	11	2017

I.3. Responsabilidades respecto del Manual

Responsable	Responsabilidad
Grupo Estratégico de Seguridad de la Información (GESI)	<ul style="list-style-type: none"> • Dar visto bueno al documento. • Proponer mejoras.
Responsable de la Seguridad de la Información en la Institución (RSII)	<ul style="list-style-type: none"> • Revisar este documento. • Autoriza el presente manual en apego al documento de Objetivos y Lineamientos del Sistema de Control Interno y a la Guía para la Emisión de la Normativa Interna de Banobras.
Gerencia de Seguridad de la Información	<ul style="list-style-type: none"> • Gestionar la actualización de estas políticas. • Elaborar propuestas de modificaciones y mejora a las presentes políticas. • Coordinar la revisión y actualización del presente documento cuando se requiera o derive de: <ul style="list-style-type: none"> ➢ Modificaciones al marco jurídico y normativo aplicable. ➢ Observaciones y/o recomendaciones por parte de las instancias de supervisión y fiscalización, así como, de las autoridades competentes. ➢ Cambios en la estructura organizacional de Banobras; y, mejora del proceso de calidad regulatoria. ➢ Mejoras al proceso de tecnologías de la información y comunicaciones. • Enviar a guarda y custodia el documento. • Gestionar la publicación de este documento en la Normateca.
Gerencia de Control Interno	<ul style="list-style-type: none"> • Revisar el documento en apego a los Objetivos y Lineamientos del Sistema de Control Interno de Banobras.
Gerencia de Reingeniería de Procesos	<ul style="list-style-type: none"> • Gestionar la emisión y difusión de este manual.
Direcciones Generales Adjuntas	<ul style="list-style-type: none"> • Promover, aplicar y cumplir lo señalado en este documento. • Proponer cambios en el ámbito de sus responsabilidades para su mejora y/o actualización.

MNOI50000113 Página 5 de 47 Elaboró JCRR/GMR/IRL Revisó SOO	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						17	11	2017

I.4. Marco jurídico y normativo

A continuación se señalan los ordenamientos jurídicos en que se sustentan las políticas del presente documento, en el entendido que es una referencia efectuada de manera enunciativa más no limitativa:

- Ley General de Transparencia y Acceso a la Información Pública
- Ley Federal de Transparencia y Acceso a la Información Pública
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
- Ley de Instituciones de Crédito
- Disposiciones de Carácter General Aplicables a las Instituciones de Crédito.
- Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Nacional Digital, en Materia de Tecnologías de la Información y Comunicaciones, y en la Seguridad de la Información, así como establecer el Manual Administrativo de Aplicación General en dichas materias.
- Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.
- Manual General de Organización de Banobras.
- Manual Administrativo de Aplicación General en Materia de Control Interno.
- Objetivos y Lineamientos del Sistema Control Interno.
- Código de Conducta.
- Guía para la Emisión de la Normativa Interna.

I.5. Instancias de autorización

El presente documento es autorizado por el Responsable de la Seguridad de la Información quien da conocimiento al Grupo Estratégico de Seguridad de la Información (GESI), lo anterior de conformidad con la Guía para la Emisión de la Normativa Interna, emitida por la Gerencia de Reingeniería de Procesos y de acuerdo con lo establecido por el Consejo Directivo en el Documento Objetivos y Lineamientos del Sistema de Control Interno en Banobras.

MNOI50000113 Página 6 de 47 Elaboró JCRR/GMR/IRL Revisó SOO	Aprobado/Autorizado					Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año	Día	Mes	Año
	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					17	11	2017

Sección II. Políticas

II.1. Política General de Seguridad de Información

Objetivo: Definir las políticas que propicien una adecuada protección de la información de Banobras.

II.1.1. Definición de la Política General de Seguridad de la Información

Política de Seguridad de la Información de Banobras:

“Banobras reconoce que la información de su propiedad y la de sus clientes, así como, los activos de información y la infraestructura que la soporta, son esenciales para la continuidad del negocio y para el cumplimiento de su misión y su visión; por lo que es fundamental protegerlos, restringiendo el acceso, uso y revelación, conforme a sus intereses institucionales”.


II.1.2 Políticas Generales de Seguridad de Información

1. La Dirección General debe asegurarse de que existan los recursos humanos, materiales y tecnológicos para implementar planes y programas en aspectos de seguridad de la información.
2. La Dirección General debe nombrar un Responsable de Seguridad de la Información Institucional (RSII).
3. El RSII debe establecer un Grupo Estratégico de Seguridad de la Información (GESI), que será responsable de implantar y mantener un Sistema de Gestión de la Seguridad de la Información (SGSI).
4. El RSII debe coordinar la revisión anual del cumplimiento de los objetivos y las métricas de seguridad de la información.
5. El RSII, a través de la Gerencia de Seguridad de la Información, debe verificar que se definan e implementen controles que se deriven de este Manual de Políticas de Seguridad.
6. Las Direcciones Generales Adjuntas, deben alinear sus procesos de gestión y operación, a este Manual de Políticas Generales de Seguridad de la Información.
7. El RSII, a través de la Gerencia de Seguridad de la Información, debe verificar que se desarrolle y cumpla la implementación de controles del Sistema de Gestión de Seguridad de la Información.

II.1.3. Revisión de la Política General de Seguridad de la Información

En este documento se establecen las Políticas Generales de Seguridad de la Información, que tienen efecto inmediato a partir de la fecha de su autorización y publicación cuya revisión debe ser de manera anual para cumplir las necesidades de la Institución en materia de seguridad de la información.

MNOI50000113 Página 7 de 47	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
Elaboró JCRR/GMR/IRL	Dirección de Contraloría Interna / Responsable de Seguridad de la Información								
Revisó SOO							17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN					Vigente a partir de:		
						Día	Mes	Año
						23	03	2018

II.1.4. Conocimiento de la Política General de Seguridad de la Información de Banobras

El Manual de Políticas Generales de Seguridad de la Información de Banobras, es un documento de carácter normativo, por lo que es fundamental su difusión entre todos los colaboradores de la Institución, para su conocimiento.

II.2. Organización para la seguridad de la información

Objetivo: Establecer la organización necesaria para fortalecer la seguridad de la información dentro de la Institución, en cumplimiento con las regulaciones aplicables.


II.2.1. Organización

Roles y responsabilidades de la seguridad de la información

En cumplimiento a la normativa externa e interna aplicable, la administración de la seguridad de la información institucional de Banobras, corre a cargo del siguiente grupo de servidores públicos:

1. El Director General de Banobras, quien tiene la responsabilidad de promover la seguridad de la información Institucional.
2. El RSII, es responsable del cumplimiento de las normativas aplicables a la seguridad de la información de la Institución.
3. El GESI debe atender oportunamente la formación de los grupos y equipos necesarios para hacer cumplir las funciones establecidas en el proceso de Administración de la Seguridad de la Información (ASI) y en el Proceso de Operación de los Controles de Seguridad (OPEC) y del ERISC del MAAGTICSI.
4. El Director de Tecnologías de Información y Comunicaciones, como titular de la UTIC, es responsable de asegurar la alineación operativa de TIC a la normativa aplicable en materia de seguridad de la Información.
5. Las direcciones de Recursos Materiales y Jurídico, deben asegurarse de que los contratos de prestación de servicios TIC, cuenten con cláusulas que promuevan el cumplimiento de esta política.
6. Los mandos medios y superiores de las áreas de los procesos sustantivos y de apoyo, son responsables del cumplimiento de estas Políticas Generales de Seguridad de la Información.
7. Todos los colaboradores en general que presten sus servicios a Banobras, son responsables de conocer y cumplir las Políticas de este manual que les corresponda.

MNOI50000113 Página 8 de 47	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN						Vigente a partir de:		
							Día	Mes	Año
							23	03	2018

Segregación de funciones

Son los mandos medios y superiores de las áreas, que tienen a su cargo los procesos sustantivos y de apoyo de la Institución, quienes deben definir conforme al manual de organización, las funciones para que se preserve una adecuada segregación de actividades, por tipo de producto, operación, monto, nivel jerárquico, área, unidad de negocio o administrativa y comités.

Esta segregación debe evitar conflictos de interés que minimicen al máximo el riesgo de ser juez y parte en tareas de ejecución, validación y autorización.

Contacto con autoridades

En caso de ocurrir algún incidente de seguridad que involucre algún contacto con las autoridades en materia de seguridad de la información, será el RSII quien tendrá el trato con las autoridades, por medio del enlace designado por el RSII para tal efecto.

Contacto con grupos de interés especial

El RSII coordina el proceso de comunicación con grupos de interés especial, previo análisis de la necesidad de contacto con estos grupos, entre los que se incluyen, pero no de manera limitativa:

1. Consultorías
2. Asociaciones
3. Publicaciones especializadas
4. CERTs.

Seguridad de la información en la gestión de proyectos TIC's

El Director de Tecnologías de Información y Comunicaciones debe implementar los estándares funcionales, operativos y tecnológicos, que deben incorporarse en el desarrollo de proyectos, adquisición de servicios y componentes de tecnologías de información y comunicación.

El RSII a través de la Gerencia de Seguridad de la Información debe validar el cumplimiento de los estándares funcionales, operativos y tecnológicos mínimos indicados en este Manual.


II.2.2. Dispositivos móviles

Política de dispositivos móviles y acceso remoto

Es responsabilidad del personal, proteger los equipos que se le han asignado para el desempeño de sus funciones siguiendo las medidas de seguridad que a continuación se describen, como mínimo:

1. No exponer el equipo a condiciones de inseguridad física y/o ambiental.
2. Proteger las claves de acceso que le han sido asignadas

MNOI50000113 Página 9 de 47	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año				
Elaboró JCRR/GMR/IRL	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						Día	Mes	Año
Revisó SOO							17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN					Vigente a partir de:		
						Día	Mes	Año
						23	03	2018

3. No dejar el equipo desatendido en lugares públicos o en lugares donde pueda ser sustraído o dañado con relativa facilidad, como autos, maletas de viaje, cerca de ventanas, en el piso, mesas de comida o bebida, etc.

La Dirección de Recursos Materiales y la Dirección de Tecnologías de Información y Comunicaciones, en su ámbito, deben asegurar que todos los equipos móviles que Banobras asigne al personal para el cumplimiento de sus funciones, cuenten con las herramientas necesarias para propiciar la seguridad de la información. Estas herramientas, incluyen, en forma enunciativa, más no limitativa: antivirus, software de cifrado, aplicaciones seguras, entre otras.

Los equipos móviles de uso personal, no otorgados por Banobras, que requieran acceso a los servicios de la Institución, deben contar con la validación de la Gerencia de Seguridad de la Información, de que cuenta con los elementos tecnológicos de seguridad informática.

II.3. Seguridad en los Recursos Humanos

Objetivo: Definir las políticas que aseguren una adecuada protección de la información de Banobras por parte del personal interno y externo.

II.3.1 Previo al empleo

Selección

La selección del personal es responsabilidad de la Dirección de Recursos Humanos, quien realiza la evaluación integral del personal, asegurando que el perfil de competencias del candidato es el más adecuado para cumplir con el puesto requerido.

Términos y condiciones de empleo

La Dirección de Recursos Humanos, debe hacer de conocimiento del personal de la Institución, las cláusulas de confidencialidad; para los casos del personal subcontratado y honorarios los contratos deberán incluir cláusulas que refieran a la confidencialidad de la información y su no divulgación de la misma.


II.3.2 Durante el empleo

Responsabilidades de las Direcciones

Es responsabilidad de la Dirección de Recursos Humanos de informar a todo el personal de nuevo ingreso de la existencia de este Manual de Políticas Generales de Seguridad de la Información.

Es responsabilidad de los mandos medios y superiores de las áreas, promover y hacer del conocimiento a todo personal a su cargo la existencia de este Manual de Políticas Generales de Seguridad de la Información.

MNOI50000113 Página 10 de 47	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN						Vigente a partir de:		
							Día	Mes	Año
							23	03	2018

Concientización, educación y formación en seguridad de la información

Corresponde a las Direcciones Generales Adjuntas de cada área, a través de sus mandos medios y superiores, promover en todo momento, la participación en los procesos de concientización, capacitación y prevención a incidentes de seguridad, a todo el personal a su cargo, para fortalecer una cultura de seguridad de la información.

La Dirección de Recursos Humanos deberá incluir como parte de la inducción al personal de nuevo ingreso, el material informativo necesario sobre seguridad de la información.

