

**INSTITUTO DEL FONDO NACIONAL DE LA VIVIENDA PARA LOS
TRABAJADORES**



Manual General de Políticas de Control Interno

Clave de Identificación: POL-CG-001

Fecha de Publicación:	08/11/2017
Versión:	0

Contenido

1. Control de Cambios.....	5
2. Definición del Manual.....	5
3. Introducción.....	5
4. Modelo Integral del Sistema de Control Interno.....	6
4.1. Marco de Referencia.....	6
4.2. Sistema de Control Interno.....	6
4.3. Esquema del Sistema de Control Interno.....	7
4.4. Elementos de Control.....	7
4.5. Pilares de Control Interno.....	8
4.6. Establecimiento del Control Interno.....	8
4.7. Evaluación y fortalecimiento de Control Interno.....	9
4.7.1. Encuestas.....	9
4.7.2. Verificación de Medidas de Control.....	9
4.7.3. Evaluación de Procesos y Procedimientos.....	9
4.7.3.1. Auto-control.....	9
4.7.3.2. Verificación Integral de Control Interno.....	10
5. Políticas de Control Interno.....	10
6. Políticas de Normativa.....	11
6.1. De la normativa.....	11
6.1.1. Conformación de la normativa.....	12
6.1.2. De la difusión y capacitación de la normativa.....	13
6.1.3. De la actualización de la normativa.....	14
6.1.4. De la vigencia y conservación de la normativa.....	14
6.2. Cumplimiento Normativo.....	14
6.2.1. Del cumplimiento normativo.....	15
6.2.2. De la interpretación de la normativa.....	15
7. Políticas de Gestión de la Operación.....	15
7.1. Control de las Operaciones.....	16

7.1.1. Control Operativo.	17
7.1.2. Control Operativo de las Áreas.	18
7.1.2.1. Contraloría General.	19
7.1.2.2. Coordinación General de Riesgos.	19
7.1.2.3. Secretaría General y Jurídica.	19
7.1.2.4. Subdirección General de Crédito.	19
7.1.2.5. Subdirección General de Administración de Cartera.	20
7.1.2.6. Subdirección General de Administración y Recursos Humanos.	20
7.1.2.7. Subdirección General de Atención y Servicios.	21
7.1.2.8. Subdirección General de Comunicación.	21
7.1.2.9. Subdirección General de Planeación y Finanzas.	22
7.1.2.10. Subdirección General de Tecnologías de Información.	22
7.2. Monitoreo y Mejora Continua.	22
7.2.1. Monitoreo de la Operación.	23
7.2.2. Control de Personal Externo y Contratistas.	24
7.3. Gestión del Fraude.	24
7.3.1. Prevención de Fraude.	25
7.3.2. Detección de Fraude.	26
7.4. Declaración Patrimonial y de Posible Conflicto de Interés.	28
7.4.1. Esquema de la Declaración.	28
8. Políticas de Integridad de la Información.	29
8.1. Entrada de Información.	29
8.1.1. Preparación de Información.	31
8.1.2. Entrada de Datos.	31
8.1.3. Verificación de Integridad de Transacciones.	32
8.2. Procesamiento de la Información.	33
8.2.1. Integridad y Validez de Procesamiento.	34
8.2.2. Autenticación e Integridad de Transacciones.	35
8.3. Salida de Información.	35
8.3.1. Revisión y Conciliación de Salidas.	36

8.3.2. Monitoreo de la Integridad de la Información.....	37
9. Políticas de Conciliación Contable-Operativa.....	37
 9.1. Política Contable.....	37
 9.1.1. Fundamento contable.....	39
 9.1.2. Unidades de operación contable y responsables de cuentas	39
 9.1.3. Registro de transacciones y afectación de cuentas contables.	39
 9.1.4. Conciliación contable-operativa.....	40
 9.2. Política de Generación y Emisión de Reportes.....	41
 9.2.1. Preparación de Estados Financieros.....	42
 9.2.2. Agrupación y revelación de información financiera.....	42
 9.2.3. Reportes regulatorios.....	43
10. Políticas de Seguridad de la Información.	43
11. Glosario de Términos y Acrónimos	44
12. Disposición Transitoria.....	56

1. Control de Cambios

Versión**	Fecha	Descripción del Cambio
0	08/11/2017	Versión Inicial

** No eliminar las últimas 5 versiones previas.

2. Definición del Manual.

Objetivo:	Establecer el modelo operativo para el adecuado funcionamiento del Sistema de Control Interno y el logro de los objetivos estratégicos y operacionales, en el reporte de la información financiera y no financiera, así como en el cumplimiento normativo, mediante la gestión de riesgos y la efectividad de los controles.
Alcance:	El presente manual está dirigido a todo el personal del Instituto, personal externo, contratistas y usuarios de terceras partes cuyas funciones incluyan recibir, generar, almacenar, procesar o transferir información del Instituto y su personal.

3. Introducción.

El control interno es una herramienta surgida de la necesidad de operar proactivamente, a efecto de evitar y disminuir significativamente los riesgos a los que se encuentran expuestas las organizaciones y que pueden obstaculizar el cumplimiento de los objetivos estratégicos.

Para alcanzar los objetivos estratégicos, se establecen metas, procesos, procedimientos y actividades, mismos que son desarrollados por el personal de la Institución de que se trate, mismos tienen ligadas actividades de control que permiten su constante monitoreo, con el fin de valorar su funcionalidad para que, de ser necesario, se mejoren; estas actividades de control permiten evaluar el cumplimiento adecuado de los procesos o procedimientos.

En dichos procesos y procedimientos descansan las actividades y operaciones de una entidad, tales como las actividades de operación, financiamiento y administración, entre otras.

Es así que el establecimiento de un control interno adecuado permite optimizar la utilización de recursos para alcanzar una oportuna gestión financiera y administrativa, logrando mejores niveles operativos.

Es importante considerar que el control interno es un proceso ejecutado por todo el personal de una organización, diseñado para proporcionar una seguridad razonable, con miras a la consecución de objetivos estratégicos, la efectividad y eficiencia en las operaciones, la confiabilidad en la información financiera, así como el cumplimiento de las leyes y regulaciones aplicables.

El presente manual establece las medidas y controles preventivos, de detección y correctivos que se deben observar para el establecimiento, supervisión, evaluación, actualización y mejora continua del Sistema de Control Interno del Instituto.

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	6 de 57



4. Modelo Integral del Sistema de Control Interno.

4.1. Marco de Referencia.

El Sistema de Control Interno del Instituto se basa en el marco de control interno, COSO 2013, el cual es una buena práctica que permite desarrollar de manera eficiente y efectiva sistemas de control interno adaptables a los cambios del entorno operativo y de negocio, mitigando riesgos hasta niveles aceptables, además de servir como apoyo para la toma de decisiones.

El marco COSO es emitido por el Committee of Sponsoring Organizations of the Tradeway Comission (COSO), y responde a las exigencias del ambiente de negocios y operativo actuales, el cual:

- Promueve la gestión de riesgos en todos los niveles de la organización y establece directrices para la toma de decisiones de los directivos en el control de los riesgos y la asignación de responsabilidades.
- Ayuda a la integración de los sistemas de gestión de riesgos con otros sistemas que la organización tenga implantados.
- Ayuda a la optimización de recursos en términos de rentabilidad.
- Mejora la comunicación en la organización.
- Mejora el control interno de la organización.

4.2. Sistema de Control Interno.

El Sistema de Control Interno se define como el conjunto de procesos, mecanismos y elementos organizacionales relacionados entre sí, que buscan sinergia en la Institución para dar certidumbre en la toma de decisiones, enfrentar los riesgos y dar seguridad razonable de que se alcanzarán los objetivos y políticas institucionales de manera armónica.

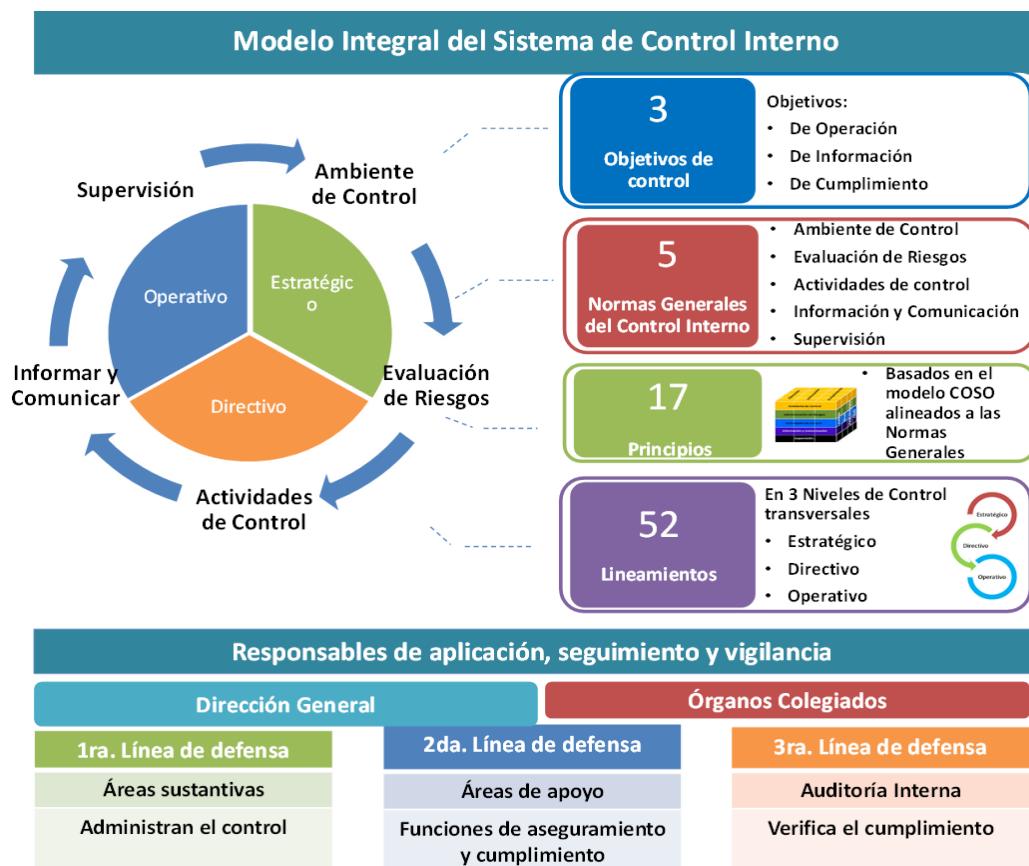
La implementación de un adecuado Sistema de Control Interno tiene como objetivo contar con:

- Seguridad razonable en las operaciones, proyectos y en el cumplimiento de los objetivos.
- Objetividad en la identificación, seguimiento, evaluación y gestión de riesgos institucionales.
- Información veraz, confiable y oportuna.
- Cumplimiento de la normativa y regulación que compete al Instituto.
- Transparencia y rendición de cuentas en la aplicación de los recursos.
- Regulación que permita controlar la dependencia de proveedores externos de conformidad con las políticas aplicables en materia.
- Fomento de valores éticos en el personal del Instituto y sus proveedores, entre otros.

Por lo que éste debe ser visto y concebido como un proceso integral dentro de la gestión y no como una actividad adicional a las que realiza el Instituto.

4.3. Esquema del Sistema de Control Interno.

Con base en los Lineamientos Generales de Control Interno, el Modelo Integral del Sistema de Control Interno, tiene la siguiente estructura:



Es importante considerar que, para la adecuada implementación de los lineamientos de control interno, deben definirse y poner en operación elementos de control que estén encaminados al cumplimiento de los objetivos del Sistema de Control Interno.

Por otro lado, para su implementación y efectividad es indispensable la participación de las tres líneas de defensa; mismas que en su conjunto y coordinadas, establecen un marco de actuación claro y estratégico.

4.4. Elementos de Control.

Se entenderá por elemento de control, a la evidencia que permita asegurar la implementación de los lineamientos de control. Se trata de aquellos instrumentos que permiten facilitar la operación del Sistema de Control Interno y proporcionan la infraestructura básica para operar las normas generales y principios.

Los elementos de control aseguran el cumplimiento y el fortalecimiento de todo el Sistema de Control Interno.

4.5. Pilares de Control Interno.

Existen 5 pilares que ponen en marcha el control interno; su principal objetivo es:

- I. Cumplimiento Normativo: Incentivar el cumplimiento de la normativa interna y externa aplicable en la realización de sus operaciones.
- II. Control de las Operaciones: Promover que la concertación, documentación, registro y liquidación diaria de operaciones, se realicen conforme a las políticas y procedimientos establecidos en los manuales del Instituto y en apego a las disposiciones legales aplicables.
- III. Integridad de la Información: Propiciar el correcto funcionamiento de los sistemas de procesamiento de información conforme a las políticas de seguridad, así como la elaboración de información completa, correcta, precisa, íntegra, confiable y oportuna, incluyendo aquella que deba proporcionarse a las autoridades competentes, y que coadyuve a la adecuada toma de decisiones.
- IV. Conciliación Contable Operativa: Verificar que los procesos de conciliación entre los sistemas de operación y contables sean adecuados y;
- V. Seguridad de la Información: Preservar la seguridad de la información generada, recibida, transmitida, procesada o almacenada en los sistemas informáticos y de telecomunicaciones, así como la aplicación de las medidas preventivas y correctivas necesarias para subsanar cualquier deficiencia detectada en materia de seguridad informática.

El enfoque de principios de control interno hace que éstos sean parte de los elementos de control básicos para el logro de los objetivos del Sistema de Control Interno.



4.6. Establecimiento del Control Interno.

Para la adecuada implementación del Sistema de Control Interno es importante el compromiso, no sólo de la Dirección General, quien define las estrategias y objetivos del Instituto, sino también de los demás niveles jerárquicos: (estratégicos, directivos y operativos), quienes deberán procurar el logro y cumplimiento de dichas estrategias y objetivos.

Lo anterior podría lograrse a través de la aplicación de los Lineamientos Generales de Control Interno en las áreas sustantivas, de apoyo y en delegaciones regionales dentro de su ámbito de competencia, a fin de que sus procesos y procedimientos cumplan los objetivos institucionales, así como los operacionales; de información y de cumplimiento mediante:

- Identificación, evaluación y gestión de riesgos.
- Ejecución de controles.
- Cumplimiento con la normativa interna y externa.
- Integridad de la información procesada y generada y;
- Fomento de los valores éticos en el personal.

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	9 de 57



4.7. Evaluación y fortalecimiento de Control Interno.

Un Sistema de Control Interno efectivo representa una herramienta fundamental que aporta elementos que contribuyen a minimizar riesgos, toda vez que, al contar con un enfoque de control fortalecido, se constituye un proceso sistémico para evaluar, mantener y mitigar los riesgos a los que pudiera estar expuesto el Instituto.

Por lo anterior, se debe analizar y valorar el grado de apropiación que el personal del Instituto tiene, respecto al propio Sistema de Control Interno, en cuanto al modo de actuar se refiere, así como en la operación diaria, con el objetivo de determinar la brecha de apropiación, ubicando las acciones correspondientes a implementar para el fortalecimiento del sistema.

En la evaluación del Sistema de Control Interno es necesario identificar el grado de madurez, el cual permitirá valorar el estatus de apropiación en el que se encuentran las áreas del Instituto, a partir de su propia operación, manejo, entendimiento y aplicación de un marco de control interno.

La evaluación se realiza por medio de encuestas, la verificación de medidas de control y la evaluación de procesos y procedimientos.

4.7.1. Encuestas.

Las encuestas están enfocadas a obtener información de cada nivel de control (Estratégico, Directivo y Operativo) sobre las condiciones específicas en las que se encuentra implementado cada lineamiento de control interno de acuerdo a su ámbito de competencia, lo que deberá estar soportado con la evidencia correspondiente.

Además de las encuestas, las áreas deberán de proporcionar los elementos de control según corresponda con su ámbito de competencia y responsabilidad en la implementación de los citados lineamientos.

Una vez analizada la información reportada en la totalidad de las encuestas aplicadas y la revisión de la evidencia y elementos de control proporcionados, se determina el grado de madurez de los Lineamientos Generales de Control Interno, así como del Sistema de Control Interno.

4.7.2. Verificación de Medidas de Control.

Su objetivo es identificar si se han definido e implementado adecuadas medidas de control para la operación de las políticas de control interno y determinar su correcta apropiación en los procesos y procedimientos del Instituto, así como determinar las áreas de oportunidad que pudieran apoyar en la mejora de la administración y control del Instituto.

4.7.3. Evaluación de Procesos y Procedimientos.

Adicionalmente, se cuentan con dos procesos de evaluación que inciden en el diseño, establecimiento y actualización de medidas y controles. Los resultados obtenidos impactan al Sistema de Control Interno.

