	Área	Dirección de Administración de Riesgos
	Nombre del documento	Documento de Seguridad
	Información Confidencial	En la sección Análisis de Riesgo, se testa las columnas: Riesgo/ Amenaza tipo de Riesgo Operacional CNBV (nivel 3), Factor de Riesgo, Clasificación del factor, Control del factor, Impacto probabilidad de que ocurra, Valor (columnas ubicadas en las páginas 28 a 36 del Documento).
	Fundamento legal	Por considerarse información RESERVADA conforme a lo establecido en los artículos 110, fracciones IV y VII de la Ley Federal de Transparencia y Acceso a la Información Pública; 113, fracciones IV y VII de la Ley General de Transparencia y Acceso a la Información Pública y lo relacionado con el Vigésimo Segundo y Vigésimo Sexto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"
	Firma del Titular del Área	Act. Aurora Cbeta Moreno Cortes
	Fecha de clasificación	25 de Junio 2020



	Área	Dirección de Seguridad de la Información
	Nombre del documento	Documento de Seguridad
	Información Confidencial	<p>En la sección Análisis de Brecha se testan las columnas: Respuesta, Brecha % y Brecha (columnas ubicadas en las páginas 40 a 56 del Documento).</p> <p>En la sección Plan de Trabajo se testan las columnas: Brecha Atención, Acciones de Remediación (columnas ubicadas en las páginas 57 a 60 del Documento).</p> <p>En la sección Mecanismos de Monitoreo y Revisión de las Medidas de Seguridad se testan las columnas: Medidas de Seguridad Actuales y Brecha (columnas ubicadas en las páginas 60 a 62 del Documento).</p>
	Fundamento legal	<p>Por considerarse información RESERVADA conforme a lo establecido en los artículos 110, fracciones IV y VII de la Ley Federal de Transparencia y Acceso a la Información Pública; 113, fracciones IV y VII de la Ley General de Transparencia y Acceso a la Información Pública y lo relacionado con el Vigésimo Segundo y Vigésimo Sexto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"</p>
	Firma del Titular del Área	Ing. José Antonio Martínez Sanchez
	Fecha de clasificación	25 de Junio 2020

Documento de Seguridad

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Nacional Financiera S.N.C., I.B.D.

CONTENIDO

I. Introducción.....	- 2 -
II. Objetivo	- 3 -
III. Alcance	- 3 -
IV. Marco Normativo	- 3 -
V. Glosario.....	- 4 -
VI. Inventario de Datos Personales y de los Sistemas de Tratamiento.	- 7 -
VII. Funciones y Obligaciones de las personas que traten Datos personales.	- 11 -
VIII. Medidas de Seguridad	- 20 -
IX. Análisis de Riesgos	- 24 -
X. Análisis de Brecha.....	- 37 -
XI. Plan de Trabajo.....	- 57 -
XII. Mecanismos de Monitoreo y Revisión de las medidas de seguridad.....	- 60 -
XIII. Programa General de Capacitación.	- 63 -
XIV. Actualizaciones.....	- 64 -
XV. Elaborado por.....	- 65 -

I. Introducción

Reconocida en los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos, toda persona tiene derecho a la protección de sus Datos personales, siendo la protección de éstos un derecho humano, tanto para el acceso, rectificación y cancelación y oposición en los términos que las leyes establezcan.

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) es el organismo constitucional autónomo garante del cumplimiento de dos derechos fundamentales: el de acceso a la información pública y el de protección de datos personales.

El 26 de enero de 2017, se promulgó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), que tiene por objeto establecer las bases, principios y procedimientos regulando su tratamiento, a efecto de garantizar el derecho que tiene toda persona física a la protección de sus datos personales en posesión de sujetos obligados.

Por sujetos obligados, de acuerdo a la LGPDPPSO, entendemos en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

El 26 de enero de 2018, el INAI publicó en el Diario Oficial de la Federación el acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público, que tienen por objeto desarrollar las disposiciones previstas en la Ley General.

A partir de la publicación de la Ley General y de los Lineamientos Generales de Protección de Datos Personales, Nacional Financiera, como institución del Gobierno Federal, adquiere el carácter de “Responsable” y debe tratar dichos datos conforme a los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad; adoptando medidas de seguridad en atención a los sistemas de datos que utiliza, plasmando en un documento de seguridad dichas medidas técnicas, físicas y administrativas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que poseen las distintas áreas de la Institución.

II. Objetivo

En cumplimiento a lo dispuesto en el artículo 35 de la LGPDPPSO, se elaboró el presente documento con el propósito de recopilar, establecer y difundir las políticas internas que deberán observar los Funcionarios Responsables y Responsables designados, para la gestión y tratamiento de los datos personales que posee NAFIN.