El RSII a través de la Gerencia de Seguridad de la Información debe establecer programas orientados a fortalecer y afianzar una cultura de seguridad de la información en el personal de la Institución. Asimismo, debe coordinar los programas o campañas de sensibilización en temas relativos a la seguridad de la información y debe mantener evidencia de los mismos.

Proceso disciplinario

Todo personal de la Institución debe reportar por medio de banseg@banobras.gob.mx, cualquier falta u omisión a las Políticas Generales de Seguridad de la Información, la Gerencia de Seguridad de la Información debe notificar al RSII, para que de acuerdo a la gravedad, informe al Órgano Interno de Control y a su vez a la Dirección de Recursos Humanos para que en el ámbito de sus competencias resuelvan lo conducente.

II.3.3 Terminación o separación del puesto

Responsabilidades de la terminación o separación del puesto

Toda terminación laboral, debe apegarse a los procesos involucrados de las Direcciones de Recursos Humanos, Recursos Materiales, Contraloría Interna y de Tecnologías de Información y Comunicaciones, promoviendo que la separación del puesto sea de una manera ordenada, disminuyendo así el riesgo hacia los activos de información que son propiedad de la Institución.

Son los mandos medios y superiores de las áreas, los responsables de comunicar de forma inmediata y oportuna a la Dirección de Recursos Humanos y a la Gerencia de Seguridad de la Información la finalización del nombramiento o cambio de puesto o funciones de los empleados, prestadores de servicios o terceros.

La Dirección de Tecnologías de Información y Comunicaciones, debe notificar de forma oportuna al Responsable Funcional, la afectación de la inhabilitación de un usuario, que por las reglas de negocio tenga funciones específicas configuradas, lo anterior para disminuir riesgos en la operación de la Institución.

II.4. Gestión de activos

Objetivo: Asegurar la protección de la información institucional y de los activos de información que la contengan.

MNOI50000113 Página 11 de 47	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Elaboró JCRR/GMR/IRL Revisó SOO	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					17	11	2017

II.4.1. Responsabilidad por los activos

Inventario de activos

Un activo de información, es un elemento reconocible que almacena datos, registros, información en cualquier medio y que tiene las características siguientes:

1. Es valioso para Banobras por la información que contiene.
2. No es de fácil reemplazo y en algunos casos pudiera ser irreplicable.

Es responsabilidad de los mandos medios y superiores de las áreas de cada dirección de Banobras identificar sus activos de información.

La Dirección de Tecnologías de Información y Comunicaciones, debe mantener un registro actualizado sobre los activos informáticos que soporten los servicios TIC de Banobras.

El GESI debe coordinar la identificación de los activos esenciales de la Institución, como lo señala el MAAGTICSI; y promover su protección de estos activos.

Propiedad de los activos

Toda información que se genere a partir de un activo propio, arrendado o contratado por un servicio, es propiedad de Banobras.

Todo activo de información debe ser asignado a un responsable y autorizado por su jefe inmediato (nivel mínimo Gerente).

La persona responsable del activo debe:


1. Salvaguardar la integridad, disponibilidad y confidencialidad del activo.
2. Hacer uso del activo únicamente para los propósitos y actividades de la Institución.
3. Reportar cualquier incidente o problema relacionado con el activo de información.
4. Cualquier omisión (con dolo o involuntaria) de reportar algún incidente relacionado a cualquier activo bajo su guarda y custodia, se considera una falta hacia la seguridad de la información que en su caso debe reportarse a las autoridades competentes.
5. Realizar lo necesario para mantener el activo de información en buenas condiciones que garantice y cumplan su función.

Todos los aplicativos y sistemas institucionales que soporten algún proceso, deben tener un responsable funcional del área de negocio y ser integrados por la Dirección de Tecnologías de Información y Comunicaciones, a su catálogo de servicios y proveer los recursos necesarios así como las herramientas tecnológicas que ayuden a fortalecer la seguridad lógica y física de la información del activo; así como, el resguardo del licenciamiento correspondiente..

Uso aceptable de los activos

Banobras considera que los recursos para el procesamiento de la información son prioritarios para el desarrollo de los procesos de negocio y el adecuado cumplimiento de sus funciones; por lo que, es responsabilidad del personal, el salvaguardar de cualquier alteración o modificación no autorizada, daño o destrucción que limite su disponibilidad para el adecuado desarrollo de sus actividades.

MNOI50000113 Página 12 de 47	Aprobado/Autorizado					Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año			
Elaboró JCRR/GMR/IRL	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					Día	Mes	Año
Revisó SOO						17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN			Vigente a partir de:		
				Día	Mes	Año
				23	03	2018

El uso aceptable de los activos de información incluye:

1. Evitar daños temporales o permanentes a los activos de información, causados por accidentes, imprudencias o daños dolosos.
2. Reportar cualquier falla o mal funcionamiento detectado.
3. Informar a los jefes inmediatos, de cualquier falla o vulnerabilidad de los activos de información.
4. Notificar de cualquier necesidad de protección o mejora, en los controles para los activos de información.
5. Usar los activos de información únicamente para los propósitos de la Institución.
6. Reportar cualquier uso no adecuado del activo de información a su jefe inmediato.

Devolución de activos

Todo personal que preste sus servicios a Banobras, al concluir sus funciones, tiene la obligación de entregar los activos informáticos asignados en buen estado físico y de operación, así como los activos de información y la documentación correspondiente.

II.4.2 Clasificación de la información

Directrices de clasificación


Cada área debe clasificar y etiquetar su información de acuerdo a la Ley General de Transparencia y Acceso a la Información Pública y la Ley Federal de Transparencia y Acceso a la Información Pública.

La información debe clasificarse como:

1. **Información reservada:** es la información creada y usada por Banobras, en la realización de sus procesos de negocio, que corresponda a lo dispuesto en los artículos 113, 114 y 115 de la Ley General de Transparencia y Acceso a la Información Pública y los artículos 110, 111 y 112 de la Ley Federal de Transparencia y Acceso a la Información Pública.
2. **Información confidencial:** es la información creada y usada por Banobras, en la realización de sus procesos de negocio, que corresponde a lo previsto en el artículo 142 de la Ley de Instituciones de Crédito, y a lo dispuesto en los artículos 116, 117, 118, 119 y 120 de la Ley General de Transparencia y Acceso a la Información Pública y los artículos 113, 114, 115, 116 y 117 de la Ley Federal de Transparencia y Acceso a la Información Pública. Su divulgación externa debe estar en apego a los términos de las disposiciones aplicables.
3. **Información pública:** toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados en el ámbito federal, es pública, accesible a cualquier persona y sólo podrá ser clasificada excepcionalmente como reservada o confidencial, en términos de la Ley General de Transparencia y Acceso a la Información y la Ley Federal de Transparencia y Acceso a la Información.

Todas las áreas de la Institución, tienen la obligación de designar un enlace en materia de transparencia, quien será responsable al interior de su DGA, de coordinar y dar cumplimiento puntual a los diferentes requerimientos en la materia, lo anterior, con base en el Manual de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. En caso de

MNOI50000113 Página 13 de 47	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Elaboró JCRR/GMR/IRL Revisó SOO	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN					Vigente a partir de:		
						Día	Mes	Año
						23	03	2018

solicitarse información a través de la Ley de Transparencia, la Unidad Administrativa competente deberá solicitar la clasificación de información al Comité de Transparencia.

Etiquetado de la información

La información clasificada como reservada o confidencial, debe ser confirmada por el Comité de Transparencia, y debe contener la leyenda de “clasificación” de conformidad con las disposiciones aplicables.

El etiquetado de la información, se aplica sólo para la información clasificada.

Protección y manejo de la información

1. La Dirección de Tecnologías de la Información y La Dirección de Recursos Materiales deben proveer mecanismos de protección de la información, de acuerdo a su clasificación.
2. Todo activo de información protegido según su clasificación, debe contar con un control de acceso, donde se establezca qué personas son las autorizadas para el manejo de la información en el activo
3. Los funcionarios están obligados a no revelar a terceras personas la información que conozcan por el ejercicio de sus funciones, por lo que están obligados a mantenerla confidencial y privada para evitar su divulgación.
4. Los usuarios de acuerdo a sus funciones podrán trabajar y hacer uso de la información institucional en los activos de información asignados y resguardar la versión final.

Protección de datos personales

En materia de protección de datos personales, se deberá cumplir lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como considerar lo siguiente:

- Datos personales
- Medidas de seguridad
- Tratamiento de datos personales

Todo tratamiento de datos personales que efectúen las áreas de cada dirección, deberán justificar con un fin concreto, lícito, explícito y legítimo, relacionado con las atribuciones que la normatividad le aplique.

Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, las áreas deberán considerar y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como cuidar su confidencialidad, integridad y disponibilidad.

MNOI50000113 Página 14 de 47	Aprobado/Autorizado					Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año	Día	Mes	Año
	Elaboró JCRR/GMR/IRL Revisó SOO	Dirección de Contraloría Interna / Responsable de Seguridad de la Información				17	11	2017

II.4.3. Manejo de los medios de almacenamiento

Gestión de medios extraíbles

La Dirección de Tecnologías de Información y Comunicaciones, debe proporcionar los servicios necesarios para asegurar el manejo de la información dentro de Banobras.

Está restringido el uso de medios removibles de almacenamiento, por lo que se deshabilita la funcionalidad de los puertos USB y unidades ópticas de grabación en todos los equipos de cómputo institucionales de Banobras; la autorización de uso de los medios removibles debe ser tramitada, justificada y autorizada por la dirección del solicitante, a través de la mesa de servicios de Banobras con el visto bueno de la Gerencia de Seguridad de la Información.

El RSII, a través de la Gerencia de Seguridad de la Información, debe concientizar sobre el buen uso y mejores prácticas del manejo de medios removibles de almacenamiento, para el traslado de la información de Banobras.

Eliminación de medios

La Dirección de Tecnologías de Información y Comunicaciones debe contar con procedimientos para asegurar la baja y el borrado confiable de los activos informáticos.

Todo activo informático que contenga información de Banobras, debe contar con procedimientos de migración, respaldo y borrado seguro antes de que el activo sea eliminado.

El RSII a través de la Gerencia de Seguridad de la Información debe verificar el mecanismo empleado para el cumplimiento de esta actividad.

Transferencia física de medios

La Dirección de Tecnologías de Información y Comunicaciones debe contar con procedimientos seguros que garantice el traslado de los medios de información, mediante un mecanismo auditable; mismo que puede ser verificado por El RSII, a través de la Gerencia de Seguridad de la Información.

II.5. Control de accesos

Objetivo: Asegurar que sólo usuarios autorizados accedan a los servicios de información de Banobras y que lo hagan a través de privilegios adecuados a su perfil o rol en la Institución.

II.5.1 Requisitos de negocio para el control de acceso

Política de control de acceso

El RSII, a través de la Gerencia de Seguridad de la Información debe establecer controles de seguridad para la Gestión de Cuentas de Usuarios en la Institución.

MNOI50000113 Página 15 de 47	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Elaboró JCRR/GMR/IRL Revisó SOO	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					17	11	2017

Control de acceso a las redes y servicios asociados

1. Los controles de acceso a los servicios de información, deben asignarse con base en los roles y perfiles de los usuarios, según el servicio requerido.
2. La autenticación de usuarios, debe hacerse a través de canales cifrados y haciendo uso de contraseñas encriptadas.

II.5.2 Gestión del acceso a usuarios

Gestión de altas/bajas/cambios en el registro de usuarios

Todos los aplicativos y servicios TIC institucionales deben tener un registro de altas, bajas y cambios siguiendo lo dispuesto en el proceso de Gestión de Cuentas de Usuario, descrito en las Directrices de Gestión de Cuentas de Usuario.

Gestión de los derechos de acceso asignados a usuarios

Todos los accesos a servicios TIC y aplicativos deben ser asignados de acuerdo a su función, mediante roles y perfiles, propiciando una correcta segregación de funciones.

Gestión de derechos de acceso con privilegios especiales

Los usuarios con privilegios especiales de acceso, deben contar con la autorización del responsable del activo.

Las cuentas de usuarios con privilegios especiales de acceso deben ser diferentes a las cuentas que utilizan para la operación.

Gestión de información confidencial de autenticación de usuarios

La Dirección de Tecnologías de Información y Comunicaciones debe asegurar la confidencialidad de la entrega de contraseñas en todos sus procesos.

Revisión de los derechos de acceso de usuarios

Los derechos de acceso de los usuarios deben ser revisados anualmente por la Gerencia de Seguridad de la Información y validados por las áreas de negocio.