4.7.3.1. Auto-control.

Su principal objetivo es que los dueños de procedimientos auto-evalúen si los mismos se encuentran operando con los lineamientos y controles necesarios y actualizados e identifiquen, eviten y, en su caso, corrijan con oportunidad los riesgos o condiciones que limiten, impidan o hagan inefficiente el logro de metas y objetivos institucionales.

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	10 de 57



4.7.3.2. Verificación Integral de Control Interno.

Tiene como objetivo corroborar que los procedimientos se encuentran actualizados, identificar posibles riesgos que pudieran tener un impacto en la generación de información, así como verificar que se cuenta con los controles diseñados e implementados para mitigar dichos riesgos. Así mismo, detectar las áreas de oportunidad que pudieran apoyar en la mejora de la administración y control de los procedimientos del Instituto.

Estas herramientas constituyen una metodología para analizar el Sistema de Control Interno, diagnosticando la madurez de los procesos y procedimientos del Instituto con el enfoque de los responsables de la operación, respecto al cumplimiento de los objetivos y requisitos en materia de control.

Expone, por lo tanto, buenas prácticas de control interno que buscan fortalecer la cultura del control en general y del cumplimiento de objetivos en particular, contribuyendo a promover en los responsables de la gestión, el interés en el control como ayuda para mejorar el desempeño y alcanzar los objetivos del Instituto, incluyendo los objetivos operacionales, de información y de cumplimiento.

5. Políticas de Control Interno.

Las Políticas de Control Interno son medidas de control que se encuentran encaminadas a diseñar los elementos de control que soportan las Normas Generales del Control Interno.

Tienen como propósito enmarcar lineamientos generales y específicos sobre los cuales debe desarrollarse la operación del Instituto para que éste pueda alcanzar los objetivos y metas planteadas; dichas políticas establecen las guías de acción para la implementación de las estrategias de ejecución del Instituto y definen los límites y parámetros necesarios para ejecutar los procesos y actividades en cumplimiento de la función, los planes, los programas, proyectos y políticas de administración de riesgo, previamente definidos por el Infonavit.

Las Políticas de Control Interno se encuentran enfocadas para que se diseñen y establezcan medidas y controles que apoyen el alcance de los objetivos de los 5 pilares de control interno:

- I. Normativa.
- II. Gestión de la Operación.
- III. Integridad de la Información.
- IV. Conciliación Contable-Operativa.
- V. Seguridad de la Información.

En este sentido, el personal del Instituto debe tener en cuenta éstas políticas, que resultan fundamentales para diseñar y mantener un sistema de control interno efectivo.

Es importante mencionar que estas políticas consideran lo establecido en la normativa interna, externa y las buenas prácticas de control interno, tales como:

- Normas de Información Financiera Mexicanas (NIF) definidas por el Consejo Mexicano de Normas de Información Financiera, A.C. (CINIF).
- Disposiciones de Carácter General Aplicables a los Organismos de Fomento y Entidades de Fomento emitidas por la CNBV, y publicadas el 1 de diciembre de 2014 y modificadas los días 27 de agosto de 2015, 25 de agosto de 2016 y 24 de julio de 2017.
- Marco de referencia de control interno emitido por el Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	11 de 57



6. Políticas de Normativa.

La cultura institucional comprende aspectos esenciales que son inherentes para el cumplimiento normativo. En ella se contempla la misión, visión, valores y ética que se concretan en roles, actividades y conductas dentro del Instituto realizadas a través de políticas; manuales; procedimientos; Códigos de Ética; organigramas y procesos, así como en la forma de comunicar y manejar la información mediante la cual se desarrolla la cultura y filosofía del Instituto. Es por lo anterior que el correcto diseño de la normativa interna y su apropiada implementación, fomentan la confiabilidad y la transparencia en las operaciones, así como la oportuna rendición de cuentas mejorando la toma de decisiones.

Así mismo, uno de los elementos fundamentales para el adecuado funcionamiento del Sistema de Control Interno del Instituto es la observancia del marco normativo que rige su actuación, el cual colabora en forma significativa con el cumplimiento de los fines y objetivos institucionales. Por lo anterior, es indispensable que todo el personal del Instituto, así como el personal externo, contratistas y usuarios de terceras partes, tomen conciencia que el cumplimiento del marco normativo resulta indispensable para garantizar de una manera segura y razonable, así como sinergia entre las áreas del mismo.

Con base en lo anterior, se establecen las políticas relativas al cumplimiento normativo las cuales proporcionan a todo el personal del Instituto, así como al personal externo, contratistas y usuarios de terceras partes, los elementos y herramientas indispensables a efecto de que conozcan el marco normativo que rige la actuación del mismo, su estricto cumplimiento y las consecuencias que pudieran propiciar ante su inobservancia; mismas que incluyen los siguientes aspectos:

1. Política de la normativa.
2. Política de cumplimiento normativo.

6.1. De la normativa.

Objetivo

Establecer los criterios y medidas de control preventivas, de detección y correctivas, relativas a la normativa Institucional para coadyuvar con la adecuada implementación, aceptación y cumplimiento de las normas, principios y procedimientos básicos de ética y actuación por parte del personal del Instituto.

Establecer las definiciones y criterios para elaborar, formalizar, mantener y difundir la normativa interna y difundir la normativa externa aplicable al Instituto.

Alcance

Aplica en todo el ámbito del Instituto, sus recursos e información que formen parte del marco jurídico institucional.

Responsabilidades

La Secretaría General y Jurídica, la Contraloría General, las Subdirecciones Generales, Coordinaciones Generales, Delegaciones Regionales y el Centro de Investigación para el Desarrollo Sostenible son responsables de:

- Elaborar, formalizar y mantener actualizada la normativa interna del Instituto.
- Difundir y vigilar el cumplimiento de la normativa interna y externa del Instituto.
- Determinar la vigencia de la normativa interna.
- Capacitar al personal interno, externo, contratistas y usuarios de terceras partes que opera la normativa, para que sea aplicada de manera correcta.

La Secretaría General y Jurídica, a través de la Coordinación General Jurídica es responsable de emitir una opinión jurídica sobre la normativa interna y su alineación con la normativa externa aplicable al Instituto.

La Subdirección General de Tecnologías de Información, es responsable de establecer y someter ante el H. Consejo de Administración:

- La metodología y los cambios que se deriven para normar el desarrollo y formalización de la normativa interna.
- Los mecanismos para la gestión y difusión al interior del Instituto de la normativa interna y externa.
- Los mecanismos para resguardar los documentos históricos de la normativa interna y externa.

La Subdirección General de Tecnologías de Información, a través del área que realiza las funciones de Gobierno de Procesos, es responsable de administrar, difundir al interior del Instituto y resguardar la normativa interna y externa con base en la metodología y mecanismos autorizados por el H. Consejo de Administración.

La Contraloría General, en coordinación con la Subdirección General de Administración y Recursos Humanos, son responsables de fomentar la capacitación continua a nivel institucional respecto del Sistema de Control Interno.

El personal del Instituto es responsable de implementar y dar cumplimiento a la Política de la Normativa dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y de mantener especial cuidado en sus prohibiciones.

6.1.1. Conformación de la normativa.

- a. Se debe establecer una metodología formal para regular el desarrollo y formalización de manuales de operación, políticas, procesos y procedimientos, es decir, la normativa interna o de operación.
- b. La metodología formal para regular la normativa interna y todo cambio que sea aplicado a dicha metodología debe someterse a la autorización del H. Consejo de Administración.
- c. Se debe elaborar, formalizar y mantener actualizada la normativa interna, buscando operar bajo estándares de excelencia, calidad en el servicio y mejora continua.
- d. La normativa interna debe estar constituida por las normas jurídicas, administrativas, lineamientos, guías operativas, y todas aquellas disposiciones cuya observancia sea de carácter obligatorio, a efecto de mantener un control interno adecuado que propicie el cumplimiento razonable de las metas y objetivos del Instituto, velando siempre por el interés de los derechohabientes.
- e. La normativa interna debe estar alineada a los objetivos del Instituto, así como los objetivos operacionales, de información y de cumplimiento. De igual forma, debe incluir los mecanismos para la protección del patrimonio institucional.
- f. La normativa interna debe elaborarse con base en el marco legal interno y externo, enfocándose en la misión, visión, valores institucionales y Código de Ética.
- g. Toda normativa interna debe estar alineada con la externa aplicable al Instituto, así como con las políticas y lineamientos de Control Interno, y contar con la opinión jurídica correspondiente que lo corrobore.
- h. Toda la normativa interna debe contener un apartado en el que se especifique el marco legal en el que se sustenta.

- i. Se deben definir las políticas y reglas operativas a las que se deben alinear los procesos, que permitan la concertación, documentación, ejecución y registro diario de operaciones de manera íntegra.
- j. Se deben documentar las operaciones propias del Instituto en manuales, procesos y procedimientos.
- k. Los procesos deben contener la secuencia lógica de un conjunto de recursos y actividades con el objeto de generar un producto final, así como las políticas de operación de los mismos.
- l. Los procedimientos deben contener la secuencia lógica, ordenada y específica de las actividades a realizar para cumplir con un objetivo determinado, así como los lineamientos operativos. Está prohibido desarrollar procedimientos sin relación a un proceso formalmente documentado.
- m. Los procesos y procedimientos deben incluir todas las actividades, tareas, roles, responsabilidades y mecanismos de control, tanto del personal que opera en las Oficinas de Apoyo, como el que opera en las Delegaciones Regionales, a efecto de que la normativa vigente refleje la operación real.
- n. Se deben identificar y documentar en la normativa interna las actividades realizadas por personal externo, contratistas y usuarios de terceras partes, cuando éstos operen utilizando la infraestructura del Instituto.
- o. Se deben identificar y documentar en la normativa interna las actividades de entrega y validación de los productos o servicios de contratistas que utilizan infraestructura propia para la generación de dichos productos o servicios.
- p. La normativa interna debe incluir las actividades automatizadas para el procesamiento de información (procesamiento en línea o por lote, carga y extracción de datos, entre otros).
- q. Toda normativa interna debe tener asignado un responsable o dueño de la misma con competencia profesional, con la finalidad de establecerla, formalizarla, y mantenerla, así como difundirla y vigilar su cumplimiento.

6.1.2. De la difusión y capacitación de la normativa.

- a. Se deben establecer los mecanismos para el acceso controlado, administración, difusión al interior del Instituto y resguardo de la normativa interna y externa, mismos que deben promover que su consulta sea accesible y de fácil localización para su debida observancia.
- b. Todo cambio en los mecanismos para la administración, difusión al interior del Instituto y resguardo de la normativa institucional debe someterse a la autorización del H. Consejo de Administración.
- c. La normativa interna debe difundirse de manera oportuna, a través de los mecanismos o medios institucionalmente autorizados.
- d. La normativa institucional debe estar disponible para el personal del Instituto que lo requiera dentro de su área de responsabilidad.
- e. La normativa interna debe estar debidamente autorizada por las áreas competentes, antes de su difusión.
- f. La normativa externa aplicable al Instituto, así como la normativa interna que sea autorizada por los Órganos Colegiados, debe difundirse por parte de las áreas

responsables. Su difusión y actualización debe realizarse a través de los mecanismos Institucionales, precisando la fecha de entrada en vigor autorizada por dichos órganos.

- g. Se debe contar con programas de difusión y capacitación al personal interno, externo, contratistas y usuarios de terceras partes, tanto para oficinas de apoyo, como para Delegaciones Regionales, los cuales tengan como objetivo difundir oportunamente la normativa interna y externa, así como capacitar respecto a los roles, responsabilidades y las actividades de operación.
- h. Se debe fomentar la capacitación continua a nivel institucional respecto del Sistema de Control Interno, a efecto de sensibilizar a todo el personal en el entendimiento de las normas de conducta, los objetivos y las actividades de control y supervisión correspondientes, en sus respectivos niveles de actuación y funciones, mismas que deben permear en la normativa interna.

6.1.3. De la actualización de la normativa.

- a. Los manuales de operación, políticas, reglas operativas, procesos y procedimientos deben revisarse y en su caso actualizarse por lo menos una vez al año, con base en la metodología definida.
- b. Los manuales de operación, políticas, reglas operativas, procesos y procedimientos deben mantenerse actualizados, de acuerdo con los cambios que se presenten en la operación, ya sea por el lanzamiento de nuevos productos o programas, así como por los cambios inherentes a la operación, tomando en consideración la opinión y experiencia de los operadores de los procesos en las Oficinas de Apoyo y las Delegaciones Regionales.
- c. Se deben mantener actualizados los roles y los puestos responsables de realizar cada actividad dentro de los procesos y procedimientos documentados.

6.1.4. De la vigencia y conservación de la normativa.

- a. Al expedirse y difundirse la normativa interna y externa, debe señalarse con toda precisión la fecha en la que entra en vigor y su vigencia, cuando aplique.
- b. Cuando la normativa interna o externa deje de estar vigente debe, invariablemente, causar baja de los medios de difusión, y resguardada en un repositorio histórico, mismo que debe conservar dicha normativa.

6.2. Cumplimiento Normativo.

Objetivo

Proporcionar un entendimiento claro de las obligaciones del personal del Instituto, el personal externo, contratistas y usuarios de terceras partes, en cuanto al respeto y compromiso con los objetivos institucionales, la normativa interna y externa, y las actividades asignadas por las funciones que les correspondan, así como, describir las facultades y funciones de las áreas responsables de la interpretación de la normativa.

Responsabilidades

La Secretaría General y Jurídica es responsable de revisar y emitir opinión respecto de todas las disposiciones jurídicas relativas al Instituto, así como revisar y emitir opinión sobre la normativa interna del Instituto.

La Dirección General, la Secretaría General y Jurídica, la Contraloría General, las Subdirecciones Generales, las Coordinaciones Generales, el Centro de Investigación para el

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	15 de 57



Desarrollo Sostenible, las Delegaciones Regionales, el personal externo, contratistas y usuarios de terceras partes, son responsables de alinearse a la normativa interna y externa del Instituto, según corresponda.

El personal del Instituto es responsable de implementar y dar cumplimiento a la Política de Cumplimiento Normativo dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma, y de mantener especial cuidado en sus prohibiciones.

El personal del Instituto es responsable de hacer del conocimiento al personal externo, contratistas y usuarios de terceras partes la Política de Cumplimiento Normativo y exhortarlos a su cumplimiento.

El personal externo, contratistas y usuarios de terceras partes son responsables de dar cumplimiento a la Política de Cumplimiento Normativo dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y mantener especial cuidado en sus prohibiciones.

6.2.1. Del cumplimiento normativo.

- a. Toda la normativa difundida en los mecanismos autorizados es de observancia obligatoria.
- b. Se debe vigilar periódicamente el cumplimiento de la normativa interna y externa del Instituto.
- c. Cualquier violación o incumplimiento a la normativa interna, externa y al Código de Ética debe ser reportada o denunciada, a la Contraloría General.
- d. De presumirse una violación a la normativa o al Código de Ética, se debe dar lugar a un procedimiento de responsabilidades administrativas y, en su caso, a la aplicación de sanciones.

6.2.2. De la interpretación de la normativa.

- a. En caso existir alguna duda respecto de la interpretación de la normativa interna y externa, se debe consultar al personal competente y facultado para que se emita una opinión al respecto.
- b. Lo que no esté expresamente permitido en la normativa interna, requerimientos normativos, las leyes y regulaciones aplicables al Instituto, está prohibido.

7. Políticas de Gestión de la Operación.

Las Políticas de Gestión de la Operación estructuran los criterios para definir los flujos de trabajo establecidos en los manuales de operación, políticas, reglas operativas, procesos y procedimientos, así como los parámetros para el diseño de las actividades y tareas requeridas para dar cumplimiento a los objetivos definidos para cada uno de los procesos y los criterios de actuación que han de tenerse en cuenta en la toma de decisiones cuando se presenten condiciones inesperadas en la operación del Instituto. Así mismo, establecen las acciones y mecanismos asociados a los procesos que permiten prever los riesgos que pueden inhibir el cumplimiento de las metas y sus resultados, y definen los parámetros de medición del desempeño de los procesos y del personal que tiene bajo su responsabilidad la ejecución de dichos procesos.

Las Políticas de Gestión de la Operación incluyen:

1. Política de Control de las Operaciones.
2. Política de Monitoreo y Mejora Continua.

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	16 de 57



3. Política de Gestión y Prevención de Fraudes.
4. Política de Declaración Patrimonial y de Posible Conflicto de Interés.

7.1. Control de las Operaciones.

Objetivo

Establecer las medidas de control preventivas, de detección y correctivas para gestionar la operación del Instituto, considerando los requerimientos legales y estatutarios, con el fin de proporcionar información íntegra, confiable, disponible, así como oportuna, para una adecuada toma de decisiones.

Alcance

Aplica en todos los ámbitos del Instituto; sus recursos, información, sus procesos internos o externos vinculados a través de contratos o acuerdos, así como al personal del Instituto en el ejercicio de sus funciones y al personal externo vinculados a través de contratos o acuerdos.