Retirada o adaptación de los derechos de acceso

Es responsabilidad de la Dirección de Recursos Humanos, notificar las bajas o cambios de adscripción del personal, a la Gerencia de Seguridad de la Información, para la ejecución del cambio o remoción de los derechos de acceso.

Es responsabilidad de los mandos medios y superiores de las áreas que cuenten con personal externo, que tengan acceso a los servicios TIC y a los aplicativos Institucionales, notificar las bajas o cambios de funciones del personal, a la Gerencia de Seguridad de la Información, para la ejecución del cambio o remoción de los derechos de acceso.

MNOI50000113 Página 16 de 47	Aprobado/Autorizado					Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año			
Elaboró JCRR/GMR/IRL	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					Día	Mes	Año
Revisó SOO						17	11	2017

II.5.3 Responsabilidades del usuario

Uso de información confidencial para la autenticación

Todo el personal de Banobras es responsable de su contraseña, la cual es confidencial y debe mantenerse secreta.

Para hacer uso de la infraestructura tecnológica de Banobras, los usuarios deben aceptar los términos y condiciones de la Política de Uso Aceptable de Aplicativos y Servicios Tecnológicos Institucionales de Banobras.

El usuario debe cambiar la contraseña inicial, después de que le fue asignada al sistema o aplicativo, mismo que debe estar configurado para que esto sea de forma automática.

Solo deben tener acceso a los aplicativos institucionales los usuarios autorizados, con la cuenta asignada para tal efecto; en ningún caso deben acceder usando una cuenta diferente.

II.5.4 Control de acceso a sistemas y aplicaciones

Restricción del acceso a la información

La Dirección de Tecnologías de Información y Comunicaciones debe asegurar que las aplicaciones cuenten con un control de acceso centralizado, donde el usuario debe ser identificado con un user-id y una contraseña segura.

La administración de los derechos de acceso a los aplicativos, directorio activo y bases de datos institucionales, se realiza mediante roles y/o perfiles.

Todos los usuarios con acceso a los aplicativos institucionales deben identificarse en forma única y contar con los derechos de acceso asignados previamente, de acuerdo a su rol y perfil.

Procedimientos seguros de inicio de sesión

Todo aplicativo institucional debe contar con las configuraciones necesarias para limitar el tiempo de la sesión activa.


Gestión de contraseñas de usuario

Los sistemas o aplicativos institucionales deben contar con un control de contraseñas seguro y un mecanismo de historial, para evitar la no reutilización de las mismas.

Uso de herramientas de administración de sistemas

La Dirección de Tecnologías de Información y Comunicaciones debe restringir y controlar estrictamente el uso de herramientas que puedan estar en capacidad de anular los controles del mismo sistema; en caso de que requiera utilizar este tipo de herramientas por causas debidamente justificadas, se debe informar al RSII, a través de la Gerencia de Seguridad de la Información.

MNOI50000113 Página 17 de 47	Aprobado/Autorizado					Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año			
Elaboró JCRR/GMR/IRL	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					Día	Mes	Año
Revisó SOO						17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN						Vigente a partir de:		
							Día	Mes	Año
							23	03	2018

Control de acceso al código fuente de los programas

La Dirección de Tecnologías de Información y Comunicaciones debe contar con un mecanismo para controlar el acceso a la consulta del código fuente de los sistemas o aplicativos de la Institución.

II.6. Cifrado

Objetivo: Asegurar el uso adecuado y eficaz del cifrado para proteger la confidencialidad, autenticidad o integridad de la información.

II.6.1 Controles criptográficos

Política de uso de los controles criptográficos

Para el envío de información electrónica hacia una red externa, la Dirección de Tecnologías de Información y Comunicaciones debe proporcionar mecanismos que permitan cifrar dicha información.

Gestión de claves y certificados

Las claves y certificados del cifrado que se utilicen en el almacenamiento y transmisión de la información, deben ser resguardados por la Gerencia de Seguridad de la Información.

II.7. Seguridad física y ambiental

Objetivo: Asegurar que sólo usuarios autorizados tengan acceso a las instalaciones de procesamiento de información, para prevenir cualquier daño físico o interferencia con los equipos o la instalación.

II.7.1 Áreas seguras

Perímetro de seguridad física

El RSII, a través de la Gerencia de Seguridad de la Información y en conjunto con la Dirección de Recursos Materiales, debe informar al GESI la designación de las áreas seguras de la Institución.


La Dirección de Recursos Materiales y la Dirección de Tecnologías de Información y Comunicaciones son responsables de definir un espacio físico seguro, que cumpla con lo mínimo para asegurar el procesamiento y almacenamiento de la información.

Se deberán de implementar los mecanismos necesarios que permitan limitar el acceso a las áreas seguras, solamente para el personal autorizado

No se permitirá el acceso a las áreas seguras al personal que no esté expresamente autorizado.

Es responsabilidad de las personas autorizadas a las áreas restringidas, permitir el acceso al personal ajeno a éstas.

MNOI50000113 Página 18 de 47	Aprobado/Autorizado					Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año			
Elaboró JCRR/GMR/IRL	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					Día	Mes	Año
Revisó SOO						17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN					Vigente a partir de:		
						Día	Mes	Año
						23	03	2018

Control físico de entrada

Las áreas seguras deben contar con mecanismos de ingreso que consideren la autorización, registro y validación de los accesos.

Seguridad de oficinas, despachos y recursos

La Dirección de Recursos Materiales debe proporcionar a cada empleado un espacio físico asignado que cuente con mobiliario protegido para el resguardo de información física.

La Dirección de Recursos Materiales debe proporcionar a cada empleado un acceso controlado para el uso de las instalaciones de acuerdo a sus funciones dentro de la Institución, el acceso a áreas restringidas debe ser autorizado por la dirección responsable del área restringida.

Protección contra amenazas externas y ambientales

La Dirección de Recursos Materiales debe facilitar los recursos necesarios para establecer perímetros de seguridad física con el fin de proteger áreas que contengan información crítica de la Institución, así como el área de procesamiento de datos.

Los perímetros de seguridad física deben estar definidos e identificados.

El perímetro de seguridad física de los centros de cómputo de Banobras, debe considerar los requerimientos definidos en el Manual de Políticas y Procedimientos para los Recursos Materiales y Servicios Generales en Banobras.

El trabajo en áreas seguras

Las áreas de acceso a las instalaciones de Banobras, deben ser controladas y debe restringirse el acceso a las áreas seguras para evitar el acceso no autorizado.

II.7.2. Seguridad de los equipos

Ubicación y protección de equipos

Todo equipo que almacene, procese o transmita información esencial para la operación de Banobras, debe ser protegido para disminuir el riesgos de amenazas ambientales o físicas; tales como, inundaciones, rayos, sismos, radiaciones, polvo, humedad, vandalismo, explosión, humo etc.

La Institución debe contar con un centro de datos primario, que garantice la protección de los equipos que soportan los procesos institucionales, así como, los servicios de soporte.


Además, debe contar con un centro de datos secundario, cuya ubicación geográfica sea diferente del centro de datos primario, que garantice la continuidad de las operaciones, ante una contingencia.

Todos los equipos de soporte que se encuentran fuera de los centros de datos, deben estar ubicados y protegidos en áreas restringidas, de acuerdo a las especificaciones del fabricante.

Para lo anterior, la Dirección de Tecnologías de Información y Comunicaciones debe considerar:

- Que ambos centros de datos, principal y secundario, cumplan con los estándares internacionales y con la norma mexicana "Centros de Datos de Alto Desempeño Sustentable y Energético – Requisitos y Métodos de Comprobación".

MNOI50000113 Página 19 de 47	Aprobado/Autorizado					Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año			
Elaboró JCRR/GMR/IRL	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					Día	Mes	Año
Revisó SOO						17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN			Vigente a partir de:		
				Día	Mes	Año
				23	03	2018

- Que ambos centros de datos, principal y secundario, consideren los estándares mínimos para la protección física y ambiental; siguiendo las Directrices de Seguridad de Cómputo Institucional.

Para los centros de datos de Banobras debe estar provisto como mínimo de:

- Señalización adecuada de todos los equipos y elementos de seguridad, como luces de emergencia, etc.; que establezcan las normas de seguridad industrial y de salud ocupacional.
- Sistemas de aire acondicionado de precisión redundante y adecuada, para tener una temperatura idónea para el correcto funcionamiento de los equipos y prevenir fallas.
- Unidades de alimentación ininterrumpida (UPS), redundante.
- Alarmas de detección de humo y sistemas automáticos de extinción de fuego.
- Extintores y equipo contra incendio con capacidad de detener el fuego generado por equipo eléctrico.
- Contar con un control de acceso sólo para personal autorizado.

Instalaciones de suministro

Las instalaciones de procesamiento de información que opera la Institución, debe contar con equipos que suministren de energía eléctrica de forma ininterrumpida por al menos 24 horas, tales como generadores y UPS, así como, sus procedimientos documentados en caso de contingencia.

Seguridad en cableado

El cableado debe cumplir con las especificaciones del fabricante para minimizar errores físicos. No debe estar expuesto a condiciones ambientales que aceleren su deterioro, tales como: agua, corrosivos, exceso de calor, etc.

Todo el cableado de datos debe estar debidamente etiquetado en los paneles de parcheo y adecuadamente instalado, para facilitar su mantenimiento. Cuando exista un cambio en el cableado, se debe actualizar la memoria técnica correspondiente.

El cableado de datos y de energía debe estar separado en distintitas canaletas o ductos, para evitar interferencias, siguiendo las normas aplicables.


El acceso a los cuartos donde residan los paneles de parcheo y tableros de distribución eléctrica, deben ser restringido al personal responsable de la red y del soporte técnico o mantenimiento de la misma.

Mantenimiento de los equipos

Todo activo de información debe contar con programas de soporte y mantenimiento, para su correcto funcionamiento y disponibilidad.

La Dirección de Tecnologías de Información y Comunicaciones debe validar que los mantenimientos que se lleven a cabo, sean realizados por personal capacitado, de acuerdo a las

MNOI50000113 Página 20 de 47 Elaboró JCRR/GMR/IRL Revisó SOO	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN					Vigente a partir de:		
						Día	Mes	Año
						23	03	2018

especificaciones del fabricante. Asimismo, asegurarse que se conserve un registro de todos los mantenimientos preventivos y correctivos efectuados.

Salida de activos

La Gerencia de Seguridad de la Información en coordinación con la Gerencia de Servicios Generales debe establecer un procedimiento para el registro de entrada y salida de equipos de cómputo (internos y externos).

Seguridad de los equipos y activos fuera de las instalaciones

Todo equipo que almacene, procese, transmita información crítica de Banobras debe operar dentro de las instalaciones de la Institución o de las contratadas para tal efecto.

La Dirección de Tecnologías de Información y Comunicaciones debe establecer un procedimiento que asegure que la información y/o configuraciones no queden expuestas.

Los equipos que por necesidad salgan de las instalaciones de Banobras sean propias o arrendadas, deben apegarse al procedimiento de salida de equipos que se encuentra como anexo en el Manual de Políticas y Procedimientos para los Recursos Materiales y Servicios Generales en Banobras.

Los equipos de cómputo móviles (laptops) de Banobras deben ser protegidos con las medidas y mecanismos de seguridad de la información, con los que cuente la Institución.

Los equipos de cómputo móviles (laptops) de Banobras que se encuentran fuera de las instalaciones y requieran conectarse a la red interna de Banobras solo podrán realizarlo por medio del cliente de VPN institucional.

Reutilización o baja de dispositivos de almacenamiento

La Dirección de Tecnologías de Información y Comunicaciones, debe contar con un proceso de baja o devolución, que confirme el borrado seguro de la información en los activos y la Gerencia de Seguridad de la Información verificara aleatoriamente la ejecución de este proceso.

Equipo informático de usuario desatendido


La Dirección de Tecnologías de Información y Comunicaciones, debe implementar en todo equipo informático las configuraciones necesarias para su bloqueo de forma automática en un tiempo máximo de 5 minutos, una vez que éste se encuentre desatendido.

Política de escritorio seguro y bloqueo de pantalla

Todo el personal que preste sus servicios dentro de Banobras, debe cumplir con los siguientes lineamientos al ausentarse de su lugar de trabajo o finalizar su jornada laboral:

- En caso de contar con puerta, cajones o archiveros, éstos deben cerrarlos con llave.
- Retirar del escritorio cualquier tipo de información, sin importar el medio en que se encuentre (papel, post-its, discos, medios magnéticos) y resguardarla en gabinetes con llave o cualquier otro mueble con acceso controlado.
- Destruir de manera segura aquella información que ya no será utilizada.

MNOI50000113 Página 21 de 47	Aprobado/Autorizado					Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año			
Elaboró JCRR/GMR/IRL	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					Día	Mes	Año
Revisó SOO						17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN						Vigente a partir de:		
							Día	Mes	Año
							23	03	2018

- No dejar documentos con información sobre impresoras, copiadoras, etc.
- No utilizar la información impresa que sea confidencial o de uso restringido para reciclaje.

II.8. Políticas de seguridad en las operaciones

Objetivo: La presente Política tiene por objetivo salvaguardar la confidencialidad, integridad y disponibilidad de la información que se procesa mediante los distintos mecanismos de comunicación y operación de los sistemas de información.

II.8.1. Responsabilidades y procedimientos de operación

Documentación de procedimientos de operación

Los procedimientos de operación y los procesos de todas las áreas de la Institución, deben documentarse en manuales de operación de acuerdo a lo establecido en el documento de Objetivos y Lineamientos del Sistema de Control Interno de Banobras en el apartado III.1.4

La Dirección de Tecnologías de la Información es responsable de documentar sus procedimientos y de contar con memorias técnicas para la administración de los aplicativos y sistemas de información, mismos que deben estar actualizados y vigentes.

Administración de cambios

La Dirección de Tecnologías de Información y Comunicaciones debe establecer un proceso documentado para la administración de cambios en los ambientes operativos.

Todo el personal que participa en un cambio, en un componente de algún servicio TIC o sus elementos de configuración, deben apegarse estrictamente a los lineamientos establecidos en el documento del "Proceso de Administración de Cambios".

El Proceso de Administración de Cambios debe contar con un grupo de trabajo, facultado para promover, identificar y evaluar cuando se requiera un cambio en la infraestructura tecnológica de la Institución; este grupo debe sesionar al menos una vez al mes para informar los cambios realizados o en proceso.

En este grupo debe participar al menos un representante de la Gerencia de Seguridad de la Información.

Todo cambio o modificación de los datos en las bases de datos productivas, deben contar con el visto bueno del director responsable del aplicativo o responsable funcional con nivel jerárquico inferior inmediato.

Gestión de capacidades

La Dirección de Tecnologías de Información y Comunicaciones debe monitorear el uso de los recursos y proyectar los requerimientos de capacidad a futuro, con el fin de analizar las tendencias para el desempeño de los sistemas y aplicaciones.

MNOI50000113 Página 22 de 47	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						17	11	2017

Separación de los entornos de desarrollo, de pruebas y operativos

La Dirección de Tecnologías de Información y Comunicaciones debe mantener separados los ambientes de producción, prueba y desarrollo, para reducir riesgos de acceso no autorizado o cambios al sistema; considerando el establecimiento de reglas para el desarrollo o mantenimiento de software y su implementación en producción.

Los ambientes de desarrollo y de producción deben ubicarse en segmentos diferentes.

Los ambientes de prueba deben ser lo más parecido posible, en todos los aspectos, al ambiente de producción buscando así implementaciones efectivas.

La Dirección de Tecnologías de Información y Comunicaciones debe establecer mecanismos para la protección de datos e información sensible o reservada.

Los compiladores, editores y servicios relacionados con el desarrollo de sistemas no deben ser accesibles en el ambiente de producción.

II.8.2. Protección contra código malicioso

Controles contra el código malicioso

La Dirección de Tecnologías de Información y Comunicaciones debe asegurar que todos los equipos de escritorio, móviles (laptops) y servidores utilizados en la red de la Institución, tengan instalado el software antivirus, anti-malware, anti-xploits, anti-spam y anti-spyware institucional y mantenerlo actualizado, tanto en versión como en definición de firmas. Así mismo, deben cumplir con una configuración base de parches de seguridad.

Los proveedores o personal externo que tengan equipos y que necesiten conectarse a la red de la Institución, deben contar con un software de antivirus autorizado por la Dirección de Tecnologías de Información y Comunicaciones.

El software de antivirus anti-malware, anti-xploits, anti-spam y anti-spyware institucional debe permitir como mínimo:

1. Ejecutar búsqueda automática, manual o programable.
2. Limpiar archivos infectados.
3. Mantener en cuarentena los archivos que no puedan ser limpiados.
4. Contar con mecanismos para prevenir y contener amenazas, así como, negación de servicios.
5. Proveer la capacidad de actualizaciones automáticas y programables.
6. Registrar los incidentes de virus y contar con la capacidad de análisis de registro.
7. Detectar código malicioso.
8. Generar alertas.
9. Llevar una administración centralizada.

El software contra código malicioso y sus componentes deben ser actualizados cuando exista una nueva versión o definición de firmas, con base a los contratos con el fabricante.

La Dirección de Tecnologías de Información y Comunicaciones debe dar acceso al RSII y a la Gerencia de Seguridad de la Información al repositorio de los reportes mensuales detallando las incidencias detectadas por el antivirus.

MNOI50000113 Página 23 de 47	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Elaboró JCRR/GMR/IRL Revisó SOO	Dirección de Contraloría Interna / Responsable de Seguridad de la Información							
						17	11	2017	

II.8.3. Respaldo y borrado de información

Respaldo de información

Todos los mandos medios y superiores de las áreas dentro de la Institución, son responsables de identificar la información que sea sensible para la operación de su área de acuerdo a su criticidad y deben dar aviso a la Dirección de Tecnologías de Información y Comunicaciones para gestionar su respaldo y periodicidad.

La Dirección de Tecnologías de Información y Comunicaciones debe:

1. Implementar procedimientos para respaldar la información de la Institución.
2. Respaldo periódicamente toda la información (configuraciones, logs, file systems, bases de datos, etc.) que resida en los sistemas de la Institución, considerando su criticidad.
3. Asegurar que el respaldo de la información de los sistemas, en lo posible no degrade su operación.
4. Los respaldos deben llevarse a cabo preferentemente fuera de los horarios de operación y se documentan las excepciones.
5. Proveer espacios suficientes para almacenamiento y resguardo de la información del negocio que será respaldada periódicamente, siendo responsabilidad de cada usuario el manejo de la información a respaldar.
6. Revisar y validar periódicamente la información respaldada, para evitar que se pierda, se vuelva obsoleta o se deteriore; asegurando que la información sea recuperable y que cumple con los principios de integridad y disponibilidad.
7. Evitar que los medios de respaldo utilizados para el almacenamiento de información se vuelvan obsoletos. En la medida de lo posible, debe utilizar tecnologías de punta que permitan reducir el espacio físico que ocupan estos medios.
8. Almacenar los respaldos generados en un sitio protegido contra el medio ambiente y con controles estrictos de acceso, que debe ubicarse a una distancia razonable fuera del alcance de un evento en la zona principal.
9. Mantener un registro actualizado, con acceso controlado, que contenga los datos de todos los archivos respaldados, fuera de las instalaciones de la Institución, indicando la fecha más reciente en que la información fue modificada y la naturaleza de la misma.


Restauración e integridad

La Dirección de Tecnologías de Información y Comunicaciones debe implementar medidas y procedimientos para promover la integridad y disponibilidad de la información de la Institución que sea respaldada.

La Dirección de Tecnologías de Información y Comunicaciones debe:

1. Garantizar que los respaldos no sean alterados.
2. Garantizar la integridad, disponibilidad y confidencialidad de los respaldos por lo menos cinco años, desde su último respaldo.
3. Realizar pruebas programadas y documentadas de restauración de información, simulando situaciones de contingencia, bajo parámetros de tiempo establecidos, en donde

MNOI50000113 Página 24 de 47	Aprobado/Autorizado					Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año			
Elaboró JCRR/GMR/IRL	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					Día	Mes	Año
Revisó SOO						17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN			Vigente a partir de:		
				Día	Mes	Año
				23	03	2018

se revise la integridad y funcionalidad de los respaldos de información reportando los resultados al RSII, a través de la Gerencia de Seguridad de la Información.

Almacenamiento de información

La Dirección de Tecnologías de Información y Comunicaciones debe proporcionar y administrar espacio de almacenamiento suficiente para que las áreas puedan resguardar copia de su información institucional. Asimismo, debe contar con un inventario de usuarios autorizados en los recursos de almacenamiento de cada área.

Queda prohibido la utilización de recursos de almacenamiento institucional para archivos de uso personal o de diversión.

La Dirección de Tecnologías de Información y Comunicaciones debe contar con procedimientos y mecanismos de borrado o destrucción y de la información de la Institución, que ya no sea necesaria, ni por la operación, ni por requerimientos legales.

Toda la información que ya no sea utilizada se debe eliminar de forma segura, de acuerdo a los criterios que establezcan las áreas responsables de la información.

II.8.4. Registro de actividad

Registro de eventos

Todos los sistemas y aplicaciones críticos de la Institución, bases de datos y dispositivos de red y servidores, deben contar con registros de eventos y bitácoras de seguridad protegidos debidamente.

La Dirección de Tecnologías de Información y Comunicaciones debe resguardar por un periodo de al menos tres años todos los registros de incidentes, alarmas, cambios, configuraciones, entre otros, que deben estar disponibles para su extracción y revisión por parte de la Gerencia de Seguridad de la Información, cuando sean requeridos.

La Dirección de Tecnologías de Información y Comunicaciones, debe asegurar que los registros de acceso a sistemas, bitácoras, bases de datos y cualquier otro registro de seguridad de los aplicativos; se almacenen en un repositorio accesible para cualquier tipo de revisión o análisis.

Protección de la información de los registros

La Gerencia de Seguridad de la Información, debe validar que se implementen controles para la generación y conservación de bitácoras de seguridad, para los sistemas identificados como parte de una infraestructura esencial.

En estas bitácoras se debe registrar el usuario, nombre de equipo, dirección IP, hora de entrada y salida del sistema, así como, el tipo de consulta o cambios realizados en la configuración de las aplicaciones. Estas bitácoras deben tener un tiempo mínimo de almacenamiento de 90 días en línea.

Los controles que se implanten para proteger estos registros, deben incluir protección contra modificaciones, daños, mal uso o corrupción de los datos.

MNOI50000113 Página 25 de 47	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año				
Elaboró JCRR/GMR/IRL	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						Día	Mes	Año
Revisó SOO							17	11	2017

Registro del administrador y el operador

La Dirección de Tecnologías de Información y Comunicaciones debe contar con un registro de las actividades de los operadores y administradores de los sistemas. Éstos deben incluir como mínimo lo siguiente:

1. El tiempo en que ocurrió el evento.
2. Detalles del evento o fallas en el mismo.
3. Detalles de la cuenta de usuario y/o administrador implicado.

Sincronización de reloj

Todos los equipos de cómputo, sistemas, servidores, bases de datos y de comunicaciones que se encuentren en los dominios de red de la Institución, deben estar sincronizados con una fuente común y exacta de tiempo (servidor NTP).

La Dirección de Tecnologías de Información y Comunicaciones y las áreas de negocio con contratos de servicios con terceros, deben implementar y documentar procedimientos para que los cambios de horario no afecten la operación de la Institución.

Todos los equipos de cómputo y comunicaciones deben configurarse para que se sincronicen con el servidor NTP.

II.8.5 Control de software en sistemas operacionales

Instalación de software

La Dirección de Tecnologías de Información y Comunicaciones debe contar con procedimientos para la validación del software que sea instalado. Asimismo, debe asegurarse que todo el software que se instale en los servidores y equipos de cómputo personal cuente con el licenciamiento vigente, suficiente para atender los requerimientos del negocio.

La Dirección de Tecnologías de Información y Comunicaciones es responsable de administrar y resguardar las licencias del software institucional.

Todo el software que se instale en ambientes productivos debe ser previamente evaluado y probado en ambientes de pruebas. La instalación del software autorizado debe ser realizado por personal calificado, siguiendo los lineamientos de control de cambios y llevando un control estricto de las versiones.

Todo el software que se instale en los equipos de cómputo personal de Banobras debe estar inventariado en un catálogo de software institucional. Es responsabilidad de la Dirección de Tecnologías de Información y Comunicaciones gestionar la adquisición del software requerido por las áreas de negocio.


La Dirección de Tecnologías de Información y Comunicaciones es la única instancia autorizada para instalar, actualizar y desinstalar el software de los equipos de cómputo.