Responsabilidades

La Dirección General, la Secretaría General y Jurídica, la Contraloría General, las Subdirecciones Generales, las Coordinaciones Generales, el Centro de Investigación para el Desarrollo Sostenible, las Delegaciones Regionales, son responsables de:

- Establecer las metas operacionales alineadas a los objetivos institucionales.
- Establecer mecanismos de control que soporten la correcta operación de las normas generales de control interno.
- Apegarse a lo estipulado en la normativa interna vigente y sus excepciones.
- Identificar, administrar y dar seguimiento a los riesgos que puedan derivarse de la operación.
- Definir e implementar los mecanismos de control aplicables a la operación que mitiguen todos los riesgos identificados en la operación, así como ejecutar y monitorear la eficacia de los controles establecidos, incluyendo los ejecutados a través de la infraestructura tecnológica, la gestión de la seguridad y los procesos de adquisición de desarrollo y mantenimiento de aplicaciones.
- Establecer indicadores de desempeño para medir el cumplimiento del objetivo de los procesos y procedimientos.
- Establecer la estructura organizacional, las líneas de reporte, los niveles de autoridad y responsabilidad, la rendición de cuentas, así como el plan para la transmisión del conocimiento.
- Evaluar el desempeño y la competencia profesional del personal interno.
- Evaluar la viabilidad operativa y financiera de los productos o servicios a su cargo.
- Hacer del conocimiento del personal externo y contratistas los valores y la cultura del Instituto, así como el Código de Ética, la Guía de Responsabilidad Social, al igual que los documentos a los que deben apegarse.
- Establecer, difundir y vigilar el cumplimiento de la normativa interna y externa del Instituto.

La Subdirección General de Tecnologías de Información, a través del área que realiza las funciones de Gobierno de Procesos, es responsable de establecer un proceso de verificación de normativa interna.

La Dirección General, la Secretaría General y Jurídica, la Contraloría General, las Subdirecciones Generales, las Coordinaciones Generales, el Centro de Investigación para el Desarrollo Sostenible, las Delegaciones Regionales, son responsables de implementar y dar cumplimiento a la Política de Control de las Operaciones dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma, y de mantener especial cuidado en sus prohibiciones.

El personal del Instituto es responsable de hacer del conocimiento al personal externo, contratistas y usuarios de terceras partes la Política de Control de las Operaciones y exhortarlos a su cumplimiento.

El personal externo, contratistas y usuarios de terceras partes son responsables de dar cumplimiento a la Política de Control de las Operaciones dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y mantener especial cuidado en sus prohibiciones.

7.1.1. Control Operativo.

- a. Anualmente, se deben establecer las metas operacionales a través de un proceso donde se planee y supervise la ejecución con base en el plan definido. Dichas metas deben estar alineadas a los objetivos institucionales.
- b. Se debe establecer la estructura organizacional, las líneas de reporte, los niveles de autoridad y responsabilidad apropiadas para llevar a cabo la operación y promover la consecución de los objetivos institucionales.
- c. Se debe mantener una adecuada segregación de funciones, considerando el nivel jerárquico y área, evitando que las funciones de inicio, ejecución, registro, evaluación, contabilización, autorización y monitoreo estén concentradas en la misma persona.
- d. Se deben establecer canales adecuados de comunicación e información en la estructura organizacional para la correcta rendición de cuentas.
- e. Se debe establecer un plan para la transmisión del conocimiento operativo que permita continuar con la ejecución de la operación de forma oportuna y dar puntual cumplimiento a los objetivos institucionales, en caso de cambios del personal estratégico y táctico.
- f. Se debe corroborar que las funciones se desempeñen con integridad y apego a los valores éticos institucionales; toda desviación identificada debe ser reportada a la Contraloría General.
- g. Se debe realizar una evaluación del desempeño y la competencia profesional del personal interno, considerando el esquema establecido por el área que realiza las funciones de Recursos Humanos.
- h. Todo producto o servicio debe contar con una evaluación de viabilidad operativa y financiera. Los productos deben contar con una autorización formal antes de su implementación basada en los resultados de las pruebas de viabilidad.
- i. La operación del Instituto debe apegarse a lo estipulado en la normativa interna vigente, siempre y cuando no existan observaciones que impacten la razonabilidad de la integridad, confidencialidad y disponibilidad de las operaciones del Instituto, sus recursos, información, así como sus procesos internos o externos vinculados a través de contratos o acuerdos.
- j. En la normativa interna vigente que cuente con observaciones que impacten la razonabilidad de la integridad, confidencialidad y disponibilidad de las operaciones del Instituto, sus recursos, información, así como sus procesos internos o externos vinculados a través de contratos o acuerdos, debe redefinirse su operación y los mecanismos de control, posterior a la notificación de dichas observaciones.
- k. Se deben identificar, administrar y dar seguimiento a los riesgos que puedan derivarse de la operación, con el objetivo de minimizar las posibles pérdidas en las que se pudiera incurrir, tomando en cuenta los cambios que se producen en el entorno regulatorio y los impactos potenciales en los nuevos productos.

- I. Se deben definir e implementar los mecanismos de control aplicables a la operación que mitiguen los riesgos identificados, mismos que han de apoyar al cumplimiento del objetivo de la normativa interna, estar alineados con la tolerancia al riesgo a nivel institucional, al impacto en la segregación de funciones, así como al análisis de costo beneficio de su implementación.
- m. Se debe impulsar la definición e implementación de mecanismos de control que prevengan la mitigación de los riesgos identificados y llevarse a cabo de forma automática.
- n. Se deben definir e implementar mecanismos de control que detecten la materialización de los riesgos con mayores impactos y probabilidad de ocurrencia.
- o. En la medida de lo posible, se deben programar en las aplicaciones institucionales mecanismos que pongan en marcha las reglas operativas establecidas.
- p. Se deben establecer mecanismos de control que soporten la correcta operación de las normas generales de control interno.
- q. Se debe asignar un responsable con competencia profesional para ejecutar y monitorear la eficacia de los controles, el cual debe tener un nivel jerárquico superior al responsable de su ejecución.
- r. Se deben establecer indicadores de desempeño para medir el cumplimiento del objetivo de los procesos y procedimientos, considerando la frecuencia operativa de los mismos.
- s. Se debe corroborar la correcta implementación de los mecanismos de control definidos y que son ejecutados a través de la infraestructura tecnológica, la gestión de la seguridad y los procesos de adquisición de desarrollo y mantenimiento de aplicaciones.
- t. Se deben definir e implementar mecanismos de control que corroboren la integridad, disponibilidad y confidencialidad de la información de los productos y servicios ofrecidos.
 - a. Los problemas operativos se deben identificar y atender la causa raíz, sin excepción alguna, con el fin de reducir la reincidencia de los mismos.
 - u. La normativa interna verificada debe ser actualizada con base en las observaciones generadas, por medio de un proceso ágil, que apoye la redefinición oportuna de las debilidades de control identificadas.
 - v. No se deben delegar a personal externo o contratistas, responsabilidades que estén vinculadas directamente al cumplimiento de los objetivos institucionales, así como con los objetivos operacionales, de información y de cumplimiento.
 - w. Se deben identificar y gestionar los riesgos que se originan en las operaciones delegadas a contratistas y que puedan impactar directa o indirectamente en la consecución de los objetivos institucionales, en la identificación, administración y seguimiento de los riesgos.
 - x. Se debe hacer del conocimiento del personal externo y contratistas los valores y la cultura del Instituto, así como el Código de Ética, la Guía de Responsabilidad Social, al igual que los documentos a los que deben apegarse.
 - y. Las excepciones a la política de Control de las Operaciones deben estar justificadas por el responsable de la operación, con el visto bueno del Personal Directivo, así como autorizada por la Contraloría General.

7.1.2. Control Operativo de las Áreas.

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	19 de 57



7.1.2.1. Contraloría General.

- a. Se debe establecer un marco de control interno para facilitar la sostenibilidad y el logro de los objetivos del Instituto. Para tal fin, el control interno debe evaluarse, adaptarse y mejorarse permanentemente de acuerdo con las necesidades institucionales, los requerimientos normativos y las buenas prácticas asociadas.
- b. Se debe establecer un proceso para que las áreas corroboren el rendimiento operativo de la normativa interna; este proceso de auto-control debe incluir los criterios para su ejecución eficaz.
- c. Se debe establecer un esquema para verificar la razonabilidad de la operación del Instituto, con la finalidad de corroborar que la normativa interna se encuentre alineada al marco de control interno establecido.
- d. Se debe establecer un esquema para corroborar la adecuada gestión de las quejas de servicio incluyendo evaluación de la razonabilidad de las medidas tomadas para solventarlas y brindar un servicio de calidad.

7.1.2.2. Coordinación General de Riesgos.

- a. Se debe establecer un esquema de gestión de los riesgos que inciden sobre la actividad y entorno del Instituto, adoptando buenas prácticas y estándares de Gestión Integral de Riesgos, como una forma de facilitar el cumplimiento del propósito, la estrategia y los objetivos institucionales, los objetivos operacionales, de información y de cumplimiento, tanto de origen estatutario como legal, además de contribuir a la continuidad en la prestación de los servicios ofrecidos a los derechohabientes, patrones y público en general.
- b. La gestión de riesgos debe realizarse en forma preventiva y continua, misma que debe estar integrada y ser inherente a la planeación estratégica y al plan que defina los procesos y proyectos operativos del Instituto.
- c. Anualmente, se deben actualizar los riesgos identificados que impacten la planeación estratégica y el plan que defina los procesos y proyectos operativos del Instituto.
- d. Se debe difundir a los grupos de interés el estado de la evaluación de riesgos, de modo que la gestión de riesgos sea un proceso estructurado, integral, participativo y continuo.

7.1.2.3. Secretaría General y Jurídica.

- a. Se debe corroborar que los actos y hechos que se generen y tengan efectos jurídicos cuenten con el soporte legal adecuado, así como con la debida asesoría legal al momento de tomar las decisiones del Instituto.

7.1.2.4. Subdirección General de Crédito.

- a. Se deben diseñar productos financieros eficientes para que cada derechohabiente acceda a una solución de vivienda de calidad.
- b. Se debe corroborar la integridad de la información de los derechohabientes con la que se generan los productos financieros, antes de la aprobación de los mismos.
- c. Se deben diseñar productos y servicios ágiles con el objeto de ser entregados con oportunidad y calidad, centrados en las necesidades y expectativas del derechohabiente.

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión 0	0	Hoja 20 de 57	

7.1.2.5. Subdirección General de Administración de Cartera.

- a. Se deben planear, diseñar e implementar estrategias y productos para la adecuada administración del portafolio crediticio, así como para la cobranza y recuperación del mismo.
- b. Se deben diseñar soluciones de cobranza eficientes con base en la situación real de la cartera.
- c. Se deben implementar soluciones de cobranza con base en las posibilidades y situación particular de cada acreditado y que permitan la recuperación de la cartera.
- d. Se deben diseñar productos y servicios ágiles con el objeto de ser entregados con oportunidad y calidad, centrados en las necesidades y expectativas del derechohabiente.
- e. Los productos y servicios implementados deben ser ágiles, con el objeto de ser entregados con oportunidad y calidad y centrados en las necesidades y expectativas del derechohabiente.
- f. Se debe ofrecer información oportuna y de calidad para que cada derechohabiente tome las mejores decisiones a lo largo de su ciclo de vida.
- g. Se deben definir e implementar mecanismos de control e indicadores de desempeño para corroborar que los productos y servicios sean entregados con oportunidad y calidad.
- h. Se debe reportar periódicamente a las diferentes áreas del Instituto el resultado del rendimiento de los productos y servicios implementados. Con base en dicho resultado, se deben realizar acciones de mejora en la oportunidad y calidad de los productos y servicios.

7.1.2.6. Subdirección General de Administración y Recursos Humanos.

- a. Se debe establecer un marco y la normativa interna para la gestión de los recursos humanos alineados con la Política de Seguridad de la Información en los Recursos Humanos.
- b. Se deben definir e implementar acciones para el fortalecimiento del talento humano en los procesos de planificación, selección, vinculación, inducción, capacitación, compensación, bienestar social, seguridad social y salud ocupacional, evaluación del desempeño y desvinculación.
- c. Los mecanismos de reclutamiento, selección de personal, contratación y desarrollo personal deben aplicar la igualdad de oportunidades, evitando cualquier tipo de discriminación o preferencia de raza, edad, género, ideología o institución educativa.
- d. Se deben establecer directrices que le permitan contar con la logística necesaria para proveer al personal un adecuado ambiente de trabajo y los servicios necesarios para el normal desarrollo de sus actividades, asegurando la provisión oportuna de equipos y suministros de oficina y preservando el buen estado de conservación y de seguridad de las instalaciones del Instituto.

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	21 de 57



- e. Se debe difundir y promover el cumplimiento del Código de Ética, para lo cual se deben establecer indicadores para identificar problemas potenciales y tendencias respecto de su cumplimiento.
- f. Se debe implementar un esquema de evaluación del desempeño y competencia profesional del personal interno, considerando parámetros cuantitativos y cualitativos, así como tomando en cuenta las responsabilidades asignadas al personal y el logro de los objetivos institucionales, incluyendo los objetivos operacionales, de información y de cumplimiento.
- g. Se debe revisar que el esquema de evaluación del desempeño y sus resultados sean íntegros para corroborar que no se realicen conductas inapropiadas.
- h. Se debe corroborar que la adquisición de bienes y servicios sea realizada de acuerdo con los principios legales, las necesidades y requerimientos técnicos de las áreas solicitantes y, considerando las mejores condiciones de cantidad, calidad, oportunidad y seguridad.
- i. El proceso de adquisición de bienes y servicios debe contar con criterios de transparencia y eficiencia, promoviendo la optimización de recursos del Instituto.
- j. El proceso de adquisición de bienes y servicios debe mantener la confidencialidad de la información, por lo que está prohibido proporcionar información a terceros, que pueda afectar la transparencia del proceso.
- k. Se debe corroborar que la vigencia de los contratos y pedidos, resultado del proceso de adquisición de bienes y servicios que celebre el Instituto, no sea anterior a la fecha de formalización de los mismos.

7.1.2.7. Subdirección General de Atención y Servicios.

- a. Se deben establecer procesos para una eficaz y eficiente gestión de servicio y que estimulen la cultura de servicio dirigida a los derechohabientes, patrones y público en general.
- b. Se deben implementar los productos y servicios definidos por las diferentes áreas del Instituto, corroborando que la información se procese y mantenga íntegra, confidencial y disponible.
- c. Se deben definir e implementar los mecanismos para la recepción y gestión de quejas de servicio y solicitudes relacionadas con el Instituto, de manera que la información se mantenga íntegra, confidencial y disponible.
- d. Se debe controlar de manera veraz y oportuna el manejo de las quejas de servicio tomando las correspondientes medidas viables para solventar la queja y brindar un servicio de calidad.

7.1.2.8. Subdirección General de Comunicación.

- a. La comunicación en el Instituto debe tener como marco de actuación el respeto, la transparencia, la oportunidad, la pertinencia, la veracidad y el diálogo; de igual forma, debe estar orientada a garantizar su reputación y a mantener una adecuada relación con los grupos de interés, a fin de contribuir a la sostenibilidad y al desarrollo de la estrategia del Instituto.
- b. Se debe corroborar que todos los colaboradores del Instituto reciban información veraz, clara y oportuna a través de la utilización de canales efectivos de

comunicación interna, para facilitar el adecuado desempeño de sus procesos y fortalecimiento de la cultura organizacional.

7.1.2.9. Subdirección General de Planeación y Finanzas.

- a. Se debe establecer un esquema de gestión financiera, atendiendo criterios de ética, transparencia y responsabilidad frente al riesgo financiero, dentro del marco legal y estatutario y en línea con sus objetivos institucionales. Lo anterior, para soportar las decisiones de inversión, obtención de recursos, reparto de excedentes financieros y manejo de liquidez, con el fin de maximizar el valor del Instituto y garantizar su sostenibilidad en el contexto del sano equilibrio entre lo social y lo económico.
- b. Debe existir un plan financiero que defina la dirección y la estrategia a seguir, así como la forma y estructura general bajo la cual se dé cumplimiento a los objetivos institucionales.
- c. Debe existir un plan que defina los procesos y proyectos que se instrumentan durante un periodo y que son la base para medir los resultados con respecto al plan financiero.
- d. Se debe corroborar la disponibilidad de los recursos necesarios, para el funcionamiento adecuado del Instituto y la provisión de éstos que permitan la proyección y crecimiento establecido en el plan financiero.
- e. Se deben elaborar y presentar los estados financieros del Instituto que cumplan con los requerimientos establecidos por la ley. Los estados financieros se deben elaborar con el objetivo de informar la situación financiera, sus cambios y los resultados en el periodo correspondiente.
- f. Se debe establecer un esquema para definir, gestionar y supervisar las metas operacionales que tengan como fin la consecución de los objetivos institucionales.
- g. Se deben establecer procesos eficientes para la recaudación y administración del Fondo de Ahorro y la Subcuenta de Vivienda, otorgando rendimientos.
- h. Se deben diseñar productos y servicios ágiles con el objeto de ser entregados con oportunidad y calidad, centrados en las necesidades y expectativas del derechohabiente.