II.8.6 Gestión de la vulnerabilidad técnica

Gestión de las vulnerabilidades

La Institución a través de la Dirección de Tecnologías de Información y Comunicaciones y la Dirección de Contraloría Interna deben establecer el alcance de las evaluaciones que se realicen

MNOI50000113 Página 26 de 47	Aprobado/Autorizado					Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año			
Elaboró JCRR/GMR/IRL	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					Día	Mes	Año
Revisó SOO						17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN					Vigente a partir de:		
						Día	Mes	Año
						23	03	2018

para identificar vulnerabilidades en el hardware, software, sistemas, aplicaciones, seguridad, recuperación de información y redes.

La Dirección de Tecnologías de Informaciones y Comunicaciones debe coordinar la realización de los análisis de vulnerabilidades con una metodología que certifique las pruebas de caja gris y caja negra y disminuir el riesgo por falta de disponibilidad.

El RSII, a través de la Gerencia de Seguridad de la Información, debe documentar el seguimiento a las acciones de mejora, para solventar las vulnerabilidades detectadas, siguiendo el plan de remediación propuesto por la Dirección de Tecnologías de Información y Comunicaciones.

Las restricciones a la instalación de software

Queda prohibido al personal no autorizado instalar y/o ejecutar software para explorar (escanear) redes, equipos de cómputo y sistemas de información, en busca de protocolos, puertos, recursos compartidos y vulnerabilidades; así como, el descubrimiento y monitoreo no autorizado del tráfico de la red de la Institución. La Dirección de Tecnologías de Información y Comunicaciones debe implementar mecanismos para restringir la instalación de software no autorizado.

II.8.7. Consideraciones de las auditorías de los sistemas de información

Todos los sistemas deben contar con un registro de auditoría, que permita identificar la trazabilidad operativa.

Los aplicativos deben contar con un repositorio independiente, para almacenamiento de estos eventos, al cual tendrá acceso personal autorizado por el RSII.

Controles de auditoría de los sistemas de información

Las actividades de auditoría que involucren la revisiones de sistemas y aplicativos institucionales, deben ser calendarizadas y planeadas para prevenir interrupciones en la operación, con un perfil de consulta y un estado de inhabilitado hasta su requerimiento por parte de la Gerencia de Auditoría.


La Gerencia de Seguridad de la Información, será quien autorice la activación de los usuarios de auditoría en cada revisión, con previo conocimiento del alcance y su temporalidad.

En caso de auditores externos se debe observar, además de lo anterior, lo que aplique del dominio de Relación con Proveedores.

II.9. Seguridad de las comunicaciones

Objetivo: Asegurar la protección de la información en las redes y de las instalaciones de soporte dentro de la organización y con terceros.

MNOI50000113 Página 27 de 47 Elaboró JCRR/GMR/IRL Revisó SOO	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN						Vigente a partir de:		
							Día	Mes	Año
							23	03	2018

II.9.1. Gestión de seguridad de red

Controles de red

La Dirección de Tecnologías de Información y Comunicaciones es responsable del diseño, implementación, establecimiento, contratación, administración, mantenimiento y soporte de las redes de voz y datos y de toda la infraestructura de comunicaciones que las soportan.

La Dirección de Tecnologías de Información y Comunicaciones debe implementar procedimientos y controles tecnológicos para asegurar la integridad, disponibilidad y confidencialidad de la información, en su transmisión en las redes e infraestructuras de comunicaciones de la Institución.

La Dirección de Tecnologías de Información y Comunicaciones debe establecer los requerimientos técnicos para la conexión a la red y sus servicios.

Banobras debe contar con la infraestructura necesaria para la protección de la información y sus activos tecnológicos, así como, para el monitoreo y detección oportuna de incidentes de seguridad.

La Dirección de Tecnologías de Información y Comunicaciones debe implementar mecanismos para el uso del servicio de internet en la Institución, la cual debe contar con herramientas de seguridad y de filtrado de contenido, que permitan la segmentación de navegación conforme a la operación de las áreas.

El uso de servicio de internet se considerará con el mínimo acceso y sólo se podrá requerir un mayor acceso mediante una solicitud debidamente justificada, requisitada y autorizada por el director del área, quien será responsable de verificar el buen uso del servicio requerido.

La Dirección de Tecnologías de Información y Comunicaciones debe proteger la información que de estos servicios que se deriven, mediante la correcta configuración de los servidores y/o dispositivos sobre los que operan estos servicios.

Seguridad de los servicios de red

La Dirección de Tecnologías de Información debe implementar:


- Mecanismos que midan y aseguren niveles de disponibilidad y tiempos de respuesta, que garanticen la adecuada ejecución de las operaciones y servicios bancarios que se realizan.
- Medidas de control que aseguren la protección y confidencialidad de la información, generada por la realización de operaciones bancarias, a través de cualquier medio tecnológico.

La Gerencia de Seguridad de la Información, debe llevar a cabo revisiones periódicas de conexiones externas, tomando en consideración los siguientes puntos:

1. Vigencia
2. Dueño de la conexión externa por parte de la Institución
3. Descripción de la conexión externa
4. Uso de la conexión externa
5. Arquitectura de seguridad

Los tipos de conexiones externas que se pueden permitir son las siguientes:

MNOI50000113 Página 28 de 47	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año				
Elaboró JCRR/GMR/IRL	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						Día	Mes	Año
Revisó SOO							17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN					Vigente a partir de:		
						Día	Mes	Año
						23	03	2018

- Conexiones con instalaciones de la Institución que no están integradas a la red interna
- Conexiones con otras entidades financieras
- Conexiones con proveedores
- Conexiones públicas
- Conexiones a través de Redes Privadas Virtuales (VPN).

Se pueden establecer redes abiertas, únicamente al proporcionar servicios a la población, las cuales deben estar separadas y aisladas de la red de datos.

Segregación en las redes

La administración e infraestructura debe estar clasificada en zonas de seguridad, basadas en funciones, tipo de datos y requerimientos de acceso a los espacios de almacenamiento.

Se deben utilizar mecanismos de autenticación y cifrado para la protección de la comunicación inalámbrica.

Requerimientos de seguridad

La Dirección de Tecnologías de Información y Comunicaciones debe cuidar el cumplimiento de los requerimientos de seguridad mínimos para cada elemento de la red institucional, entre ellos:


- Zonas:
 - Zona de acceso - debe contar con, al menos, los siguientes controles de seguridad:
 - Acceso desde internet:
 - Firewall
 - Sistema de Prevención de Intrusiones (IPS)
 - Servidor de VPNs, en caso de acceder a servicios de red internos
 - Servidor de autenticación de dominio
 - Acceso hacia internet
 - Filtrado de contenido
 - Zonas de distribución - debe contar con al menos los siguientes controles:
 - Listas de Control de Acceso (ACL), en ruteadores y switches
 - Zona interna - debe contar al menos con los siguientes controles de seguridad:
 - Listas de Control de Acceso (ACL), en ruteadores y switches
 - Sistema de Prevención de Intrusiones (IPS)
 - Zona centro o núcleo - debe protegerse por los siguientes controles de seguridad:
 - Firewalls
 - Sistema de Prevención de Intrusiones (IPS)
 - Antivirus

- Requerimientos de protección para segmentos que transmitan información confidencial:

Todos los segmentos de red que transmitan información confidencial, deben hacerlo de forma encriptada. Ya sea con encriptación de punto a punto, o bien, mediante la encriptación de la información en sí.

- Requerimientos para el monitoreo de los elementos y dispositivos de red:

MNOI50000113 Página 29 de 47 Elaboró JCRR/GMR/IRL Revisó SOO	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN					Vigente a partir de:		
						Día	Mes	Año
						23	03	2018

Es necesario que la red y los dispositivos que la componen se monitoreen de forma regular, con la finalidad de identificar de manera oportuna problemas de desempeño que pudieran estar relacionados con incidentes de seguridad.

4. Configuración de dispositivos de red:

Para el cumplimiento de esta política de seguridad en red, la Dirección de Tecnologías y Comunicaciones debe definir configuraciones seguras para cada tipo de dispositivo que integra la red y debe aplicar a todos los dispositivos que la componen. Es necesario que dichos estándares tomen como referencia la información sobre vulnerabilidades y las especificaciones de los fabricantes para integrar la configuración segura.

5. Requerimientos de seguridad física para cableado y dispositivos de red:

El cableado de la red de datos debe cumplir con las especificaciones del fabricante, para minimizar errores físicos en la red. No debe estar expuesto a condiciones ambientales que aceleren su deterioro, tales como: agua, corrosivos, exceso de calor, etc.

II.9.2. Transferencia de información

Políticas y procedimientos de transferencia de información


Se debe crear un procedimiento o contratación de servicios, en caso de ser necesario, para la distribución y balanceo del tráfico, para los enlaces principales de la Institución, considerando disponibilidad, confidencialidad, criticidad y redundancia.

Los recursos de red de la Institución no deben ser utilizados para propósitos personales, específicamente:

1. No está permitido descargar o intercambiar documentos con información institucional, música, video e imágenes de internet en cualquier medio y desde cualquier medio y sólo se autorizará en caso de que la Institución o actividad específica lo justifique.
2. Dentro de la red de la Institución, no está permitido conectar a internet equipos personales o servidores de red por otro medio que no sea el oficialmente autorizado por la Institución.
3. El acceso a blogs, redes sociales y páginas de entretenimiento, juegos, deportes, pornografía, música, videos, contenido violento, religión, y otros contenidos, no relacionado con las actividades de trabajo no está permitido, salvo autorización previa de la Dirección solicitante.
4. La Dirección de Tecnologías de Información y Comunicaciones, es la única con autoridad para permitir monitorear el tráfico de la red. Este monitoreo se debe efectuar solamente con la finalidad de detectar anomalías, fallas o actividades sospechosas, los informes deben estar disponibles para la Gerencia de Seguridad de la Información.
5. Será sancionado cualquier uso comercial de los recursos y servicios de red e internet con fines diferentes a los institucionales.
6. Está prohibido descargar programas de internet “no autorizados” o sin licencia de uso institucional.

La transferencia de información a través de servicios en la nube, sólo será autorizada por personal de la Gerencia de Seguridad de la Información, de la Dirección de Tecnologías de Información y Comunicaciones y por la Dirección solicitante, quien ésta última será responsable de verificar que cuente con mecanismos mínimos de seguridad, como contraseñas y cifrado en los archivos que utilicen este servicio.

MNOI50000113 Página 30 de 47	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN			Vigente a partir de:		
				Día	Mes	Año
				23	03	2018

Es responsabilidad de la Dirección de Tecnologías de Información y Comunicaciones, que los servicios que se otorguen para la transferencia de información sean habilitados exclusivamente, es decir no deben habilitarse otros permisos de navegación.

Acuerdos sobre la transferencia de información

Todas las áreas de la Institución que tengan intercambio de información con cualquier entidad externa, pública o privada, deben establecer acuerdos específicos para la transferencia de información.

Los acuerdos de intercambio de información que se establezcan, deben considerar como mínimo los siguientes aspectos:

- Acuerdos sobre etiquetado de la información
- Definición del medio de transporte para transferencia de la información
- Canales autorizados para la transferencia de la información
- Definición de responsabilidades por divulgación o pérdida de información.

Mensajería electrónica

La Dirección de Tecnologías de Información y Comunicaciones debe cuidar la disponibilidad y confiabilidad del correo electrónico institucional.

El personal de la Institución está obligado a utilizar de forma adecuada los servicios de red y el servicio de correo electrónico institucional.

La Dirección de Tecnologías de Información y Comunicaciones debe implementar políticas para la administración del correo electrónico institucional, que garantice la trazabilidad y la no repudiación.

La Dirección de Tecnologías de Información y Comunicaciones tiene la facultad de suspender el servicio de correo electrónico institucional a la persona que haga mal uso.

No está permitido el uso del correo electrónico de la Institución para:

- Difundir cadenas de correos.
- Difundir mensajes de discriminación racial, religiosa, política o de cualquier otra naturaleza.
- Difundir mensajes que promocionen negocios personales o particulares.

Las únicas cuentas de correo autorizadas para el envío de mensajes de correo masivo, son aquellas que por la naturaleza de sus funciones en la Institución hayan sido creadas con este propósito específico.


Los usuarios deben borrar, sin abrir, todos los correos electrónicos que procedan de cuentas de correo que les sean desconocidas o cuyo “asunto” pueda relacionarse con publicidad o virus (SPAM).

Los mensajes de correo electrónico no deben borrarse porque pueden formar parte de una evidencia en los casos de auditorías.

No hacer uso de mensajería instantánea o redes sociales, para compartir información de operaciones.

Toda la información recibida, transmitida y almacenada en los servidores de correo electrónico de Banobras se considera información de la Institución.

MNOI50000113 Página 31 de 47 Elaboró JCRR/GMR/IRL Revisó SOO	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN			Vigente a partir de:		
				Día	Mes	Año
				23	03	2018

Todos los correos electrónicos que se emitan desde cuentas de correo de la Institución deben contar con la leyenda:

“La información contenida en el presente correo es confidencial y para uso exclusivo de la persona o Institución a que se refiere. Si usted no es el receptor deliberado es ilegal cualquier distribución, divulgación, reproducción, completa o parcial, aprovechamiento, uso o cualquier otra acción relativa a ella. Por favor notifique al emisor e inmediatamente bórrala de forma permanente de cualquier computadora en la que resida y en caso de existir, destruya cualquier copia impresa”.

Confidencialidad o acuerdos de no revelación

La Dirección de General Adjunta de Administración es responsable de establecer y mantener actualizado el contenido de todos los acuerdos de confidencialidad y de no revelación de información, que debe incluirse en los contratos, tanto para personal interno, proveedores, etc., según su área de competencia.

II.10. Adquisición, desarrollo y mantenimiento de los sistemas de información

Objetivo: Asegurar que la seguridad de la información es parte integral del ciclo de vida de los sistemas.

II.10.1. Requerimientos de seguridad de los sistemas de información


Análisis y especificación de los requerimientos de seguridad

La Dirección de Tecnologías de Información y Comunicaciones debe procurar que:

1. Los aplicativos de cómputo se construyan de forma modular, basados en una arquitectura orientada a servicios, como lo establece la normativa aplicable.
2. Los requisitos para el desarrollo de nuevos sistemas o para la realización de mejoras a los existentes se especifiquen y documenten formalmente.
3. Todas las aplicaciones cuenten con un módulo de seguridad, mediante el cual sólo se administre y gestione el ABC (altas, bajas y cambios) de usuarios, asegurando la trazabilidad de las sesiones de cada usuario. Este módulo debe contar con herramientas para la generación de reportes del control de acceso y gestión de usuarios.
4. Los módulos de administración operativa y de seguridad deben estar separados entre sí y estar excluidas de los módulos de operación del negocio.
5. El módulo de seguridad debe alimentarse desde la base de datos de recursos humanos y mantenerse actualizada.
6. El módulo de seguridad debe permitir la creación, asignación y el cambio de perfiles.

El RSII, a través de la Gerencia de Seguridad de la Información, será el responsable de validar la funcionalidad del módulo de seguridad de los sistemas.

MNOI50000113 Página 32 de 47	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN					Vigente a partir de:		
						Día	Mes	Año
						23	03	2018

II.10.2. Seguridad de las comunicaciones en redes públicas

Protección de las transacciones por redes publicas

Para compartir los servicios en redes públicas se deben establecer los mecanismos necesarios para la protección de la información, incluyendo como mínimo los siguientes aspectos:

1. Redes Privadas Virtuales (VPN).
2. Responsabilidades en torno a la seguridad de las bancas electrónicas contratadas por la Institución.
3. Lineamientos de control generales.
4. Autenticación de usuarios.
5. Autenticación de transacciones.
6. Trazabilidad de las operaciones.
7. Control de sesiones.


II.10.3. Seguridad en el desarrollo y los procesos de soporte

Política de desarrollo seguro

- La Dirección de Tecnologías de Información y Comunicaciones debe:
- Establecer un marco institucional para el desarrollo de software, en el cual se establezca una metodología para todo el ciclo de vida del desarrollo.
- Documentar todas las etapas del proceso de desarrollo de software.
- Adoptar las metodologías institucionales para el desarrollo de proyectos y cumplir con los lineamientos definidos por la PMO de Banobras.
- Asegurar su participación continua durante el proyecto en desarrollo.
- Proveer ambientes controlados para el desarrollo de software institucional
- Contar con repositorio controlado que contenga la documentación y el código fuente de los desarrollos institucionales o adquiridos, así como, un control de versiones.
- Asegurar que todo desarrollo institucional cuente con una arquitectura documentada que contenga al menos los siguientes aspectos técnicos:
 - Modularidad
 - Escalabilidad
 - Integración con sistemas legados
 - Seguridad
 - Disponibilidad
 - Confiabilidad
 - Soporte.

El RSII, a través de la Gerencia de Seguridad de la Información, debe revisar que se consideren los aspectos de seguridad en todas las fases del desarrollo. Asimismo, debe coordinar con los responsables de los procesos de desarrollo, para que se cuente con las medidas de seguridad para que el código de las soluciones tecnológicas, componentes, productos y demás elementos

MNOI50000113 Página 33 de 47	Aprobado/Autorizado					Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año			
Elaboró JCRR/GMR/IRL	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					Día	Mes	Año
Revisó SOO						17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN			Vigente a partir de:		
				Día	Mes	Año
				23	03	2018

relacionados, no se copie, envíe, transmita o difunda por cualquier medio distintos a su desarrollo.

Para los desarrollos subcontratados, es de vital importancia, definir de manera contractual la posesión del código fuente, para lo cual, deben existir mecanismos legales que permitan asegurar a la Institución mantener la titularidad del código fuente.

Procedimiento de control de cambios en los sistemas

Todo cambio o modificación en ambiente productivo del software institucional, debe apegarse al proceso de control de cambios de la Dirección de Tecnologías de Información y Comunicaciones.

Revisión técnica de aplicaciones después de cambios en la plataforma operacional

Previo al inicio de la puesta en operación en ambiente productivo, de un aplicativo se debe realizar el análisis de vulnerabilidades correspondiente, el cual preferentemente debe realizarlo un tercero, distinto a quién desarrolló el aplicativo; el resultado del análisis debe presentarse al Grupo de Administración de Cambios para su consideración y liberación correspondiente.

Cuando se modifiquen o actualicen los sistemas operativos y/o bases de datos, los sistemas afectados deben contar con un periodo de pruebas documentado, a fin que no existan efectos adversos en las operaciones o en la seguridad de la organización.

II.10.4. Datos prueba

Protección de los datos de pruebas

Todos los datos de prueba, preferiblemente deben contar con un mecanismo de enmascaramiento de la información reservada y/o confidencial.

Una vez utilizados los datos de prueba estos serán borrados antes de su pase a producción.


II.10.5. Responsabilidades del soporte, de aplicativos y sistemas de información

Todas las Direcciones que tengan bajo su responsabilidad aplicativos o sistemas institucionales deben nombrar un responsable funcional, por aplicativo o sistema, quien verifica periódicamente el funcionamiento.

El responsable funcional debe ser empleado de Banobras, tener un nivel mínimo de subgerente y conocer la operación funcional del sistema, mismo que tendrá las siguientes facultades:

- Solicitar modificaciones funcionales, encaminadas a la mejora de la operación del aplicativo.
- Realizar validaciones en ambiente de pruebas y aprobar su pase a producción.
- Gestionar la atención de incidencias y/o solicitudes relacionadas con la operación del aplicativo.
- Gestionar las solicitudes de información relativas a auditorías, con el conocimiento y anuencia del dueño de la información.

MNOI50000113 Página 34 de 47 Elaboró JCRR/GMR/IRL Revisó SOO	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN			Vigente a partir de:		
				Día	Mes	Año
				23	03	2018

- Mantener informada a la dirección sobre el funcionamiento del aplicativo o sistema.
- Contar con una definición de perfiles en los aplicativos preservando la segregación de funciones.
- Documentar la definición, alcance de los roles y/o perfiles de los aplicativos.
- Participar en el proceso de validación que realiza la Gerencia de Seguridad de la Información.

La administración, mantenimiento y soporte de los sistemas institucionales, son responsabilidad de la Dirección de Tecnologías de Información y Comunicaciones, quien designa al personal capacitado para cumplir tales funciones.

La Dirección de Tecnologías de Información y Comunicaciones debe contar con al menos un responsable de la administración de cada aplicativo o sistema de la Institución, el cual debe de:

- Realizar el mantenimiento correctivo y preventivo.
- Atender las solicitudes de mejora de la dirección propietaria de los sistemas.
- Atender los requerimientos de las áreas de seguridad.

La administración y mantenimiento a los aplicativos o sistemas institucionales deben apegarse a las directrices establecidas por la Subdirección de Soluciones Tecnológicas.

La Gerencia de Seguridad de la Información debe participar en el proceso de gestión, de las solicitudes de alta, inhabilitación o cambio de accesos, en los aplicativos o sistemas institucionales.

La Gerencia de Seguridad de la Información y el responsable funcional deben participar en la definición de perfiles en los aplicativos.

La Dirección de Tecnologías de Información y Comunicaciones a través de su mesa de servicio, es quien gestiona e informa del proceso de ABC (altas, baja y cambio) conforme a las solicitudes.

II.11. Relación con proveedores

Objetivo: Asegurar la protección de los activos de información de la institución, cuando los servicios TIC sean provistos por terceros.


II.11.1. Seguridad de la información en las relaciones con los proveedores

Política de seguridad de información para la relación con los proveedores

Banobras reconoce que aun cuando la protección de los activos de información sea provista mediante un servicio tercerizado, ésta continua siendo responsabilidad de la Institución, por lo cual, se deberán aplicar las siguientes políticas:

En toda contratación de servicios de TIC deben establecerse acuerdos de niveles de servicio (SLA) y acuerdos de niveles de operación (OLA).

MNOI50000113 Página 35 de 47	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Elaboró JCRR/GMR/IRL Revisó SOO	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN						Vigente a partir de:		
							Día	Mes	Año
							23	03	2018

Los terceros que presten algún servicio a la Institución y que tengan acceso a activos de información o a la infraestructura de redes y sistemas de la Institución, deben conocer y cumplir, en todo momento las políticas de seguridad.

Todos los contratos que formalice Banobras con un prestador de servicios, debe incluir una cláusula específica que asegure el cumplimiento a la política de seguridad de la información y los cambios que de ésta se deriven, durante el periodo de vigencia del contrato.

En caso de requerirse el trabajo de un tercero en las instalaciones de la Institución o bien su acceso remoto a las redes y sistemas de la Institución, debe existir un responsable por parte de la Institución que solicite los accesos requeridos por el tercero.

Los accesos de terceros a servicios de la Institución (red, aplicaciones, equipos, bases de datos e información) deben estar autorizados y acordes a los perfiles de funciones creados para tal efecto.

El acceso físico a los inmuebles de la Institución por parte de terceros debe registrarse en bitácoras (entrada y salida) y designar un responsable del área que visite, para que lo acompañe en todo momento durante la visita.

La seguridad dentro de los acuerdos con los proveedores

Todos los requisitos de seguridad de la información deben establecerse y acordarse con cada proveedor que pueda acceder, procesar, almacenar, transmitir, o proveer los componentes de la infraestructura de TI para la información de la Institución, asegurando el cumplimiento de los lineamientos que apliquen, de esta política.

La contratación de un tercero debe reunir todos los requisitos establecidos por el área de adquisiciones de la Institución.

Se debe considerar en los acuerdos de contratación de un tercero, además de los requisitos establecidos por el área competente de la Institución los siguientes puntos de seguridad de la información entre otros.

- Compromiso por parte de los terceros de no incurrir o participar en ningún tipo de actividad sospechosa o dañina para las instalaciones, información y/o operación de la Institución.
- Se debe establecer que al ocurrir algún incidente con los activos que estén utilizando (tecnológicos o información), se solucione el problema recobrando la operación normal de la Institución.
- Clausulas de restricción para el copiado y acceso a la información.
- Cubrir los requerimientos para control de accesos y procedimientos de autorización para acceder a los activos de información de la Institución (tecnológicos e información).
- Que se cuente con mecanismos para asegurar la protección de virus y código malicioso.
- La existencia de penalizaciones por incumplimiento a las políticas de seguridad.

Asimismo, se debe contar con acuerdos de confidencialidad firmados por los representantes legales de las empresas proveedoras de servicios, para asegurar que la información y los activos de información de la Institución a los que se tengan acceso durante la relación laboral y después, no se divulgue sin autorización, ni sea utilizada o modificada en perjuicio de la Institución. El área Jurídica, debe asegurarse de que en los contratos se incluya lo anterior.