7.1.2.10. Subdirección General de Tecnologías de Información.

- a. Se debe habilitar al Instituto para que disponga de la información requerida por los usuarios de la misma y se adapte oportunamente a los cambios generados por el entorno, los procesos y objetivos del Instituto, usando como referencia la arquitectura tecnológica definida y operando bajo un modelo operativo basado en buenas prácticas.
- b. Se debe proteger la información y sus ciber-activos con el fin de contar con información íntegra, disponible y confidencial, requerida para la toma de decisiones, así como la operación segura y la respuesta oportuna a incidentes o ataques sobre sus ciber-activos, de forma que se garantice la continuidad de los servicios.

7.2. Monitoreo y Mejora Continua.

Objetivo

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	23 de 57



Establecer las medidas de control preventivas, de detección y correctivas para evaluar y monitorear la efectividad operativa, con el fin de generar las acciones de mejora preventiva y correctiva para un mejor rendimiento operativo.

Alcance

Aplica en todos los ámbitos del Instituto; sus recursos, información, procesos internos o externos vinculados a través de contratos o acuerdos, así como al personal del Instituto en el ejercicio de sus funciones y al personal externo vinculados a través de contratos o acuerdos.

Responsabilidades

La Dirección General, la Secretaría General y Jurídica, la Contraloría General, las Subdirecciones Generales, las Coordinaciones Generales, el Centro de Investigación para el Desarrollo Sostenible y las Delegaciones Regionales, son responsables de implementar y dar cumplimiento a la Política de Monitoreo y Mejora Continua dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma, y de mantener especial cuidado en sus prohibiciones.

La Subdirección General de Tecnologías de Información, a través del área que realiza las funciones de Gobierno de Procesos, es responsable establecer el Sistema de Gestión de la Calidad.

El personal del Instituto es responsable de hacer del conocimiento al personal externo, contratistas y usuarios de terceras partes la Política de Monitoreo y Mejora Continua y exhortarlos a su cumplimiento.

El personal externo, contratistas y usuarios de terceras partes son responsables de dar cumplimiento a la Política de Monitoreo y Mejora Continua dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y mantener especial cuidado en sus prohibiciones.

7.2.1. Monitoreo de la Operación.

- a. Se debe corroborar periódicamente la eficacia y eficiencia de los mecanismos de control implementados, así como medir periódicamente el cumplimiento de los objetivos de la normativa interna, con base en los indicadores de desempeño diseñados y el cumplimiento de los objetivos institucionales, incluyendo los objetivos operacionales, de información y de cumplimiento.
- b. Se deben definir e implementar mecanismos que corroboren que las reglas operativas se encuentran operando eficaz y eficientemente.
- c. Se deben realizar revisiones programadas para corroborar que ninguna persona pueda realizar actividades en áreas de responsabilidad única sin ser monitoreada. Ante la posibilidad o evidencia de ocurrencia de actos inadecuados, se deben organizar las operaciones del Instituto, a fin de establecer una adecuada segregación de funciones.
- d. Se debe monitorear que los riesgos no sean materializados, poniendo especial atención en los riesgos asumidos.
- e. Se deben considerar los señalamientos emitidos por los Órganos Colegiados y entidades externas, referentes a la mejora continua de la operación del Instituto.
- f. Se deben analizar periódicamente las quejas, denuncias y peticiones presentadas por los derechohabientes, patrones y personal del Instituto, para la mejora continua de la operación del Instituto.

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	24 de 57



- g. Para las quejas recurrentes de los derechohabientes, patrones y personal del Instituto se debe identificar y atender la causa raíz, sin excepción alguna, con el fin de reducir la reincidencia de las mismas.
- h. Se debe corroborar que las medidas correctivas derivadas de observaciones generadas por la Auditoría Interna, la Contraloría General, el Auditor Externo o cualquier otro revisor, sean implementadas de manera oportuna y coherente.
- i. Se debe corroborar que el proceso de auto-control sea realizado en tiempo y forma, conforme a los criterios establecidos.
- j. En el proceso de auto-control realizado, se deben definir e implementar los compromisos de mejora continua de la operación del Instituto, con base en los criterios establecidos.
- k. Se debe diseñar e implementar un Sistema de Gestión de la Calidad enfocado en la satisfacción de las necesidades y expectativas de los derechohabientes, acreditados, patrones y público en general, el cumplimiento de la normativa institucional vigente y el compromiso con la mejora continua, a fin de lograr los objetivos institucionales, así como los objetivos operacionales, de información y de cumplimiento, con criterios de eficacia y eficiencia en la prestación de los servicios.

7.2.2. Control de Personal Externo y Contratistas.

- a. La gestión de personal externo, contratistas y usuarios de terceras partes, debe apegarse a la Política de Relación con Contratistas.
- b. El cumplimiento del objetivo y entregables estipulados en los contratos del personal externo y contratistas debe ser revisado en periodos regulares de acuerdo con la duración de su contrato.
- c. Se debe determinar el impacto con relación al Instituto de la evaluación del control interno de los contratistas que generan un producto o servicio que se interrelaciona con los procesos y procedimientos Institucionales, utilizando infraestructura propia, ya que por la naturaleza del producto o servicio que desempeñan tienen acceso a información operativa, reservada o confidencial del Instituto.
- d. Se debe evaluar el desempeño de las actividades realizadas por el personal externo y contratistas, documentando la supervisión de los trabajos que realizan, así como su competencia profesional; el resultado debe ser considerado para la toma de decisiones sobre la relación que guarda el Instituto con los contratistas.
- e. Se deben registrar cronológicamente los actos u omisiones en que incurra el personal externo y contratistas cuando éstos representen incumplimiento de obligaciones, a fin de hacer efectivas las garantías establecidas en los contratos formalizados.
- f. La falta de evidencia de la evaluación del desempeño de las actividades realizadas por el personal externo y contratistas, la no identificación del incumplimiento de obligaciones o las garantías efectivas no aplicadas, debe dar lugar a un proceso de responsabilidades administrativas, y en su caso, a la aplicación de sanciones.

7.3. Gestión del Fraude.

Objetivo

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	25 de 57



Establecer las medidas de control para prevenir y detectar el fraude, investigarlo y combatirlo cuando se produce, minimizando los daños e impactos a la reputación y maximizando las opciones de recuperación del perjuicio ocasionado al Instituto.

Alcance

Aplica al personal del Instituto, así como al personal interno o externo, vinculados a través de contratos o acuerdos, en el ejercicio de sus funciones.

Responsabilidades

La Secretaría General y Jurídica, la Contraloría General, las Subdirecciones Generales, las Coordinaciones Generales, Delegaciones Regionales, y del Centro de Investigación para el Desarrollo Sostenible son responsables de:

- Establecer las tareas y mecanismos de control que prevengan y detecten el fraude, la corrupción, y el soborno.
- Definir e implementar mecanismos de control que ayuden a mitigar los riesgos de fraude susceptibles.
- Implementar los mecanismos de control contra acciones que induzcan, promuevan, inciten o desemboquen en fraude, corrupción o soborno.

La Contraloría General con el apoyo de la Coordinación General de Riesgos son responsables de:

- Establecer la normativa interna del proceso anti-fraude.
- Identificar, analizar, evaluar y priorizar los riesgos de fraude en los procesos y procedimientos del Instituto.
- Identificar, analizar y evaluar en las áreas del Instituto, las acciones que induzcan, promuevan, inciten o desemboquen en fraude, corrupción o soborno.
- Definir los mecanismos de control contra acciones que induzcan, promuevan, inciten o desemboquen en fraude, corrupción o soborno.
- Planificar, llevar a cabo e informar sobre la evaluación de la efectividad de mecanismos de control anti-fraude.
- Establecer e impartir un programa de concienciación anti-fraude.
- Establecer un mecanismo para la notificación anti-fraude.
- Establecer un proceso de respuesta a reportes anti-fraude.

El personal del Instituto, contratistas y usuarios de terceras partes son responsables de notificar a la Contraloría General, cualquier actividad sospechosa que pudiera inducir, promover, incitar, desembocar en fraude, corrupción o soborno, así como cuando se produzcan, además de notificar cualquier situación que pueda significar el desperdicio de recursos sin propósito, dispendios o despilfarros, así como el abuso de autoridad.

El personal del Instituto es responsable de implementar y dar cumplimiento a la la Política de Gestión de Fraude dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma, y de mantener especial cuidado en sus prohibiciones.

7.3.1. Prevención de Fraude.

- a. La normativa interna debe establecer tareas y mecanismos de control que impulsen el desarrollo de acciones coordinadas contra el fraude, la corrupción, y el soborno, que promuevan la transparencia en la gestión de la administración, disuada las conductas indebidas e incentive el compromiso del personal del Instituto al cumplimiento y respeto de todos sus mecanismos de transparencia y anti-fraude.

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	26 de 57



- b. Se debe establecer la normativa interna del proceso anti-fraude, que incluya las prácticas para prevenir y detectar el fraude, la corrupción y el soborno, e investigarlos y combatirlos cuando se producen.
- c. Se deben identificar los riesgos de fraude en los procesos y procedimientos del Instituto; dichos riesgos de fraude deben ser analizados, evaluados y priorizados para su mitigación.
- d. Se debe llevar a cabo el análisis, evaluación y priorización sobre riesgo de fraude, por lo menos una vez al año.
- e. Se deben definir e implementar mecanismos de control que ayuden a mitigar los riesgos de fraude.
- f. Se deben identificar, analizar y evaluar en las áreas del Instituto, las acciones que induzcan, promuevan, inciten o desemboquen en fraude, corrupción o soborno del personal del Instituto, personal externo, contratistas y usuarios de terceras partes.
- g. Se deben definir e implementar los mecanismos de control contra acciones que induzcan, promuevan, inciten o desemboquen en fraude, corrupción o soborno del personal del Instituto, personal externo, contratistas y usuarios de terceras partes.
- h. Se debe planificar y llevar a cabo una evaluación de la efectividad de los mecanismos de control anti-fraude.
- i. Se debe informar a los involucrados sobre los resultados de auditorías internas y externas, con el fin de reforzar o evaluar los mecanismos de control anti-fraude.
- j. Se debe establecer e impartir un programa de concientización anti-fraude que incluya la difusión oportuna de los mecanismos contra acciones que induzcan, promuevan, inciten o desemboquen en fraude, corrupción o soborno, así como un control antifraude y fomento de la denuncia, con base en los puestos de trabajo y áreas de riesgo del personal del Instituto.

7.3.2. Detección de Fraude.

- a. Se debe establecer un mecanismo para la notificación de actividades sospechosas que pudieran inducir, promover, incitar, desembocar en fraude, corrupción o soborno, así como cuando se produzcan; estos mecanismos deben de tener como mínimo las siguientes características:
 - Confidencialidad.
 - Anonimato.
 - Disponibilidad para todo el Instituto.
 - Asistencia en tiempo real.
 - Seguimiento contra represalias.
- b. Se debe notificar cualquier actividad sospechosa que pudieran inducir, promover, incitar o desembocar en fraude, corrupción o soborno, así como cuando se produzcan; entre las actividades sospechosas que deben ser reportadas, se encuentran las siguientes:
 - Apropiación o uso indebido de recursos financieros y otros bienes del Instituto. Cambio ilícito de destino o uso indebido de los recursos financieros y otros bienes del Instituto y/o administrados por éste, para favorecer intereses propios o de terceros.
 - i. Apropiación o uso indebido de bienes, equipos o inventarios, malversación de fondos, pagos a proveedores ficticios, pagos dobles, manipulación de excedentes de tesorería, apropiación de dinero, inadecuada utilización de

fondos de caja menor, entre otros, cuya propiedad sea del Instituto o administrados por éste.

- ii. Conceptos ficticios de compensación.
- iii. Sobrepasso de los límites autorizados de gasto.

- Manejo inadecuado de activos de información. Crear, acceder, eliminar, modificar, alterar, divulgar o usar activos de información de manera inapropiada o dolosa con fines indebidos o para beneficio personal.

- Corrupción. Abuso de posiciones de poder o de confianza, para beneficio particular; entre los que se incluyen, mas no limitan la existencia de otros adicionales:

- i. Ofrecer o solicitar, entregar o recibir, bienes en dinero o en especie, en servicios o beneficios, a cambio de acciones, decisiones u omisiones.

- ii. Aceptar dádivas, para el personal o sus familiares, cuyo tipo y monto hayan sido expresamente prohibidas en el Código de Ética u otro documento institucional.

- Falsedad en informes. Creación, eliminación, modificación, alteración o divulgación de cualquier tipo de información tendiente a distorsionar la realidad del desempeño propio, del Instituto en general, o de terceros. Incluye la supresión de información material que afecte la toma de decisiones; entre los que se incluyen, mas no limitan la existencia de otros adicionales:

- i. Suministro de información falsa para encubrir desempeño deficiente o para acceder a bonificaciones.

- ii. Utilizar falsos reportes para engañar a inversionistas, entidades financieras, reguladores o terceros en general.

- iii. Manipulación de estados financieros: reconocimiento inapropiado de ingresos, sobreestimación o subestimación de activos, subestimación de pasivos, estimados significativos y no acordes con la realidad del Instituto, entre otros.

- iv. Ocultamiento y violación deliberada a normas cambiarias, impositivas, contables, de seguridad, salud ocupacional, ambientales, del mercado financiero, en general de la normativa interna y normativa externa aplicable al Instituto.

- v. Ocultamiento de errores contables.

- c. Se debe notificar cualquier situación que pueda significar el desperdicio de recursos sin propósito, dispendios o despilfarros, así como el abuso de autoridad.

- d. Se debe establecer un proceso de respuesta a reportes anti-fraude, con el fin de investigar y tratar el fraude, soborno o corrupción, así como el desperdicio de recursos; dicho proceso debe contener como mínimo las siguientes características:

- Investigar cualquier violación a esta política, fraude, corrupción o soborno que se denuncie, se detecte o se sospeche razonablemente.

- Requerir la cooperación del personal pertinente en la investigación.

- Comunicar a los involucrados sobre los resultados de la investigación y otras funciones de cumplimiento, según proceda.

- Aplicar medidas disciplinarias de acuerdo a la criticidad de los hechos.

- Tratar de manera confidencial la investigación y que los resultados de la investigación sean confidenciales.

- e. Cuando sea requerido, se debe buscar la colaboración del personal técnico para obtener información precisa de cómo se produjeron los hechos y determinar la información que

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	28 de 57



pudo quedar comprometida, con el fin de mejorar la gestión y los mecanismos de control de la plataforma tecnológica y los aplicativos del Instituto.

7.4. Declaración Patrimonial y de Posible Conflicto de Interés.

Objetivo

Establecer los mecanismos de control para gestionar el proceso por el cual se presenta la Declaración Patrimonial y de Posible Conflicto de Interés, con el fin de mantener la información íntegra, confidencial y disponible.

Alcance

Aplica al personal del Instituto en el ejercicio de sus funciones.

Responsabilidades

La Dirección General, la Secretaría General y Jurídica, la Contraloría General, las Subdirecciones Generales, las Coordinaciones Generales, Delegaciones Regionales, y el Centro de Investigación para el Desarrollo Sostenible, son responsables de corroborar que el personal obligado presente la Declaración Patrimonial y de Posible Conflicto de Interés, en adelante la Declaración.

La Contraloría General es responsable de:

- Establecer la normativa interna para la presentación de la Declaración.
- Definir los requerimientos operativos para establecer el aplicativo para la presentación de la Declaración.
- Definir y mantener las reglas operativas para la generación y presentación de la Declaración.
- Clasificar la información relacionada con la Declaración de acuerdo con la Política de Gestión de Activos.
- Analizar la información resultado de la presentación de la Declaración, determinar e investigar la consistencia de los datos presentados y determinar las sanciones que, en su caso, correspondan.
- Dar seguimiento a los posibles conflictos de interés.

La Subdirección General de Tecnologías de la Información, a través de las áreas que realizan las funciones de Desarrollo, Adquisición y Mantenimiento de Aplicativos, es responsable de implementar y mantener el aplicativo para la presentación de la Declaración Patrimonial y la Declaración de Posible Conflicto de Interés.

El personal del Instituto es responsable de implementar y dar cumplimiento a la Política de Declaración Patrimonial y de Posible Conflicto de Interés dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma, y de mantener especial cuidado en sus prohibiciones.

7.4.1. Esquema de la Declaración.

- a. Se debe establecer la normativa interna para la presentación de la Declaración Patrimonial y de Posible Conflicto de Interés, incluyendo las políticas específicas para la presentación de la misma y las excepciones operativas.
- b. Se debe establecer y administrar un aplicativo para la presentación de la Declaración Patrimonial y de Posible Conflicto de Interés.
- c. Se debe definir el nivel organizacional del personal obligado a presentar la Declaración Patrimonial y de Posible Conflicto de Interés.

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	29 de 57



- d. El personal obligado, debe incluir dentro de la Declaración Patrimonial y de Posible Conflicto de Interés, la situación que guarda su cónyuge o concubina, concubinario y la de sus dependientes económicos.
- e. Se debe definir un calendario y tiempos límite para la presentación de la Declaración Patrimonial y de Posible Conflicto de Interés.
- f. Se debe corroborar que la información relacionada con la Declaración Patrimonial y de Posible Conflicto de Interés se encuentre identificada, clasificada y gestionada de acuerdo con la Política de Gestión de Activos.
- g. Se debe presentar y corroborar que el personal obligado presente la Declaración Patrimonial y de Posible Conflicto de Interés por medio del aplicativo establecido para este fin, conforme a la normativa interna vigente, el calendario y tiempos límite establecidos.
- h. Se debe realizar un análisis de la información registrada en la Declaración Patrimonial y de Posible Conflicto de Interés y determinar la consistencia de los datos presentados. Las inconsistencias identificadas deben ser analizadas para su corrección o determinar las sanciones que en su caso correspondan, así como proponer las medidas necesarias para evitar la comisión de infracciones.
- i. Se debe dar seguimiento a los posibles conflictos de interés, en caso de que el personal obligado haya realizado transacciones comerciales dentro del Instituto, en donde exista un interés económico, personal, familiar o del grupo, directo o indirecto.
- j. En el caso de incumplimientos a la Política de la Declaración Patrimonial y Posible Conflicto de Interés o infracciones a la misma, se deben llevar a cabo las acciones conducentes a fin de determinar las sanciones que en su caso correspondan, así como proponer las medidas necesarias para evitar la comisión de infracciones.
- k. Los incumplimientos a la Política de Declaración Patrimonial y Posible Conflicto de Interés deben estar documentados formalmente.

8. Políticas de Integridad de la Información.

Uno de los activos más importantes con los que cuenta el Instituto es la información sobre la gestión de la operación y del personal y que a través de procesos y aplicaciones que generan, almacenan, procesan o transfieren dicha información, es utilizada para la toma de decisiones. Por lo anterior es necesario contar con controles eficaces y eficientes para mitigar los riesgos de errores operativos por información no íntegra, y con ello proveer información confiable a la Dirección General del Instituto.

En tal virtud, es relevante establecer las Políticas de Integridad de la Información, a fin de proporcionar las directrices para corroborar que la información que es generada, recibida, transmitida, procesada o almacenada como parte de los procesos operativos se encuentre completa, correcta, precisa, confiable y sea oportuna.

Dichas políticas incluyen diversos aspectos de cómo se debe manejar la información en el Instituto, incluyendo:

1. Entrada de información.
2. Procesamiento de la información.
3. Salida de información.

8.1. Entrada de Información.

Objetivo

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	30 de 57



Establecer las medidas de control preventivas, de detección y correctivas para que la información esté dispuesta y sea ingresada por personal autorizado y calificado siguiendo los formatos y procedimientos establecidos, teniendo en cuenta una adecuada segregación de funciones respecto al origen y aprobación de estos documentos. Detectar errores e irregularidades para que sean informados y corregidos.

Establecer las medidas de control para que las correcciones y renvíos de los datos que fueron erróneamente ingresados se realicen, sin comprometer los niveles de autorización de las transacciones originales y en donde sea apropiado para la reconstrucción, retener los documentos fuentes originales durante el tiempo necesario.

Establecer las medidas de control para corroborar que las transacciones sean exactas, completas y válidas. Verificar la información ingresada y editar o devolver para corregir tan cerca del punto de origen como sea posible.

Alcance

Aplica en todos los ámbitos del Instituto; sus recursos, información, sus procesos internos o externos vinculados a través de contratos o acuerdos, así como al personal del Instituto en el ejercicio de sus funciones.

Responsabilidades

La Secretaría General y Jurídica, la Contraloría General, las Subdirecciones Generales, Coordinaciones Generales, Delegaciones Regionales, y el Centro de Investigación para el Desarrollo Sostenible, son responsables de homologar la información institucional.

Los dueños de los procesos y procedimientos son responsables de:

- Generar, gestionar, formalizar los formatos para entrada de información.
- Definir el listado de personal para el diseño y actualización de los formatos de entrada de información.
- Documentar en los procesos y procedimientos correspondientes los formatos para entrada de información.
- Establecer los criterios de entrega de los documentos fuente, así como para corroborar que la información sea íntegra y precisa.
- Definir e implementar mecanismos de control para los documentos fuente.
- Establecer los niveles de autorización para la entrada de información de transacciones en los procesos y procedimientos.
- Establecer los accesos de acuerdo con el rol y las responsabilidades definidas.
- Establecer en los procesos y procedimientos el uso de los documentos fuentes aplicables, así como las actividades para corrección y sobre-escritura de errores, y manejo de excepciones.
- Revisar periódicamente las bitácoras para verificar los errores de entrada de datos.
- Definir, en la medida de lo posible, mecanismos de control automático que corroboren que la información se ingrese de manera completa, correcta, precisa, confiable y oportuna.
- Definir e implementar mecanismos de control para la verificación de la integridad de transacciones, así como los errores.

La Subdirección General de Tecnologías de Información, a través del área que realiza las funciones de desarrollo, adquisición y mantenimiento de aplicativos, es responsable de implementar verificaciones y controles automáticos definidos por los dueños de los procesos y los procedimientos, en los aplicativos institucionales.

La Subdirección General de Tecnologías de Información, a través del área que realiza las funciones de seguridad informática, es responsable de establecer y ejecutar los procedimientos adecuados para proveer, registrar, modificar y eliminar los accesos y privilegios del personal del

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	31 de 57



Instituto a la infraestructura tecnológica, sistemas y aplicaciones institucionales, cumpliendo con los perfiles establecidos por los dueños de los procesos y procedimientos.

Los dueños de los procesos y procedimientos son responsables de hacer del conocimiento del personal externo, contratistas y usuarios de terceras partes, los formatos para entrada de información, así como la Política de Entrada de Información, y los exhortan a su cumplimiento.

Los dueños de los procesos y procedimientos son responsables de hacer del conocimiento de las entidades externas y contratistas, los formatos para entrada de información, así como la Política de Entrada de Información, y vigilan su cumplimiento.

El personal del Instituto es responsable de implementar y dar cumplimiento a la Política de Entrada de Información dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma, y de mantener especial cuidado en sus prohibiciones.

El personal del Instituto es responsable de hacer del conocimiento al personal externo, contratistas y entidades externas, la Política de Entrada de Información y exhortarlos a su cumplimiento.

El personal externo, contratistas y entidades externas son responsables de dar cumplimiento a la Política de Entrada de Información dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y mantener especial cuidado en sus prohibiciones.

8.1.1. Preparación de Información.

- a. Se debe homologar la información institucional definiendo las reglas de calidad, integridad, confidencialidad y disponibilidad de cada uno de los datos operativos.
- b. Se debe contar con una lista de personal autorizado para el diseño y actualización de los formatos de entrada de información, que incluya las firmas correspondientes.
- c. Se deben establecer los formatos para entrada de información, considerando controles para un adecuado y completo llenado en la información, exactitud del registro de los datos, control en el flujo de la información, así como facilitar la revisión de la información fuente contra la información en los aplicativos.
- d. Todos los formatos para entrada de información deben incluir características que aseguren la calidad e integridad de cada dato de entrada y la documentación mínima requerida (sin espacios vacíos, considerando menús y sub menús) y deben estar autorizados.
- e. Los formatos para entrada de información que no sean los autorizados o se encuentren incompletos, deben ser devueltos para su corrección al personal encargado de su preparación.
- f. En los formatos para entrada de información se debe asignar automáticamente un identificador único y secuencial para cada uno de ellos.
- g. Se deben formalizar en la normativa interna las actividades relacionadas con la Política de Preparación de Información.

8.1.2. Entrada de Datos

- a. Se deben usar los formatos autorizados para entrada de datos para el ingreso de la información operativa; los formatos para entrada de información debidamente completados deben ser considerados documentos fuente para el ingreso de información operativa.

- b. Como parte de los procesos y procedimientos se deben establecer los criterios para la entrega oportuna de los documentos fuente, y los criterios para corroborar que la información de dichos documentos sea íntegra y precisa.
- c. Se deben definir e implementar mecanismos de control para que la captura de los datos se realice conforme a los criterios de entrega de los documentos fuente.
- d. Se debe de corroborar que el documento fuente cuente con un identificador único; en caso de presentarse alguna excepción en el orden o de existir algún faltante en el identificador único y secuencial de cada documento fuente, se deben identificar y corregir el documento en incumplimiento.
- e. Se deben establecer los niveles de autorización requeridos para la captura, edición, autorización, aceptación y rechazo de la información, así como el tipo de información origen aceptable para cada tipo de transacción, considerando una adecuada segregación de funciones.
- f. Con base en los niveles de autorización definidos se deben formalizar y asignar los accesos de acuerdo con el rol y las responsabilidades definidas.
- g. Se deben definir e implementar mecanismos de control, los cuales consideren el despliegue de mensajes de error inmediatamente después de su identificación, mensajes de sobre-escritura y niveles de escalamiento de corrección de errores.
- h. Se deben definir e implementar mecanismos de control, los cuales consideren que, en el caso de presentarse errores en los datos de captura, no se ingresen los datos hasta que el error sea corregido o se sobrescriba. Los errores que no se puedan corregir inmediatamente deben registrarse en una bitácora de eventos suspendidos y se debe continuar con el ingreso de los datos válidos.
- i. Se debe establecer una revisión periódica de las bitácoras para verificar los errores y ejecutar un análisis de patrones de comportamiento e identificación de las causas raíz.
- j. Los documentos fuente deben ser resguardados por un periodo de tiempo suficiente de acuerdo con los requerimientos legales, regulatorios o de la operación.
- k. Se debe formalizar en los procesos y procedimientos Institucionales el uso de los documentos fuente aplicables a la operación.
- l. Se deben formalizar en la normativa interna las actividades relacionadas con la Política de Entrada de Información.

8.1.3. Verificación de Integridad de Transacciones.

- a. Se deben diseñar e implementar mecanismos de control para corroborar la precisión, integridad, validez y cumplimiento con los requerimientos del ingreso de los datos. Los controles pueden ser: de secuencia, límites mínimo y máximo, rangos, cifras control, validez, razonabilidad, menú de datos, existencia, verificación de llaves, dígito verificador, completitud, duplicidad, revisión de relaciones lógicas y ediciones limitadas por tiempo.
- b. Los datos de las transacciones generados manualmente, por sistema o mediante interfaces internas o externas, deben ser verificados automáticamente en su precisión, integridad y validez inmediatamente después de su ingreso, ya sean transacciones en línea o por lote.
- c. Se deben definir e implementar los mecanismos de control, los cuales consideren que, en caso de presentarse errores de validación de los datos de las transacciones, no se procesen las transacciones hasta que el error sea corregido o se sobrescriba. Los

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	33 de 57



errores que no se puedan corregir inmediatamente deben registrarse en una bitácora de eventos suspendidos y se debe continuar con el procesamiento de las transacciones válidas.

- d. Se deben definir los niveles de autorización requeridos para el ingreso, modificación y autorización de transacciones, así como para las reglas de validación de integridad, considerando una adecuada segregación de funciones.
- e. Con base en los niveles de autorización definidos, se deben formalizar y asignar los accesos de acuerdo con el rol y las responsabilidades definidas.
- f. Se deben formalizar en la normativa interna las actividades relacionadas con la Política de Verificación de Integridad de Transacciones.

8.2. Procesamiento de la Información.

Objetivo

Establecer las medidas de control preventivas, de detección y correctivas para mantener la integridad y validación de la información a través del ciclo de procesamiento y poder detectar transacciones erróneas, que no interrumpan el procesamiento de transacciones válidas.

Establecer las medidas de control para verificar el apropiado direccionamiento, autenticidad del origen e integridad de las transacciones entre los aplicativos institucionales, o con aplicativos de terceras partes. Mantener la autenticidad y la integridad durante la transmisión o el transporte de las transacciones.

Alcance

Aplica en todos los ámbitos del Instituto; sus recursos, información, sus procesos internos o externos vinculados a través de contratos o acuerdos, así como al personal del Instituto en el ejercicio de sus funciones.

Responsabilidades

Los dueños de los procesos y procedimientos son responsables de apegarse a las Políticas de Seguridad de la Información.

Los dueños de los procesos y procedimientos son responsables de:

- Definir implementar mecanismos de control para la integridad de procesamiento de transacciones, así como para la reconciliación de procesamiento, y la identificación, gestión, corrección y seguimiento de errores de procesamiento.
- Definir, en la medida de lo posible, mecanismos de control automáticos que corroboren que la información se ingrese de manera completa, correcta, precisa, confiable y oportuna.
- Establecer los niveles de autorización para el procesamiento de transacciones en los procesos y procedimientos.

La Subdirección General de Tecnologías de Información, a través del área que realiza las funciones de desarrollo, adquisición y mantenimiento de aplicativos, es responsable de implementar verificaciones y controles automáticos definidos por los dueños de los procesos y los procedimientos, en los aplicativos Institucionales.

La Subdirección General de Tecnologías de Información, a través de sus áreas operativas, es responsable de la gestión y control de las transacciones en los aplicativos institucionales y de la identificación, gestión y corrección de errores de procesamiento.

La Subdirección General de Tecnologías de Información, a través del área que realiza las funciones de seguridad informática, es responsable de establecer y ejecutar los procedimientos

adequados para proveer, registrar, modificar y eliminar los accesos y privilegios del personal del Instituto a la infraestructura tecnológica, sistemas y aplicaciones institucionales, cumpliendo con los perfiles establecidos por los dueños de los procesos y procedimientos.

Los dueños de los procesos y procedimientos son responsables de hacer del conocimiento del personal externo, contratistas y usuarios de terceras partes la Política de Procesamiento de la Información y los exhortan a su cumplimiento.

El personal del Instituto es responsable de implementar y dar cumplimiento a la Política de Procesamiento de la Información dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma, y de mantener especial cuidado en sus prohibiciones.

El personal del Instituto es responsable de hacer del conocimiento al personal externo, contratistas y usuarios de terceras partes la Política de Procesamiento de la Información y exhortarlos a su cumplimiento.

El personal externo, contratistas y usuarios de terceras partes son responsables de dar cumplimiento a la Política de Procesamiento de la Información dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y mantener especial cuidado en sus prohibiciones.

8.2.1. Integridad y Validez de Procesamiento.

- a. Se deben definir e implementar los mecanismos de control para autorizar el procesamiento de transacciones, corroborando el uso de aplicaciones y herramientas apropiadas, y autorizadas.
- b. Las salidas del procesamiento de transacciones deben incluir una bitácora que contenga las cifras control del procesamiento de dichas transacciones, considerando registros de entrada, procesados, rechazados, en suspenso, entre otros.
- c. Se debe verificar que el procesamiento de transacciones se realiza de forma completa y precisa mediante controles automáticos, los cuales deben incluir la revisión de errores de secuencia y de duplicados, conteo de transacciones/registros, revisión de relaciones lógicas y cifras control, revisión de rangos e insuficiencia de memoria para procesamiento.
- d. Se deben definir e implementar los mecanismos de control, los cuales consideren que en el caso de presentarse errores de transacciones no se procesen hasta que el error sea corregido o se sobreesciba la transacción. Los errores que no se puedan corregir inmediatamente deben registrarse en una bitácora de eventos suspendidos y se debe continuar con el procesamiento de las transacciones válidas.
- e. Se debe dar el seguimiento apropiado a las transacciones fallidas, hasta que los errores sean remediados o las transacciones sean canceladas.
- f. Se debe tener documentada formalmente la secuencia del procesamiento por lote, misma que debe ser implementada en las herramientas de programación de dicho procesamiento.
- g. Las salidas del procesamiento por lote deben incluir una bitácora que contenga la suficiente información relacionada a la secuencia del procesamiento por lote, para asegurar que los datos no son agregados inapropiadamente, cambiados o perdidos durante el procesamiento.
- h. A cada transacción se le debe asignar automáticamente un identificador único y secuencial.