MNOI50000113 Página 36 de 47	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Elaboró JCRR/GMR/IRL Revisó SOO	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					17	11	2017

II.11.2. Gestión de suministro de servicios del proveedor

Seguimiento y revisión de servicios del proveedor

Se tienen que mantener políticas y procedimientos que aseguren, en todo momento, el nivel de calidad del servicio y la seguridad e integridad de la información; lo anterior, con especial énfasis cuando la Institución contrate la prestación de servicios con proveedores externos para el procesamiento y almacenamiento de dicha información.

La Institución debe periódicamente supervisar, revisar o auditar la provisión de los servicios que ofrecen los terceros. Los proveedores tienen la obligación de entregar a la Institución, oportunamente, la evidencia digital necesaria en caso de incidentes de seguridad o aquella que les sea requerida.

Los proveedores de servicios de correo electrónico tienen la obligación de entregar a la Institución la totalidad de los correos electrónicos y bitácoras, así como, de no conservar información alguna mediante borrado seguro, al término del contrato.

Gestión de cambios a servicios del proveedor

Se deben gestionar los cambios en la provisión de los servicios, que están ofreciendo los proveedores, incluyendo el mantenimiento y la mejora de las políticas, los procedimientos y los controles de seguridad de la información existentes, teniendo en cuenta la criticidad de los procesos y sistemas de la Institución afectados, así como la reevaluación de los riesgos.

II.12. Gestión de incidentes en la seguridad de la información

Objetivo: Establecer lineamientos mínimos para gestionar los incidentes de seguridad de la información.

II.12.1. Gestión de incidentes de seguridad de la información y mejoras

Responsabilidades y procedimientos

El RSII debe establecer el ERISC, definir roles y responsabilidades de los integrantes, asimismo, dar a conocer las reglas de operación del mismo y la guía técnica de atención a incidentes a los participantes.


El ERISC debe estar conformado por personal de Banobras con conocimientos técnicos y operativos de las infraestructuras de la Institución.

El ERISC es responsable de elaborar y dar mantenimiento al procedimiento para la respuesta a incidentes de seguridad, el cual debe ser avalado por el GESI.

El ERISC debe conocer los procedimientos de respuesta a incidentes, que considera al menos etapas de:

1. Identificación y reporte.
2. Contención.

MNOI50000113 Página 37 de 47	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Elaboró JCRR/GMR/IRL	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					17	11	2017
Revisó SOO									

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN					Vigente a partir de:		
						Día	Mes	Año
						23	03	2018

3. Recuperación.
4. Solución.
5. Lecciones aprendidas.

El ERISC debe coordinar las acciones para solucionar los incidentes que afecten los servicios de información, para la operación de la Institución, en corresponsabilidad con las áreas afectadas e involucradas en la operación.

Los procedimientos para la notificación de incidentes deben estar fácilmente accesibles para todos los usuarios.

Informar eventos de seguridad de la información

La Dirección de Tecnologías de Información y Comunicaciones debe notificar de forma inmediata al RSII y a la Gerencia de Seguridad de la Información, de todos los incidentes o amenazas detectados que puedan causar la degradación en los niveles de servicios acordados, en las infraestructuras catalogadas como esenciales de Banobras.

Es responsabilidad de todo el personal de Banobras reportar a la mesa de servicios los incidentes de seguridad de la información que tengan una probabilidad de materializar un riesgo.

Algunos ejemplos de incidentes son, sin ser limitativos:

1. Accesos físicos no autorizados.
2. Accesos lógicos no autorizados.
3. Negación o degradación de servicios a sistemas de información.
4. Recepción de correo basura.
5. Robo de información.
6. Incumplimiento a las políticas de seguridad de la información.
7. Falla en la identificación o etiquetado de la información (de acuerdo a su clasificación).
8. Ataques de virus.
9. Incumplimiento con leyes sobre protección de datos personales.

Informar sobre puntos débiles de seguridad de la información

El monitoreo de la seguridad debe llevarse a cabo por la Dirección de Tecnologías de Información y Comunicaciones y en una base de 7x24 (7 días a la semana por 24 horas).

El ERISC puede solicitar la información necesaria, que permita identificar incidentes de seguridad relacionados con el ambiente de red y sistemas, así como, herramientas de monitoreo de seguridad en redes (IPS, firewalls, entre otros.)

El RSII y la Dirección de Tecnologías de la Información deben notificar a los Grupos Colegiados sobre las debilidades detectadas en la Institución

Respuesta a incidentes de seguridad

Los miembros del ERISC deben estar capacitados para el uso de las herramientas adquiridas por Banobras para el análisis y la respuesta a incidentes.

Se deben llevar a cabo sesiones de análisis de los incidentes conforme a la criticidad identificada, para la prevención y su solución.

Los procedimientos de respuesta a incidentes de seguridad se deben ser actualizados periódicamente.

MNOI50000113 Página 38 de 47	Aprobado/Autorizado					Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año			
Elaboró JCRR/GMR/IRL	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					Día	Mes	Año
Revisó SOO						17	11	2017

Aprendiendo de incidentes de seguridad de la información

El ERISC debe definir dentro de su procedimiento de Gestión de Incidentes de Seguridad de la Información un proceso de lecciones aprendidas.

Recolección de evidencia

Es responsabilidad del ERISC recolectar y documentar la evidencia relativa a los incidentes de seguridad que se identifiquen.

Es responsabilidad de la Gerencia de Seguridad de la Información verificar que se encuentre el resguardo de toda documentación y evidencia de los incidentes relativos a la seguridad de la información dentro de un repositorio para su análisis.

II.13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio

Objetivo: La Dirección General Adjunta de Administración de Riesgos, coordinara en conjunto con las Direcciones de la Institución la generación de un plan de acción para mantener la continuidad de los procesos, operaciones y servicios críticos de Banobras; lo anterior, para casos de contingencias provocados por acciones deliberadas, accidentales, fallas de los sistemas o desastres naturales.

II.13.1. Continuidad de la seguridad de la información

Planificación de la continuidad de la seguridad de la información

Se debe nombrar a un responsable para la coordinación del plan de continuidad del negocio, en caso de un desastre, de acuerdo a lo establecido en el “Manual de Políticas y Procedimientos de Continuidad del Negocio”.

El coordinador del plan de continuidad debe mantener una estrecha comunicación con las áreas directivas, operativas, tecnológicas, personal de seguridad física y Protección Civil.


La Dirección de Tecnologías de Información y Comunicaciones debe proporcionar soluciones y servicios tecnológicos que permitan la redundancia para los procesos contemplados en el plan de recuperación de la Institución.

Implantación del plan de la continuidad de la seguridad de la información

Todas las Direcciones Generales Adjuntas a través de sus Direcciones responsable de procesos sustantivos y de apoyo, deben contar con una estrategia de recuperación documentada y validada, siguiendo el “Manual de Políticas y Procedimientos de Continuidad del Negocio”.

La Gerencia de Seguridad de la Información debe validar que los planes de continuidad reciban mantenimiento, esto de acuerdo al marco de referencia establecido.

MNOI50000113 Página 39 de 47 Elaboró JCRR/GMR/IRL Revisó SOO	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN					Vigente a partir de:		
						Día	Mes	Año
						23	03	2018

Verificación, revisión y evaluación de la continuidad de la seguridad de la información

La Gerencia de Seguridad de la Información debe estar en conocimiento de los planes de recuperación, a fin de verificar el cumplimiento a la normativa de seguridad de la información institucional, e informar de los hallazgos para su actualización.

II.14. Cumplimiento

Objetivo: Coadyuvar al cumplimiento de los requerimientos legales, contractuales o regulatorios a los que está sujeto Banobras; así como, fomentar la revisión y seguimiento a eventos que provoquen una interrupción total o parcial de los servicios prestados, evitando violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad.

II.14.1. Cumplimiento con requerimientos legales y contractuales

Identificación de normativa aplicable y requisitos contractuales

Es responsabilidad del RSII a través de la Gerencia de Seguridad de la Información, que se definan las políticas que coadyuven al cumplimiento de los requerimientos regulatorios en materia de seguridad de la información.

El RSII, a través de la Gerencia de Seguridad de la Información debe coordinarse con los responsables de la administración de los servicios de TIC y con aquellos responsables de la operación de los mismos, a fin de que los acuerdos de nivel de servicio y los acuerdos de nivel operacional sean determinados y considerados en función de los programas de continuidad y de contingencia de la UTIC y del proceso.

Es responsabilidad del RSII, a través de la Gerencia de Seguridad de la Información, de enviar a la Unidad de Gobierno Digital un informe semestral, en los meses de julio del año al que corresponda y en enero del año siguiente, sobre el estado que guarda el cumplimiento del proceso de Administración de la Seguridad de la Información (ASI) y la información relativa a la operación de la totalidad de los controles de seguridad, distinguiendo los controles de seguridad mínimos establecidos en la normatividad, de aquellos derivados del análisis de riesgos.

Derechos de propiedad intelectual

El RSII, a través de la Gerencia de Seguridad de la Información, en coordinación con los responsables de las soluciones e infraestructuras tecnológicas de la Institución, deben validar uso de licencias y cumplimiento con los derechos de autor de toda aplicación y herramienta de software utilizada en las estaciones de trabajo. Todo el software instalado en las computadoras de la Institución debe ser legal.

Para cualquier desarrollo y en su caso mantenimiento de aplicativos de cómputo, se debe señalar que se constituirán a favor de Banobras los derechos patrimoniales inherentes a la propiedad intelectual, a través del registro correspondiente, en el que se incluyan la totalidad de los componentes del aplicativo de cómputo de que se trate, como son: el código fuente, el diseño físico y lógico, los manuales técnicos y de usuario.

MNOI50000113 Página 40 de 47	Aprobado/Autorizado					Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año			
Elaboró JCRR/GMR/IRL	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					Día	Mes	Año
Revisó SOO						17	11	2017

Protección de los registros

La Dirección de Tecnologías de Información y Comunicaciones debe asegurar que cada operación o actividad realizada por los usuarios de los aplicativos institucionales o sistemas, deje constancia electrónica, conforme a registros de auditoría.

La Dirección de Tecnologías de Información y Comunicaciones debe instrumentar condiciones de seguridad, que impidan borrar o alterar los registros de auditoría y las bitácoras de seguridad de los sistemas.

Privacidad y protección de la información de identificación personal

Uno de los objetivos de la seguridad de la información es la protección de datos del cliente en cualquier forma. Dichos datos son custodiados por una serie de controles físicos y lógicos para impedir algún daño a su confidencialidad, integridad y disponibilidad.

Adicionalmente, la Ley Federal de Protección de Datos Personales en Posesión de Particulares y su Reglamento es aplicable para la Institución, motivo por el cual Banobras debe implementar los controles necesarios para preservar la confidencialidad, integridad y disponibilidad de los siguientes datos personales:

1. Datos personales de los clientes.
2. Datos personales de los colaboradores de la Institución.

Esta información es catalogada como confidencial dentro del esquema de clasificación de la información adoptado por la Institución, y su trato es con base a los lineamientos de la entidad emisora de dicha Ley y su Reglamento en materia de protección de datos personales y en coordinación con los clientes de la Institución.

Asimismo, se debe considerar el secreto bancario de conformidad con la Ley de Instituciones de Crédito.

II.14.2. Revisiones de seguridad de la información

Revisión independiente de seguridad de la información


Se deben realizar revisiones por parte de una consultoría/despacho independiente para evaluar el grado de cumplimiento con los controles de la seguridad de la información.

Considerando como mínimo lo siguiente:

1. Que el personal que preste éste servicio, cumpla con los requisitos de experiencia requeridos en el anexo.
2. Que la metodología a seguir, cumpla con los marcos de gobierno y estándares que apliquen a la Institución.
3. Que los entregables técnicos y ejecutivos, cuenten con los elementos necesarios para la comprensión de cada prueba.

El RSII, a través de la Gerencia de Seguridad de la Información, da seguimiento a los análisis, actividades y resultados que se deriven de las revisiones realizadas.

MNOI50000113 Página 41 de 47	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Elaboró JCRR/GMR/IRL Revisó SOO	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN			Vigente a partir de:		
				Día	Mes	Año
				23	03	2018

Cumplimiento de las normas y políticas de seguridad

El personal que labora en la Institución, tiene la obligación de adoptar cualquier regulación en materia de seguridad de la información, que sea aplicable a la Institución, o bien, cualquier normatividad que sea aprobada.

Revisión del cumplimiento con normatividad relacionada con TIC

Las actividades de auditoría que involucren la revisiones de sistemas, aplicativos institucionales, deben ser calendarizadas y planeadas para prevenir interrupciones en la operación.