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	35 de 57



- i. Se debe registrar en una bitácora las transacciones procesadas, incluyendo fecha y hora del ingreso de información e identificador de usuario que la ingresó, para cada transacción en línea o en procesamiento por lote; las modificaciones de datos maestros deben incluir el histórico de dichas modificaciones y responsable.
- j. Los aplicativos y bases de datos institucionales deben contar con mecanismos de control que mantengan la integridad de los datos ante interrupciones inesperadas durante el procesamiento de la información.
- k. Se deben definir e implementar los mecanismos de control para confirmar la integridad de los datos después de presentarse fallas o interrupciones durante el procesamiento de la información. Cualquier cambio al procesamiento debe ser reportado y aprobado antes de ser procesado.
- l. Se deben definir los niveles de autorización requeridos para el ingreso, modificación y autorización para el procesamiento de transacciones, así como para las reglas de validación, se debe asignar y formalizar que los ajustes y sobre-escritura de las transacciones y de los servicios críticos, sean revisadas por personal distinto al que ingresó los datos, considerando una adecuada segregación de funciones.
- m. Con base en los niveles de autorización definidos se deben formalizar y asignar los accesos de acuerdo con el rol y las responsabilidades definidas.
- n. Se debe llevar un mecanismo de control para reconciliar las transacciones procesadas, y de esta forma reportar y dar seguimiento a las diferencias identificadas.
- o. Se deben formalizar en la normativa interna las actividades relacionadas con la Política de Integridad y Validez de Procesamiento.

8.2.2. Autenticación e Integridad de Transacciones.

- a. La transferencia de información debe apegarse a las Políticas de Seguridad de la Información, que incluyen los mecanismos para la transferencia de la información, los acuerdos de transferencia de información, mensajería electrónica y acuerdos de confidencialidad de transferencia de información.
- b. Se deben formalizar en la normativa interna las actividades relacionadas con la Política de Autenticación e Integridad de Transacciones.

8.3. Salida de Información.

Objetivo

Establecer las medidas de control preventivas, de detección y correctivas, las actividades y roles asociados para corroborar que la salida de transacciones se maneja de una forma autorizada, es entregada al destinatario apropiado y protegida durante la transmisión, así mismo, se verifica, detecta y corrige la exactitud de la salida y se usa la información proporcionada en la salida.

Alcance

Aplica en todos los ámbitos del Instituto; sus recursos, información, sus procesos internos o externos vinculados a través de contratos o acuerdos, así como al personal del Instituto en el ejercicio de sus funciones.

Responsabilidades

Los dueños de los procesos y procedimientos son responsables de:

- Apegarse a las Políticas de Seguridad de la Información.
- Realizar revisiones de razonabilidad, precisión e integridad de las salidas.
- Conciliar las transacciones de entrada contra las cifras control del procesamiento.
- Definir las salidas de aplicativos institucionales que sean entrada para otro procesamiento. Monitorear que la información y el procesamiento cumplan las reglas de calidad, integridad, confidencialidad y disponibilidad, así como gestionar las excepciones de integridad que resulten.
- Comunicar las excepciones de integridad para que se implementen las acciones correctivas oportunas.

La Subdirección General de Tecnologías de Información, a través de sus áreas operativas, es responsable de la gestión y control del procesamiento por lote.

La Subdirección General de Tecnologías de Información, a través del área que realiza las funciones de desarrollo, adquisición y mantenimiento de aplicativos, es responsable de realizar un análisis de causa raíz, para ajustar las rutinas de procesamiento y/o los controles automáticos implementados.

El personal del Instituto es responsable de implementar y dar cumplimiento a la Política de Salida de Información dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma, y de mantener especial cuidado en sus prohibiciones.

El personal del Instituto es responsable de hacer del conocimiento al personal externo, contratistas y usuarios de terceras partes la Política de Salida de Información y exhortarlos a su cumplimiento.

El personal externo, contratistas y usuarios de terceras partes son responsables de dar cumplimiento a la Política de Salida de Información dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y mantener especial cuidado en sus prohibiciones.

8.3.1. Revisión y Conciliación de Salidas.

- a. La gestión y retención de las salidas de los aplicativos del Instituto, deben apegarse a las Políticas de Seguridad de la Información.
- b. Se deben realizar revisiones de razonabilidad, precisión e integridad de las salidas. Del resultado de estas revisiones, se deben reportar los errores potenciales, registrarlos en una bitácora y reportarlos para su análisis y corrección.
- c. Se debe realizar una conciliación entre las transacciones de entrada contra las cifras control del procesamiento, con la finalidad de asegurar la integridad y exactitud del procesamiento. En caso de identificar excepciones se deben registrar en una bitácora y reportarlas para su análisis y corrección.
- d. Cuando exista una secuencia de procesamiento por lote, el lote que se va a ejecutar debe validar que el lote previo se haya ejecutado correctamente para poder iniciar su procesamiento.
- e. Cuando se tenga una salida de un aplicativo institucional, la cual sea entrada para otro procesamiento, se debe validar la integridad de la salida antes de iniciar un nuevo procesamiento.
- f. Se deben formalizar en los procesos y procedimientos Institucionales las actividades relacionadas con la Política de Revisión de Salidas, Conciliación y Manejo de Errores de Transacciones.

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	37 de 57



8.3.2. Monitoreo de la Integridad de la Información.

- a. Se debe realizar periódicamente un monitoreo de la información que es generada, recibida, transmitida, procesada y almacenada para corroborar que esta cumpla las reglas de calidad, integridad, confidencialidad y disponibilidad, incluyendo la recibida por entidades externas.
- b. Se debe corroborar que la información que es generada y almacenada cuenta con el detalle suficiente y requerido, si es válida y si está soportada por evidencias que justifican la fuente de información.
- c. La información que no cumpla las reglas de calidad, integridad, confidencialidad y disponibilidad deben ser notificada puntualmente, monitoreada y analizada, para que se prioricen e implementen las acciones correctivas oportunas; cuando se trate de información proporcionada por una entidad externa se le debe reportar para que se implementen las acciones correctivas oportunas.
- d. La información de las excepciones de datos, transacciones y procesamiento debe conservarse para realizar un análisis de causa raíz, para ajustar las rutinas de procesamiento y los controles automáticos implementados.
- e. Los criterios y parámetros para el ingreso de datos y procesamiento de información que se encuentre en los aplicativos institucionales, deben ser revisados y confirmados periódicamente.
- f. La bitácora de las transacciones procesadas debe ser monitoreada periódicamente para corroborar que el procesamiento es completo, correcto, preciso, confiable y oportuno.
- g. Se deben formalizar en los procesos y procedimientos institucionales las actividades relacionadas con la Política de Monitoreo de la Integridad de la Información.

9. Políticas de Conciliación Contable-Operativa.

La información financiera debe ser útil, confiable, relevante, comprensible y comparable, para satisfacer las necesidades de los usuarios de la misma, en procura de lograr el control, la transparencia, la gestión eficiente, la rendición adecuada de cuentas y el cumplimiento de los objetivos de los estados financieros.

Estas políticas son una guía de actuación para los ejecutores directos e indirectos de las actividades relacionadas con el proceso contable del Instituto.

9.1. Política Contable.

Objetivo

Establecer las medidas de control preventivas, de detección y correctivas para llevar a cabo el proceso operativo-contable de tal manera que se pueda corroborar la razonabilidad de la información financiera, conforme a la normativa Institucional.

Alcance

Aplica en todos los ámbitos del Instituto; sus recursos, información, sus procesos internos o externos vinculados a través de contratos o acuerdos, así como al personal del Instituto que en el ejercicio de sus funciones operativas gestione registros contables.

Responsabilidades

La Contaduría General es responsable de:

- Definir los criterios de las operaciones financieras atendiendo lo establecido en las Normas de Información Financiera.
- Corroborar que la contabilidad se ajuste a la estructura básica para la aplicación de las Normas de Información Financiera y los criterios contables específicos que la CNBV establezca considerando la especialización de las operaciones del INFONAVIT.
- Establecer a los responsables de cuentas contables en cada área del Instituto.
- Establecer los criterios para gestionar y reportar la información financiera.
- Establecer el tiempo para quebrantar partidas de difícil recuperación.
- Autorizar los modelos contables de las áreas que, por la naturaleza de su operación, generen registros contables.
- Generar y entregar la información contable requerida por los Órganos Colegiados.
- Establecer un catálogo de cuentas contables.
- Corroborar y resguardar los registros contables (pólizas) con su documentación soporte.
- Corroborar que la normativa interna se encuentre alineada y operando con base en la normativa externa aplicable a criterios contables, incluyendo la normativa fiscal.
- Establecer los criterios para el proceso de conciliación contable-operativa.
- Enviar los saldos de las cuentas contables correspondientes a los responsables de cuentas contables.
- Definir e implementar los mecanismos de control para corroborar que las cuentas contables presenten saldos correctos.
- Establecer y difundir el calendario para el cierre contable.
- Solicitar la autorización del plan de trabajo y de la depuración de saldos.

El responsable de cuentas contables de cada área es responsable de:

- Reportar la información financiera requerida por la Contaduría General, en los tiempos que esta establezca.
- Solicitar la aprobación para el quebranto de partidas de difícil recuperación al H. Comité de Auditoría y al H. Consejo de Administración,
- Establecer los modelos contables en su ámbito de competencia y solicitar autorización a la Contaduría General.
- Generar y entregar la información contable requerida por los Órganos Colegiados.
- Registrar y cuantificar las transacciones con base en los criterios establecidos en las Disposiciones.
- Generar los registros contables, así como realizar reclasificaciones cuando sea necesario, con base en el catálogo de cuentas contables.
- Corroborar que los registros contables y sus reclasificaciones se encuentren y se autoricen con base en los criterios establecidos por la Contaduría General.
- Resguardar los registros contables (pólizas) con su documentación soporte.
- Corroborar que la normativa interna se encuentre alineada y operando con base en la normativa externa aplicable a criterios contables, incluyendo la normativa fiscal.
- Establecer la normativa interna para el proceso de conciliación contable-operativa interno y con las entidades externas correspondientes.
- Realizar y enviar la conciliación contable-operativa con base en los criterios establecidos por la Contaduría General.
- Definir e implementar los mecanismos de control para corroborar que saldos contables-operativos sean correctos.
- Realizar el cierre contable con base en los criterios establecidos por la Contaduría General.
- Solicitar la autorización del plan de trabajo y de la depuración de saldos.

El personal del Instituto es responsable de implementar y dar cumplimiento a la Política Contable dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma y de mantener especial cuidado en sus prohibiciones.

9.1.1. Fundamento contable.

- a. Se debe corroborar que la contabilidad del Infonavit se ajuste a la estructura básica para la aplicación de las Normas de Información Financiera Mexicanas (NIF) definidas por el Consejo Mexicano de Normas de Información Financiera, A.C. (CINIF), además debe observar los criterios contables de las NIF, excepto cuando la CNBV establezca normativa o criterios contables específicos considerando la especialización de las operaciones del Instituto.
- b. Se deben definir los criterios de las operaciones contables del Instituto atendiendo lo establecido en las Normas de Información Financiera (NIF) y las Disposiciones.

9.1.2. Unidades de operación contable y responsables de cuentas.

- a. Se debe establecer a un responsable de cuentas contables en cada área que, por la naturaleza de su operación, genere registros contables.
- b. La información financiera necesaria para presentarse ante los Órganos Colegiados y Entidades Externas debe ser reportada a la Contaduría General en los tiempos en que ésta la solicite.
- c. Cuando se necesite quebrantar partidas de difícil recuperación, que excedan el tiempo límite establecido por la Contaduría General, se debe solicitar autorización del H. Comité de Auditoría y del H. Consejo de Administración.
- d. Se debe de solicitar la aplicación de reservas a la Contaduría General, para las cuentas de difícil recuperación, que hayan excedido el tiempo límite establecido y que cuenten con la autorización del Comité de Auditoría y del H. Consejo de Administración.
- e. Se deben establecer los modelos contables en el ámbito de competencia, ya sea por mejora o por nuevos productos o servicios; así mismo, estos deberán presentarse a la Contaduría General para su autorización.
- f. Se debe generar y entregar la información contable requerida por los Órganos Colegiados en tiempo y forma.

9.1.3. Registro de transacciones y afectación de cuentas contables.

- a. Sólo se deben registrar transacciones propias de las actividades del Instituto, corroborando que se cumplan los requisitos establecidos en las Disposiciones.
- b. Las transacciones deben cuantificarse en unidades monetarias y registrarse considerando la fecha valor y fecha de registro.
- c. Debe existir un catálogo de cuentas contables, el cual debe ser seguido por las áreas que, por la naturaleza de su operación, generan registros contables.
- d. Considerando las características particulares de cada transacción, se deben registrar en la contabilidad.
- e. Se deben establecer los criterios para realizar registros contables de reclasificaciones y ajustes.
- f. Se debe verificar el cumplimiento del registro contable de las transacciones, así como los casos que requieran reclasificaciones y ajustes, los cuales deberán realizarse en apego a las Disposiciones.

- g. Las reclasificaciones y ajustes de cuentas se deben autorizar una vez que se asegure que el flujo contable se mantiene alineado al cumplimiento de los criterios contables definidos en las Disposiciones.
- h. La afectación de cuentas contables debe realizarse con base en lo establecido en los criterios contables de las Disposiciones y en el catálogo de cuentas contables vigente.
- i. Los registros contables (pólizas) con su documentación soporte, deben ser resguardados durante un tiempo mínimo de 10 años; vencido este plazo, se debe proceder conforme a las disposiciones en materia de archivos.
- j. La normativa interna debe estar alineada a la normativa externa aplicable a criterios contables, incluyendo la normativa fiscal.
- k. Los cambios en la normativa externa referentes a los criterios contables y fiscales deben ser plasmados en la normativa interna y en la operación, en tiempo y forma.
- l. Se debe dar cumplimiento a la normativa fiscal aplicable al Instituto de acuerdo con su área de responsabilidad.
- m. Se debe establecer y difundir el calendario mensual y anual de cierres contables a los responsables de cuentas contables.
- n. Los cierres contables mensuales y anuales se deben ajustar al calendario establecido por la Contaduría General.

9.1.4. Conciliación contable-operativa.

- a. Se debe establecer la normativa interna para el proceso conciliación contable-operativa, que incluya las prácticas para conciliar las transacciones con la contabilidad y el seguimiento de las partidas en conciliación, hasta que los saldos operativos y contables coincidan, con la finalidad de contar con información financiera confiable y oportuna.
- b. Se deben enviar los saldos contables a los responsables de cuentas contables para efectos de realizar la conciliación contable-operativa.
- c. La conciliación contable-operativa debe ser enviada a la Contaduría General en los plazos que ésta establezca.
- d. Se deben definir e implementar mecanismos de control para corroborar que las cuentas contables presenten saldos correctos, con la finalidad de contar con información financiera confiable y oportuna.
- e. Se debe establecer un proceso para realizar la conciliación operativa-contable mensual, así las actividades para el seguimiento oportuno de las partidas en conciliación, hasta que los saldos operativos y contables coincidan, con las entidades externas y con cualquier otro personal externo o contratista con el que se realicen actividades de operación crediticia, administración de cartera y administración del saldo de la subcuenta de vivienda, con la finalidad de contar con información financiera confiable y oportuna.
- f. Para las partidas que no sea posible conciliar se debe establecer un plan de trabajo para la depuración de saldos; dicho plan de trabajo y el resultado de la depuración de saldos debe estar revisado y autorizado por el Comité de Auditoría y el H. Consejo de Administración.

9.2. Política de Generación y Emisión de Reportes.

Objetivo

Establecer las medidas de control preventivas, de detección y correctivas para la generación de información operativa y contable que se presenta tanto en los reportes internos como en los reportes regulatorios solicitados por la CNBV.

Alcance

Aplica en todos los ámbitos del Instituto; sus recursos, información, sus procesos internos o externos vinculados a través de contratos o acuerdos, así como al personal del Instituto que en el ejercicio de sus funciones operativas gestione información financiera.

Responsabilidades

La Dirección General, la Secretaría General y Jurídica, la Contraloría General, las Subdirecciones Generales, las Coordinaciones Generales, Delegaciones Regionales, y el Centro de Investigación para el Desarrollo Sostenible, son responsables de:

- Definir e implementar los mecanismos de control para corroborar la razonabilidad de la información que se presenta en los estados financieros.
- Designar a uno o más responsables para la gestión y envío de los reportes regulatorios solicitados por la CNBV con base en las Disposiciones.
- Notificar a la Contaduría General la designación o baja de la persona responsable para la gestión y envío de reportes regulatorios.
- Corroborar que el responsable de generar los reportes regulatorios, los envíe a través del Sistema Interinstitucional de Transferencia de Información (SITI).
- Corroborar que se obtenga y resguarde el acuse de recibo original y copia por cada envío de reporte regulatorio.
- Corroborar que se entregue copia del acuse de recibo de los reportes regulatorios a la Contaduría General.
- Corroborar que el enlace único de la CNBV coordine las visitas de inspección.
- Corroborar que se gestionen los requerimientos de información solicitados.

La Contaduría General es responsable de:

- Establecer la normativa interna para la generación de los estados financieros y los reportes regulatorios requeridos.
- Definir e implementar los mecanismos de control para corroborar la razonabilidad de la información que se presenta en los estados financieros.
- Generar los estados financieros con base en los criterios establecidos en las Disposiciones.
- Presentar los estados financieros autorizados para la aprobación del Comité de Auditoría y el H. Consejo de Administración.
- Presentar los estados financieros aprobados a la CNBV y a otras entidades que lo requieran.
- Presentar los estados financieros dictaminados para autorización del Comité de Auditoría.
- Presentar los estados financieros dictaminados y autorizados al H. Consejo de Administración.
- Corroborar el cumplimiento de las fechas de elaboración y presentación de los estados financieros.
- Establecer los criterios para la información financiera con base en lo establecido en las Disposiciones.
- Establecer al responsable de autorizar la información a ser revelada.
- Corroborar que sea revelada la información de conformidad con lo establecido.
- Corroborar que sean difundidos en el portal Institucional los estados financieros dictaminados por el Auditor Externo, así como el dictamen correspondiente, en los plazos establecidos en las Disposiciones.

- Establecer a un enlace único entre la CNBV y las áreas del Instituto.

El personal del Instituto es responsable de implementar y dar cumplimiento a la Política de Generación y Emisión de Reportes dentro de sus áreas de responsabilidad; de abstenerse de realizar incumplimientos o infracciones a la misma, y de mantener especial cuidado en sus prohibiciones.

9.2.1. Preparación de Estados Financieros.

- a. Se debe establecer la normativa interna para la generación de los estados financieros, misma que permita corroborar la razonabilidad de la información que se presenta en los estados financieros.
- b. Se deben definir e implementar los mecanismos de control que permitan corroborar la razonabilidad de la información que se presenta en los estados financieros.
- c. Los estados financieros deben incluir un reporte autorizado sobre los resultados de la operación y la situación financiera del Instituto; el reporte debe incluir el análisis realizado y sus respectivos comentarios.
- d. Se deben elaborar los estados financieros mensuales, trimestrales y anuales, con las notas necesarias que presenten información relevante, los cuales deben ser expresados en los términos definidos en las Disposiciones.
- e. Los estados financieros y sus notas deben estar autorizados por el Director General, el Subdirector General de Planeación y Finanzas, el Contador General, el Auditor Interno, Coordinador General Jurídico y el Contralor General, antes de su presentación y solicitud de aprobación al Comité de Auditoría y al H. Consejo de Administración.
- f. Los estados financieros aprobados se deben presentar a la CNBV y a otras entidades que, por las operaciones que realizan con el Instituto los requieran, de acuerdo con la periodicidad establecida con dichas entidades.
- g. Los estados financieros dictaminados por el Auditor Externo se deben presentar para aprobación del Comité de Auditoría.
- h. Los estados financieros dictaminados por el Auditor Externo deben estar aprobados por el Comité de Auditoría antes de su presentación al H. Consejo de Administración.
- i. Los estados financieros dictaminados por el Auditor Externo deben contar con evidencia de la autorización del Comité de Auditoría para su presentación al H. Consejo de Administración.
- j. Se debe vigilar el cumplimiento de las fechas de elaboración y presentación de los estados financieros, establecidas en las Disposiciones.

9.2.2. Agrupación y revelación de información financiera.

- a. Se debe establecer a un responsable de autorizar la revelación de información.
- b. La agrupación de la información financiera debe realizarse de acuerdo con los criterios emitidos en las Disposiciones, corroborando la consistencia de la misma.
- c. Se deben establecer los criterios de selección de la información financiera para su revelación en las notas de los estados financieros.
- d. La información revelada a través de notas a los estados financieros debe alinearse a las necesidades del Instituto, conforme a los criterios de selección definidos, y en apego a lo establecido en las Disposiciones.

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	43 de 57



- e. La información revelada a través de notas a los estados financieros debe ser aprobada por el Director General, el Subdirector General de Planeación y Finanzas, el Contador General, el Auditor Interno, Coordinador General Jurídico y el Contralor General.
- f. La revelación de información solicitada por la CNBV mediante reportes regulatorios debe ser entregada con base en lo establecido en las Disposiciones.
- g. Se deben difundir en el portal Institucional los estados financieros trimestrales, así como los anuales dictaminados por el Auditor Externo, así como el dictamen correspondiente, en los plazos establecidos en las Disposiciones.

9.2.3. Reportes regulatorios.

- a. Se debe establecer la normativa interna para generación de reportes regulatorios, que permita corroborar la razonabilidad de la información que emite el Instituto en los reportes enviados a la CNBV.
- b. Se debe designar a un enlace único entre la CNBV y las áreas del Instituto, quien debe coordinar las visitas de inspección, así como la gestión de los requerimientos de información solicitados por la misma.
- c. Se debe designar a uno o más responsables para la gestión y envío de los reportes regulatorios solicitados por la CNBV con base en las Disposiciones. Se puede designar al número de personas que se considere necesario, en función del tipo de información de que se trate, en cumplimiento con lo establecido en las Disposiciones.
- d. La designación o baja del responsable de la gestión y envío de reportes regulatorios debe ser notificada a la Contaduría General para que sea del conocimiento de la CNBV mediante el formato correspondiente.
- e. El responsable o responsables del envío de los reportes regulatorios a la CNBV deben ser designadas por el Personal Directivo de las áreas responsables de su entrega, y estos deben contar cuando menos con un nivel jerárquico de dos niveles inferiores al del Director General.
- f. Se deben elaborar los reportes regulatorios, los cuales deben ser expresados en los términos definidos en las Disposiciones.
- g. Se debe corroborar que los reportes regulatorios sean generados con base en los requerimientos establecidos en las Disposiciones antes de su envío.
- h. Los reportes regulatorios deben ser enviados por el mecanismo establecido para esto, es decir, a través del Sistema Interinstitucional de Transferencia de Información (SITI).
- i. Para cada envío de un reporte regulatorio, se debe obtener y resguardar el acuse de recibo original y copia; se debe entregar a la Contaduría General una copia de cada acuse de recibo de los reportes regulatorios enviados a la CNBV.
- j. Se debe vigilar el cumplimiento de las fechas de elaboración y envío de los reportes regulatorios, establecidas en las Disposiciones.

10. Políticas de Seguridad de la Información.

Para el Instituto del Fondo Nacional de Vivienda para los Trabajadores la información de su operación y del personal es uno de sus activos más importantes y sin la cual sería imposible operar diariamente. Esta creciente dependencia de la información y de los sistemas que la manejan ha

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	44 de 57



hecho que las organizaciones den especial importancia a que sus activos de información se mantengan de forma segura, es decir, confidenciales, íntegros y disponibles.

A fin de cumplir con la tarea de brindar una protección adecuada a la información y sus recursos, es necesario contar con controles eficaces y eficientes, y la adopción de mejores prácticas, como es la norma ISO/IEC 27001:2013, de tal forma que se minimicen los riesgos en materia de Seguridad de la Información que pudieran afectar al Instituto.

El principal objetivo es establecer las Políticas de Seguridad de la Información, a fin de proporcionar las directrices para la protección de la información de los patrones, de los derechohabientes, del Instituto, de la operación crediticia y del personal del Instituto, así como de la información financiera.

Las políticas anteriormente referidas se encuentran descritas en el Manual General de Políticas de Seguridad de la Información (POL-CG-002) e incluyen los diversos aspectos del cómo se debe manejar la información en el Instituto y son aplicables al presente numeral en lo correspondiente a los siguientes temas específicos:

1. Política de Seguridad de la Información.
2. Política de Organización de Seguridad de la Información.
3. Política de Seguridad de la Información en los Recursos Humanos.
4. Política de Gestión de Activos.
5. Política de Control de Accesos.
6. Política de Cifrado.
7. Política de Seguridad Física y del Entorno.
8. Política de Seguridad de las Operaciones.
9. Política de Seguridad de las Comunicaciones.
10. Política de Adquisición, Desarrollo y Mantenimiento de Sistemas.
11. Política de Relación con Contratistas.
12. Política de Gestión de Incidentes de Seguridad de la Información.
13. Política de Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio.
14. Política de Cumplimiento.

11. Glosario de Términos y Acrónimos

Término/Acrónimo	Definición/Descripción
Acción de mejora	Actividades determinadas e implantadas para eliminar debilidades de control interno; diseñar, implementar y reforzar controles preventivos, de detección y correctivos; así como atender áreas de oportunidad que permitan fortalecer el Sistema de Control Interno Institucional.
Aceptación de riesgo	Decisión informada para aceptar un riesgo en particular.
Actividad	Conjunto de acciones o tareas que alguien emprende o practica como parte de sus funciones o responsabilidades.
Actividad crítica	Aquella actividad que debe ser realizada para la generación de los productos y servicios clave que permitan a la organización cumplir sus objetivos más importantes.

Activo de Información	<p>Se identifican los activos del Instituto como:</p> <p>Información: bases de datos, archivos de datos, documentación, contratos, acuerdos, manuales de usuario, material de capacitación, procesos y procedimientos operativos, planes de continuidad y contingencia, entre otros.</p> <p>Software: aplicativos, sistemas operativos, herramientas de desarrollo, etc.</p> <p>Físicos: equipamiento informático (procesadores, monitores, laptops), equipamiento de comunicaciones (teléfonos, contestadores automáticos), equipamiento de oficina (impresoras, destructoras de papel), medios magnéticos, dispositivos móviles y removibles de almacenamiento (cintas, discos, discos externos, USB), mobiliario, etcétera.</p> <p>Instalaciones: edificios, ubicaciones físicas, equipo eléctrico, red de agua y gas, etc.</p> <p>Servicios: servicios de cómputo y de comunicaciones, y servicios generales.</p>
Análisis de riesgos (Risk Analysis)	Proceso para comprender la naturaleza del riesgo y determinar el nivel del mismo, identificación y evaluación del grado de exposición a incidentes o fallas en la infraestructura tecnológica y estimación del posible daño causado en caso de presentarse una situación de este tipo.
Aplicativo institucional	Serie de programas informáticos diseñados para procesar, obtener, manipular, administrar, controlar tareas específicas, con la finalidad de cumplir con las especificaciones y necesidades operativas de los usuarios.
Auditor	Persona con los conocimientos y experiencia, capaz de realizar actividades de auditoría como son revisar, examinar y evaluar diversos procesos y procedimientos de una organización.
Auditoría	Proceso sistemático, independiente y documentado para obtener evidencia y evaluarla objetivamente, para determinar la medida en la cual se cumple un criterio de auditoría.
Autenticación	Acto o proceso de confirmar que alguien es quien dice ser. El probador (parte que se identifica) es un usuario que requiere acceder a ciertos recursos, y el verificador (parte que verifica la identidad) es un sistema que protege el acceso a

	dichos recursos y tiene que verificar que el usuario tiene permisos para acceder a estos.
Autenticidad	Propiedad de que una entidad es quien dice ser.
Bitácora	Registro manual o automático que describe de forma cronológica los eventos relevantes que cumplen o no con los estándares previamente definidos, los cuales deben tener el detalle suficiente para realizar las actividades de seguimiento.
Calidad de la información	Datos que en su conjunto cumplen con los estándares establecidos de longitud, formato, composición, aceptación de caracteres especiales, etc.
Cambio de funciones	Situación en la que el personal es promocionado, degradado o reubicado (situación en la cual su posición jerárquica se mantiene, pero cambia la unidad organizativa en la que se encuentra).
Clasificación de información	Proceso mediante el cual se determina que la información en su poder, actualiza alguno de los supuestos de reserva o confidencialidad.
CNBV	Comisión Nacional Bancaria y de Valores.
Competencia profesional	Cualificación para llevar a cabo las responsabilidades asignadas, la cual requiere habilidades y conocimientos, que son adquiridos generalmente con la formación y experiencia profesional y certificaciones. Se expresa en la actitud y el comportamiento de los individuos para llevar a cabo sus funciones y cumplir con sus responsabilidades.
Confiabilidad	Propiedad de comportamiento y resultados consistentes.
Confidencialidad	Propiedad que asegura el acceso solamente por personal o entidad autorizada y es conocida también como privacidad o secrecía.
Conflictivo de interés	Situación en que el juicio de una persona, interfieren con el cumplimiento de sus funciones dentro del Instituto.
Conformidad	Cumplimiento de un requisito.
Consecuencia	Resultado de un evento que afecta a los objetivos.
Contratista	Empresas y su personal que proveen productos o servicios al Instituto.
Control	Proceso de verificar el desempeño de distintas áreas o funciones de una organización.

	Usualmente implica una comparación entre un rendimiento esperado y un rendimiento observado, para verificar si se están cumpliendo los objetivos de forma eficiente y eficaz, y tomar acciones correctivas cuando sea necesario.
Control de Acceso	Asegurar que el acceso a los activos se encuentra autorizado o restringido de acuerdo a los requerimientos del negocio y de la seguridad.
Criterio de Valoración de Riesgos	Medidas cualitativas contra las cuales los efectos de materialización de un riesgo pueden ser evaluados respecto a los objetivos de negocio.
Criticidad	Importancia de un activo o función de la empresa y el impacto del mismo cuando no está disponible.
Custodio de los Activos	Persona designada por el Dueño de Activos, encargada de administrar y hacer efectivos los controles de seguridad que el Dueño de Activos haya definido.
Datos personales	Información que revela aspectos personales que deben manejarse con la confidencialidad o reservas del caso, como el origen étnico o racial, estado de salud, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas y preferencia sexual, entre otros.
Debilidad de control	Insuficiencia, deficiencia o inexistencia de mecanismos de control, que obstaculizan o impiden el logro de las metas y objetivos institucionales, o materializan un riesgo, identificadas mediante la supervisión, verificación y evaluación interna y/o externa.
Desastre	Resultado de la ocurrencia de uno o más agentes perturbadores severos y/o extremos, concatenados o no, de origen natural, de la actividad humana o aquellos provenientes del espacio exterior, que cuando acontecen en un tiempo y en una zona determinada, causan daños y que por su magnitud exceden la capacidad de respuesta de la comunidad afectada.
Disposiciones	Disposiciones de carácter general aplicables a los organismos de fomento y entidades de fomento. Circular Única de los Órganos y Entidades de Fomento (CUOEF),

Disponibilidad	Propiedad que asegura que los activos de la información son utilizables para personal autorizado en su uso y demanda.
Dispositivos de almacenamiento externo	Conjunto de componentes utilizados para leer, grabar o guardar datos en el soporte de almacenamiento de datos, en forma temporal o permanente, tales como disco duro externo, USB y almacenamiento magnético u óptico.
Dispositivos móviles	Instrumento con capacidades de procesamiento, con conexión a Internet, con memoria, diseñado específicamente para una función, pero que pueden llevar a cabo otras funciones más generales, tales como teléfono celular, tableta y laptop.
Documento fuente	Formato pre establecido que contiene los campos a ser completados por los dueños de los datos, con el objetivo de que se tenga dicha información disponible para su ingreso en los sistemas.
Dueño del Activo	Persona que define un activo de información de la cual es responsable, y por ende, tiene la facultad de definir su sensibilidad y los derechos de acceso de los demás usuarios.
Ediciones limitadas por tiempo	Restricciones del tiempo de edición de información en los sistemas que le son asignadas a los usuarios.
Eficacia	Cumplimiento de objetivos establecidos, en lugar, tiempo, calidad y cantidad.
Eficiencia	Logro de objetivos y metas programadas con la misma o menor cantidad de recurso
Elemento Crítico	Descripción cualitativa utilizada para enfatizar la importancia de un recurso, proceso o función que debe estar disponible y en operación constante lo más pronto posible después de que ocurra un incidente, desastre o emergencia.
Equipo Auditor	Grupo de auditores designados para desempeñar una auditoría dada; el equipo auditor puede incluir expertos técnicos y auditores en prácticas. Uno de los auditores del equipo desempeña la función de auditor líder.
Esquema de sensibilidad	Esquema que se organiza en diferentes categorías, las cuales determinan el grado de sensibilidad de la información, para definir el nivel de protección de la información.
Estados de la información	Situación física, lógica o electrónica en la que se puede encontrar la información; se identifican los siguientes 3 estados: procesamiento, en el que la

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	49 de 57



	información es modificada en parte o en su totalidad o bien, es utilizada para crear nueva información; almacenamiento en el que la información se encuentra contenida en algún sitio determinado para su resguardo; y tránsito, en el que la información cambia de un contenedor a otro.
Estrategia de Mitigación	<p>Medida utilizada para prevenir, detectar, mitigar o recuperarse ante un riesgo, dentro de la que se consideran las siguientes:</p> <p>Mitigación o Aplicación de controles: También conocido como Reducción del riesgo; consiste en la situación en la cual la organización valora los riesgos como significativos, de acuerdo a un criterio de aceptación de riesgos, y se toma la decisión de tratamiento de los mismos, para lo cual se realiza un análisis que incluye la valoración de los controles adecuados utilizados como contramedida para prevenir, detectar, mitigar o materializar un riesgo de seguridad.</p> <p>Asumir (retención): Se admite el riesgo por parte de la Organización.</p> <p>Transferir el riesgo: Cuando la organización determina que no es posible la atención directa de la amenaza se puede optar por la atención tercerizada de la amenaza; la tercerización puede incluir una unidad específica en la atención de la amenaza al interior de la organización o la atención externa por parte de un contratista ajeno a la organización.</p> <p>Evasión del riesgo: En algunos casos, un análisis del escenario de la amenaza puede permitir la evasión o eliminación de algún componente o circunstancias del escenario de amenaza y con esto la materialización del mismo.</p>
Evaluación de riesgos (Risk Evaluation)	Proceso donde se mide el riesgo mediante parámetros que lo determinan, la magnitud de la pérdida o daño posible, y la probabilidad de que dicha pérdida o daño llegue a ocurrir.
Evidencia	Base racional para llegar a conclusiones de auditorías confiables y reproducibles en un proceso sistemático.
Evidencia de la auditoría	Registros, declaraciones de un hecho u otra información que sea pertinente para los criterios de auditoría y que son verificables. <i>Reference: ISO 19011:2002 Guidelines for quality and/or environmental management systems auditing.</i>