Los permisos de acceso a los sistemas o aplicativos institucionales del personal de la Dirección de Auditoría, deben ser solo de consulta y estar inactivos; se activarán por ejercicio o revisión, el RSII a través de la Gerencia de Seguridad de la Información, será quien autorice la activación de dichos usuarios.

Los requerimientos y el alcance de las revisiones, serán acordados con el RSII, a través de la Gerencia de Seguridad de la Información.


Sección III. Infracciones a la Política de Seguridad

Las acciones que se enumeran a continuación, en manera enunciativa más no limitativa, constituyen infracciones a la Política de Seguridad de Banobras.

1. Son acciones de falta u omisión a las Políticas Generales de Seguridad de la Información:

- No firmar los acuerdos de confidencialidad o de responsabilidad de activos de información.
- No actualizar la información de los activos de información a su cargo.
- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ellos.
- No guardar de forma segura la información cuando se ausente de su puesto de trabajo o al terminar la jornada laboral.
- Dejar información en carpetas compartidas, no autorizadas o en lugares distintos al servidor de archivos institucional, obviando las medidas de seguridad.
- Dejar las gavetas abiertas o con las llaves puestas en los escritorios.
- Permitir que personas ajenas a la Institución, deambulen sin acompañamiento en el interior de las instalaciones, en áreas no destinadas al público.
- Solicitar cambio de contraseña de otro usuario.
- No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento de Banobras, para traslado, reasignación o para disposición final.
- Utilizar claves de acceso de un usuario distinto al propio para ingresar a los sistemas y/o aplicativos.

MNOI50000113 Página 42 de 47	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Elaboró JCRR/GMR/IRL Revisó SOO	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN			Vigente a partir de:		
				Día	Mes	Año
				23	03	2018

2. Son acciones de mal uso de la plataforma tecnológica institucional:

- a) Hacer uso de la red de datos institucional, para acceder, almacenar, mantener o difundir en o desde los equipos institucionales, material con contenido sexual u ofensivo, cadenas de correos y correos masivos no autorizados.
- b) La utilización de software no relacionado con la actividad laboral que pueda degradar el desempeño de la plataforma tecnológica institucional.
- c) Actuar con negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de Banobras.
- d) Conectar equipos de cómputo personal u otros sistemas electrónicos personales a la red de datos institucional, sin la debida autorización.
- e) El utilizar los recursos tecnológicos institucionales para beneficio personal.
- f) Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por la Dirección de Tecnologías de la Información y Comunicaciones.

3. Son acciones de sabotaje de la plataforma tecnológica institucional:

- a) Impedir u obstaculizar el funcionamiento a los aplicativos, bases de datos o a las redes de telecomunicaciones y datos de Banobras, sin estar autorizado.
- b) Destruir, dañar, borrar, deteriorar activos informáticos de Banobras, sin autorización.
- c) Distribuir, enviar, introducir software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica de Banobras.
- d) Alterar datos personales de las bases de datos institucionales.
- e) Realizar cambios no autorizados en la plataforma tecnológica de Banobras.


4. Son acciones de acceso no autorizado a la infraestructura tecnológica de Banobras:

- a) Acceder sin autorización expresa a todo o en parte a los sistemas de Banobras.
- b) Suplantar a un usuario ante los sistemas de autenticación y autorización establecidos.
- c) No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de Banobras o permitir que otras personas accedan con el usuario y clave del titular a éstos.
- d) Otorgar el acceso o privilegios a la infraestructura de Banobras a personas no autorizadas.
- e) Ingresar a carpetas sin autorización.

5. Son acciones de robo de información a Banobras:

- a) Ejecutar acciones tendientes a eludir o variar los controles establecidos por Banobras.
- b) Retirar de las instalaciones de la Institución, estaciones de trabajo o equipos portátiles que contengan información institucional, sin la autorización pertinente.
- c) Sustraer de las instalaciones de Banobras documentos con información institucional, o abandonarlos en lugares públicos o de fácil acceso.

MNOI50000113 Página 43 de 47 Elaboró JCRR/GMR/IRL Revisó SOO	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						17	11	2017

	POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN					Vigente a partir de:		
						Día	Mes	Año
						23	03	2018

- d) Entregar, enseñar y divulgar información institucional, a personas o entidades no autorizadas.
- e) Copiar sin autorización los programas de Banobras o violar los derechos de autor o acuerdos de licenciamiento.

Todo personal que identifique la omisión o falta de cualquiera de estas acciones debe hacer del conocimiento a la Gerencia de Seguridad de la Información quien a su vez informará al RSII, a la Dirección de Recursos Humanos, al Órgano Interno de Control de la falta u omisión de las políticas establecidas en este manual, para que dentro de sus ámbitos de competencias resuelva lo conducente.

MNOI50000113 Página 44 de 47 Elaboró JCRR/GMR/IRL Revisó SOO	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						17	11	2017

Anexo 1

Términos y definiciones

Para los efectos del presente manual, se entenderá por:

Término	Definición
Activo de información	Toda aquella información y medio que la contiene, que por su importancia y el valor que representa para la Institución, debe ser protegido para mantener su confidencialidad, disponibilidad e integridad, acorde al valor que se le otorgue.
Acuerdo de nivel de servicio SLA	El acuerdo de nivel de servicio que se compromete con la unidad administrativa solicitante, al entregar un aplicativo de cómputo o servicio de TIC (Service Level Agreement, por sus siglas en inglés).
Acuerdo de nivel operacional OLA	El acuerdo de nivel operacional entre los responsables de los diversos componentes de la arquitectura tecnológica de un aplicativo de cómputo o servicio de TIC, que se debe definir y cumplir para responder a los acuerdos de nivel de servicio SLA comprometidos (Operational Level Agreement por sus siglas en inglés).
Amenaza	Cualquier evento, circunstancia humana, natural o tecnológica que tiene el potencial de causar algún tipo de daño a los activos de información de la Institución.
Análisis de riesgos	Es el proceso general de identificación, análisis y evaluación de riesgos para identificar las fuentes de vulnerabilidades o amenazas a los activos de TIC, a la infraestructura esencial o a los activos de información.
Áreas seguras	Son sitios en los que se maneja información sensible o valiosos equipos informáticos refugio y el personal para conseguir los objetivos de negocio.
Borrado seguro	El proceso mediante el cual se elimina de manera permanente y de forma irrecuperable la información contenida en medios de almacenamiento digital.
Centro de datos	El lugar físico en el que se ubiquen los activos de TIC y desde el que se proveen servicios de TIC.
CERTs	Equipo de respuesta ante emergencias informáticas.
Código fuente	El conjunto de líneas de textos, que son las directrices que debe seguir la computadora para realizar dicho programa; por lo que es en el código fuente, donde se encuentra escrito el funcionamiento de la computadora.
Confidencialidad	La característica o propiedad de la información, de poder ser conocida únicamente por individuos autorizados.
Datos personales	Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.
Disponibilidad	La característica de la información de permanecer accesible para su uso cuando así lo requieran individuos o procesos autorizados.

MNOI50000113 Página 45 de 47	Aprobado/Autorizado					Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año			
Elaboró JCRR/GMR/IRL	Dirección de Contraloría Interna / Responsable de Seguridad de la Información					Día	Mes	Año
Revisó SOO						17	11	2017

Término	Definición
Dispositivo Móvil	Es un activo de información de computación portátil que se utiliza para el procesamiento de información de la institución para ejecutar una función específica para el negocio.
Firewall	Es un software o sistema de seguridad de la red basada en hardware que controla el tráfico de red entrante y saliente en base a un conjunto de reglas aplicadas. Un Firewall establece una barrera entre una red interna segura y de confianza a otra red (ej. Internet) que se supone que no es seguro y confiable.
Impacto	Grado de los daños y/o de los cambios sobre un activo de información, por la materialización de una amenaza.
Incidente	Es la afectación o interrupción a los activos de TIC, a las infraestructuras críticas, así como a los activos de información de una Institución, incluido el acceso no autorizado o no programado a éstos.
Integridad	La acción de mantener la exactitud y corrección de la información.
Infraestructura tecnológica	Se refiere a todos los elementos físicos o lógicos que son requeridos para brindar los servicios y soluciones informáticas, tales como: centro de cómputo y comunicaciones, equipos y redes de comunicaciones de voz y datos, servidores de cómputo principales, servidores de cómputo departamentales, y de oficina (de escritorio y portátil), equipos auxiliares de cómputo y comunicaciones, sistemas operativos, manejadores de bases de datos, productos computacionales (Paquetes de Software) adquiridas o generadas por Banobras.
Mandos medios y superiores	Es la figura que se representa a través de un nombramiento por la Institución.
Medidas de seguridad	Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales.
Plataforma tecnológica	Son las acciones necesarias para realizar o brindar los servicios informáticos, tales como mantenimiento, optimización, actualización, monitoreo y vigilancia de los componentes tecnológicos involucrados en la operación de la plataforma tecnológica.
Proceso	Conjunto estructurado de actividades organizadas alrededor de un conjunto de objetivos definidos en términos medibles y que se expresan como beneficios para Banobras.
Programa	Es el conjunto de iniciativas, proyectos y acciones planeadas y programadas para lograr un objetivo.
Proveedor	Persona o empresa seleccionada por Banobras para la prestación de un servicio o entrega de un bien.
Privilegio especial	Es el usuario facultado para realizar actividades de mantenimiento o soporte operativo o funcional a un aplicativo o una base de datos.
Responsable Funcional	Es la persona encargada de supervisar, identificar y gestionar mejoras en los aplicativos o sistemas así como su correcto funcionamiento de uno o más aplicativos que le sean asignados por la Dirección en la que se encuentre adscrito.
Repositorio	El espacio en medio magnético u óptico en el que se almacena y mantiene la información digital.
Requerimiento	Condición o capacidad definida a una necesidad por un usuario, para solucionar un problema o lograr un objetivo, y existen diversos tipos como: funcionales, de rendimiento esperado, de interfaces con otros sistemas, de definición de restricciones, del cliente, etc.

MNOI50000113 Página 46 de 47	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
Elaboró JCRR/GMR/IRL	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
Revisó SOO	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						17	11	2017

Término	Definición
Riesgo	La posibilidad de que una amenaza pueda explotar una vulnerabilidad y causar una pérdida o daño sobre los activos de TIC, las infraestructuras críticas o los activos de información de la Institución.
Roles	Conjunto de responsabilidades, actividades y autorizaciones que se otorga a una persona o equipo. Una persona o equipo pueden tener varios roles.
Seguridad de la información	La capacidad de preservar la confidencialidad, integridad y disponibilidad de la información, así como la autenticidad, confiabilidad, trazabilidad y no repudio de la misma.
Sistema o Aplicativos Institucionales	Conjunto de elementos informáticos e infraestructura tecnológicas interrelacionados que interactúan entre sí para lograr un objetivo de negocio.
Tratamiento de datos personales	Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.
User-id	Conjunto de caracteres que sirve para identificar a un usuario, para su acceso a algún sistema.
Vulnerabilidades	Las debilidades en la seguridad de la información dentro de una organización que potencialmente permite que una amenaza afecte a los activos de TIC, a la infraestructura crítica, así como a los activos de información.

Acrónimos

Acrónimos	Descripción
Banobras	Banco Nacional de Obras y Servicios Públicos S.N.C.
ERISC	El equipo de respuesta a incidentes de seguridad de TIC en la Institución.
GESI	Grupo Estratégico de Seguridad de la Información.
MAAGTICSI	Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones, y en la de Seguridad de la Información.
ASI	Proceso de Administración de la Seguridad de la Información
OPEC	Proceso de Operación de los controles de seguridad de la información.
RSII	Responsable de la Seguridad de Información Institucional.
SGSI	Sistema de Gestión de Seguridad de la Información.
UTIC	La unidad administrativa en la Institución responsable de proveer de infraestructura y servicios de TIC a las demás áreas y unidades administrativas.
TIC	Tecnologías de la Información y Comunicaciones

MNOI50000113 Página 47 de 47 Elaboró JCRR/GMR/IRL Revisó SOO	Aprobado/Autorizado						Esta página sustituye a la aprobada/autorizada el:		
	Área(s)/Órgano(s) Colegiado(s)	Acuerdo(s)/FAC	Día	Mes	Año		Día	Mes	Año
	Dirección de Contraloría Interna / Responsable de Seguridad de la Información						17	11	2017