Gestión de la Continuidad del Negocio	Proceso de gestión integral que identifica las amenazas potenciales de una organización y los impactos que pueden causar en la operación del negocio en caso de materializarse; por otro lado, la Gestión de la Continuidad del Negocio (BCM por sus siglas en inglés <i>Business Continuity Management</i>), proporciona un marco para la estructura organizacional con la capacidad para dar una respuesta efectiva que salvaguarde los intereses de sus grupos de interés clave, las actividades de creación de valor y reputación.
Gestión	Conjunto de decisiones, procesos, acciones y actividades que hacen uso eficiente y consistente de personal, tiempo y otros recursos necesarios para lograr un objetivo.
Gestión de riesgos	Proceso dinámico desarrollado para contextualizar, identificar, analizar, evaluar, responder, supervisar y comunicar los riesgos, incluidos los de corrupción, inherentes o asociados a los procesos, mediante el análisis de los distintos factores que pueden provocarlos, con la finalidad de definir las estrategias y acciones que permitan mitigarlos y asegurar el logro de metas y objetivos de una manera razonable, en términos de eficacia, eficiencia y economía en un marco de transparencia y rendición de cuentas.
Hallazgo de auditoría	Conclusión que se obtiene de la evaluación de la evidencia que se reúne durante la auditoría contra los criterios definidos Institucionalmente.
Homologar información	Equivalencia en la forma en que se mantiene la información dentro de los sistemas
Impacto	Consecuencias negativas que se generarían en la Institución, en el supuesto de materializarse el riesgo, amenaza o vulnerabilidad.
Incidente de continuidad al negocio	Situación que puede degradar o interrumpir los servicios críticos de una organización.
Incidente de seguridad de la información	Se considera como un incidente de seguridad: al acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a las Políticas de seguridad del Instituto.
INFONAVIT	Instituto del Fondo Nacional de la Vivienda para los Trabajadores.

Información	Conjunto organizado de datos con significado para quien los utiliza. Ésta puede encontrarse impresa o alojada en equipos de cómputo, servidores o dispositivos externos de almacenamiento.
Información completa	Característica de la información física que es procesada por un sistema informático y que a su salida mantiene sus valores originales.
Infraestructura tecnológica	Conjunto de elementos o dispositivos tecnológicos necesarios para dar soporte a las operaciones de la organización, entre las cuales se consideran elementos de hardware, p.ej. servidores, routers, equipo de cómputo, cableado, impresoras, teléfonos, etcétera, y elementos de software, p.ej. sistemas operativos, programas de cómputo, aplicaciones, funciones, bases de datos o bien conocidos como: Equipo electrónico de procesamiento, transmisión y/o almacenamiento de información. Programas de sistemas operativos, de administración tanto de bases de datos como de transacciones. Datos almacenados en dispositivos electrónicos, magnéticos y ópticos.
Instituto	INFONAVIT.
Integridad	Propiedad que asegura que la información no es alterada sin autorización en su transporte, procesamiento o almacenamiento. La información puede encontrarse en tres estados: procesamiento, almacenamiento y transmisión; ejemplos son: información física como documentos o fotocopias, información lógica como archivos en medios electrónicos o tecnológicos, transmitida como una conversación de pasillo o procesada como un video interno.
Interrupción	Evento previamente anticipado o no, que causa una desviación negativa en la generación de los productos y servicios conforme a los objetivos de la organización.
Mecanismo de control	Actividades determinadas e implantadas por el personal del Instituto para alcanzar los objetivos institucionales, prevenir y administrar los riesgos identificados, incluidos los de corrupción y de tecnologías de la información. Medidas físicas, tecnológicas, procedurales y administrativas aplicadas a fin de prevenir y

	corregir incidentes de seguridad de la información en el Instituto.
Mecanismo de control correctivo	Mecanismo específico de control que opera en la etapa final de un proceso, el cual permite identificar y corregir o subsanar en algún grado, omisiones o desviaciones.
Mecanismo de control de detección	Mecanismo específico de control que opera en el momento en que los eventos o transacciones están ocurriendo, e identifican las omisiones o desviaciones antes de que concluya un proceso determinado.
Mecanismo de control preventivo	Mecanismo específico de control que tiene el propósito de anticiparse a la posibilidad de que ocurran incumplimientos, desviaciones, situaciones no deseadas o inesperadas que pudieran afectar al logro de las metas y objetivos institucionales.
Mejora continua	Actividad recurrente para superar el rendimiento.
Modo de falla	Manera por la cual se analiza la ocurrencia de un error; generalmente describe la forma en que este ocurre, y el impacto en la operación de la organización.
Monitoreo	Determinar el estado de un sistema, proceso o una actividad.
Nivel del riesgo	Magnitud del riesgo expresado en términos de la combinación de las consecuencias y la probabilidad.
Objetivo de Control	Declaración de alto nivel de la postura de la Dirección en relación a los Riesgos de Seguridad de un área de interés que se desea gestionar a través del uso de controles que sean relevantes para la organización.
Partes involucradas	Son todas aquellas personas que tienen relación con los procesos en donde se encuentren no conformidades o en donde se identifiquen mejoras.
Perfil del Activo de Información	Descripción de características únicas, requerimientos de seguridad, cualidades, propiedad y valor para cada tipo de activos de información.
Personal del Instituto	Las trabajadoras y los trabajadores adscritas (os) a la Dirección General, de la Secretaría General y Jurídica, de la Contraloría General, de las Subdirecciones Generales: de Planeación y Finanzas, de Crédito, de Administración de Cartera, de Atención y Servicios, de

Instituto del Fondo Nacional de la Vivienda para los Trabajadores				
Manual General de Políticas de Control Interno				
Clave de Identificación: POL-CG-001	Versión	0	Hoja	53 de 57



	Administración y Recursos Humanos, de Comunicación, de Tecnologías de Información, de las Coordinaciones Generales Jurídica, de Recaudación Fiscal, de Riesgos, de Delegaciones Regionales, y el Centro de Investigación para el Desarrollo Sostenible. Además, se considera a las y los integrantes de los Órganos del Instituto.
Personal Directivo del Instituto	Titulares de la Dirección General, de la Secretaría General y Jurídica, de la Contraloría General, de las Subdirecciones Generales: de Planeación y Finanzas, de Crédito, de Administración de Cartera, de Atención y Servicios, de Administración y Recursos Humanos, de Comunicación, de Tecnologías de Información, de las Coordinaciones Generales Jurídica, de Recaudación Fiscal, de Riesgos, de Delegaciones Regionales, y el Centro de Investigación para el Desarrollo Sostenible.
Personal externo	Personal de contratistas que prestan servicios usando información Institucional y dentro de los aplicativos Institucionales.
Personal responsable	Encargados de implementar el plan de acción y reportar los resultados.
Plan de acción	Es la lista de actividades a realizar para corregir o mejorar algún proceso y que incluye al menos: personal responsable, recursos, fechas compromiso, reportes, reuniones.
Plan de continuidad del negocio (BCP)	Documento que guía a la organización para responder, recuperar, retomar y restaurar los niveles de operación previamente definidos después de una interrupción; normalmente este plan engloba los recursos, servicios y actividades necesarias para garantizar la continuidad del negocio.
Plan de continuidad del servicio	Colección documentada de procesos, procedimientos e información, que es desarrollada, compilada y mantenida para ser usada en caso de ocurrir un incidente, permitiendo a la organización continuar con sus actividades críticas en un nivel aceptable de operación previamente definido.
Plan de recuperación de desastres (DRP)	Documento que establece paso a paso las actividades para habilitar los elementos críticos de la organización a un nivel aceptable frente a un escenario de amenaza de alto impacto.

Probabilidad	Estimación de que se materialice un riesgo, en un periodo determinado. Posibilidad o frecuencia de ocurrencia de un evento.
Proceso	Secuencia de pasos con algún tipo de lógica que se enfoca en lograr algún resultado específico.
Registro	Anotación de ciertos eventos que son relevantes para el Instituto y deben constar permanentemente de forma oficial tales como: <ul style="list-style-type: none"> ▪ Listas de asistencia. ▪ Registros de incidentes. ▪ Eventos de seguridad. ▪ Bitácoras.
Riesgo de seguridad de la información	Medida en la cual un activo de información es amenazado por una circunstancia potencial o un evento que puede afectar en su pérdida de confidencialidad, integridad o disponibilidad y refleja los impactos adversos potenciales a las operaciones de la organización, activos de la organización, reputación o prestigio, a los datos de las personas, otras organizaciones, etcétera.
Riesgo	Evento adverso e incierto (externo o interno) que derivado de la combinación de su probabilidad de ocurrencia y el posible impacto pudiera obstaculizar o impedir el logro de las metas y objetivos institucionales. Nivel de impacto sobre las operaciones de la organización (incluyendo misión, funciones, imagen o reputación) y de los activos de la organización o personas, resultado de la operación de un sistema de información dado el impacto potencial de una amenaza y la probabilidad de que ésta ocurra.
Riesgo de fraude	Posibilidad de que por acción u omisión, mediante el abuso del poder o el uso indebido de recursos y de información, empleo, cargo o comisión, se dañan los intereses de una institución, para la obtención de un beneficio particular o de terceros; incluye corrupción, soborno, fraude, apropiación indebida u otras formas de desviación de recursos por personal del instituto, nepotismo, extorsión, tráfico de influencias, uso indebido de información privilegiada, entre otras prácticas.
Riesgo de seguridad	Posibilidad de ocurrencia de un evento no deseado que quebrante los requerimientos de confidencialidad, integridad o disponibilidad de un activo.

Riesgo residual	Riesgo resultante de la aplicación de controles de seguridad necesarios para el tratamiento de un riesgo identificado previamente. Éste es aceptable de acuerdo a los criterios de aceptabilidad definidos por la Dirección de la organización.
Seguridad de la información	Preservación de la confidencialidad, integridad y disponibilidad de la información. Son las medidas utilizadas (metodologías, controles, métricas o medidas, buenas prácticas, estándares, marcos de trabajo, políticas, mecanismos, herramientas, procesos, procedimientos, etcétera) en la administración del riesgo asociado a la información.
Siniestro	Situación crítica y dañina generada por la incidencia de uno o más fenómenos perturbadores en un inmueble o instalación afectando a su población y equipo, con posible afectación a instalaciones circundantes.
Término del Empleo	Situación en la que el personal termina su contrato, funciones, servicios o relación laboral con el Instituto.
Tipo de información	Estado de la información; la información puede ser física, la cual se presenta en documentos o fotocopias con valor para la organización; y puede ser lógica, que es la información intangible que se puede encontrar en medios electrónicos o tecnológicos.
Titular de los datos personales	Persona física a quien corresponden los datos personales.
Transacción en línea	Procesamiento de los datos de forma manual, mediante el ingreso de las solicitudes una por una.
Transacción por lote	Procesamiento de varias transacciones de forma automática mediante la configuración en sistema del orden, entradas y salidas requeridas.
Usuario	Personal con acceso a los activos de información del Instituto, con base en su rol y responsabilidad.
Usuario con derechos de acceso privilegiados	Personal con acceso con privilegios para la modificación y eliminación de activos de información del Instituto, con base en su rol y responsabilidad, que además puede tener la facultad de crear, modificar y eliminar perfiles de usuarios y asignar privilegios.
Usuario de terceras partes	Personal subcontratado por contratistas para proporcionar productos o servicios.

Valoración de riesgos	Actividades que tienen el objetivo de identificar, contextualizar, analizar y evaluar los riesgos de seguridad que enfrenta la organización.
Vulnerabilidad	Cualquier debilidad o falla de seguridad en un sistema, proceso o activo.

12. Disposición Transitoria

ÚNICA. Las presentes políticas entrarán en vigor al día siguiente de su publicación en la Intranet del Infonavit. Ahora bien, las políticas específicas que a continuación se mencionan deberán estar implementadas en su totalidad conforme a lo siguiente:

LAS POLÍTICAS CONTENIDAS EN LOS NUMERALES	A MÁS TARDAR
5. Políticas de Control Interno.	30 de abril de 2018
6. Políticas de Normativa.	28 de febrero de 2018
6.1. De la normativa.	31 de enero de 2018
6.1.1. Conformación de la normativa.	31 de enero de 2018
6.1.2. De la publicación, difusión y capacitación de la normativa.	31 de enero de 2018
6.1.3. De la actualización de la normativa.	31 de enero de 2018
6.1.4. De la vigencia y conservación de la normativa.	31 de enero de 2018
6.2. Cumplimiento Normativo.	28 de febrero de 2018
6.2.1. Del cumplimiento normativo.	28 de febrero de 2018
6.2.2. De la interpretación de la normativa.	28 de febrero de 2018
7. Políticas de Gestión de la Operación.	30 de abril de 2018
7.1. Control de las Operaciones.	28 de febrero de 2018
7.1.1. Control Operativo.	28 de febrero de 2018
7.1.2. Control Operativo de las Áreas.	28 de febrero de 2018
7.1.2.1. Contraloría General.	28 de febrero de 2018
7.1.2.2. Coordinación General de Riesgos.	28 de febrero de 2018
7.1.2.3. Secretaría General y Jurídica.	28 de febrero de 2018
7.1.2.4. Subdirección General de Administración de Cartera.	28 de febrero de 2018
7.1.2.5. Subdirección General de Administración de Crédito.	28 de febrero de 2018
7.1.2.6. Subdirección General de Administración y Recursos Humanos.	28 de febrero de 2018
7.1.2.7. Subdirección General de Atención y Servicios.	28 de febrero de 2018
7.1.2.8. Subdirección General de Comunicación.	28 de febrero de 2018
7.1.2.9. Subdirección General de Planeación y Finanzas.	28 de febrero de 2018
7.1.2.10. Subdirección General de Tecnologías de Información.	28 de febrero de 2018
7.2. Monitoreo y Mejora Continua.	30 de abril de 2018
7.2.1. Monitoreo de la Operación.	31 de marzo de 2018
7.2.2. Control de Personal Externo y Contratistas.	30 de abril de 2018

7.3. Gestión del Fraude.	30 de abril de 2018
7.3.1. Prevención de Fraude.	30 de abril de 2018
7.3.2. Detección de Fraude.	30 de abril de 2018
7.4. Declaración Patrimonial y de Posible Conflicto de Interés.	28 de febrero de 2018
7.4.1. Esquema de la Declaración.	28 de febrero de 2018
8. Políticas de Integridad de la Información.	30 de abril de 2018
8.1. Entrada de Información.	28 de febrero de 2018
8.1.1. Preparación de Información.	28 de febrero de 2018
8.1.2. Entrada de Datos	28 de febrero de 2018
8.1.3. Verificación de Integridad de Transacciones.	28 de febrero de 2018
8.2. Procesamiento de la Información.	31 de marzo de 2018
8.2.1. Integridad y Validez de Procesamiento.	30 de marzo de 2018
8.2.2. Autenticación e Integridad de Transacciones.	30 de marzo de 2018
8.3. Salida de Información.	30 de abril de 2018
8.3.1. Revisión y Conciliación de Salidas.	30 de abril de 2018
8.3.2. Monitoreo de la Integridad de la Información.	30 de abril de 2018
9. Políticas de Conciliación Contable-Operativa.	31 de marzo de 2018
9.1. Política Contable.	28 de febrero de 2018
9.1.1. Fundamento contable.	28 de febrero de 2018
9.1.2. Unidades de operación contable y responsables de cuentas.	28 de febrero de 2018
9.1.3. Registro de transacciones y afectación de cuentas contables.	28 de febrero de 2018
9.1.4. Conciliación contable-operativa.	28 de febrero de 2018
9.2. Política de Generación y Emisión de Reportes.	31 de marzo de 2018
9.2.1. Preparación de Estados Financieros.	31 de marzo de 2018
9.2.2. Agrupación y revelación de información financiera.	31 de marzo de 2018
9.2.3. Reportes regulatorios.	31 de marzo de 2018
10. Políticas de Seguridad de la Información.	30 de abril de 2018