El presente Documento de Seguridad tiene como objetivo plasmar las medidas de seguridad técnicas, físicas y administrativas mínimas adoptadas por la Institución para proteger los datos personales contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confiabilidad, integridad y disponibilidad.

III. Alcance

Para todas las Direcciones de NAFIN que, en el ejercicio de sus atribuciones y funciones, administren información en sistemas de tratamiento de Datos personales, ya sea sistemas completos, o tramos de información que le correspondan.

Para el tratamiento de Datos personales en dispositivos físicos y/o electrónicos, con independencia de su creación, procesamiento, almacenamiento y organización.

Para todo el personal de Nacional Financiera que tenga acceso a los Datos personales, estará obligado a conocer y aplicar las medidas de seguridad para cada sistema en que se concentren los datos, y aplicable a cada una de las fases de tratamiento de los Datos personales, desde la obtención de los mismos y hasta su eliminación. Manteniendo la obligación de confidencialidad, aún después de finalizada la participación en el tratamiento de los Datos personales, ya sea por cambio de funciones o por finalización de la relación laboral con la Institución.

IV. Marco Normativo

- Constitución Política de los Estados Unidos Mexicanos, Artículos 6 y 16.
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.



- Ley General de Transparencia y Acceso a la Información Pública.
- Ley Federal de Transparencia y Acceso a la Información Pública.
- Lineamientos generales de protección de datos personales para el sector público.

V. Glosario

Para los efectos de este Documento de Seguridad se entenderá por:

Aviso de privacidad: Documento de forma física, electrónica o en cualquier formato, que es generado por el responsable y puesto a disposición de los titulares de los Datos personales, a partir del momento en el cual se recaben sus Datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.

Bases de datos: Conjunto ordenado de Datos personales bajo criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

CISO: (Chief Information Security Officer), Ejecutivo de nivel superior dentro de una organización responsable de establecer y mantener la visión, la estrategia y el programa de la empresa para garantizar que los activos y las tecnologías de la información estén adecuadamente protegidos.

CNBV: Comisión Nacional Bancaria y de Valores.

Comité de Transparencia: Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los Datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual, entre otras.



Derechos ARCO: Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de Datos personales.

Documento de Seguridad: Instrumento que describe y da cuenta, de manera general, sobre las medidas de seguridad físicas y técnicas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los Datos personales que posee.

Encargado: Persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate Datos personales a nombre y por cuenta del responsable.

Instituto o INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

LGPDPPO: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos Generales: Lineamientos Generales de Protección de Datos Personales para el Sector Público.

Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los Datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
- b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
- c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y
- d) Proveer a los equipos que contienen o almacenan Datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los Datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:

- a) Prevenir que el acceso a las Bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;



- b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
- c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y
- d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de Datos personales.

NAFIN: Nacional Financiera, S.N.C.

Portabilidad de Datos personales: Prerrogativa del titular de obtener una copia de los datos que ha proporcionado al responsable del tratamiento en un formato estructurado que le permita seguir utilizándolos.

Responsable: El Director titular de un área administrativa que decide sobre el tratamiento físico o electrónico de los Datos personales.

Responsables designados / Enlaces en materia de Transparencia: Los funcionarios designados por los Directores Generales Adjuntos y los Directores de Área, quienes apoyarán en todo momento las actividades relacionadas con Datos personales.

Riesgo: Combinación de la probabilidad de un evento y su consecuencia desfavorable.

SNT: Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Sistemas: Conjunto ordenado de Datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, que estén en posesión de NAFIN, con independencia de su forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

Titular: Persona física a quien corresponden los Datos personales.

Transferencias: Toda comunicación de Datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del Titular, del Responsable o del Encargado.

Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los Datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de Datos personales.

Unidad Administrativa: Área a la que se le confieren atribuciones específicas en el Manual de Organización de Nacional Financiera, S.N.C.

Unidad de Transparencia: Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.

VI. Inventario de Datos Personales y de los Sistemas de Tratamiento.

Los sistemas que se detallan en el presente documento son aquellos que contienen Datos personales, que se encuentran tanto en soporte electrónico como físico.

De conformidad con lo establecido en el artículo 35 fracción I de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de manera enunciativa mas no limitativa, en el **Anexo 1** se presenta el inventario de Datos personales que recaba NAFIN.

NAFIN cuenta con los siguientes sistemas de tratamiento de Datos personales:

1.1. Físicos

NAFIN cuenta con un Cuadro General de Clasificación Archivística que es el instrumento técnico que refleja la estructura del archivo con base en las atribuciones y funciones de cada una de las Unidades Administrativas que integran la Institución, de igual manera cuenta con un Catálogo de Disposición Documental, este instrumento refleja el registro general y sistemático que establece los valores documentales, los plazos de conservación (vigencia documental) en Archivo de Trámite y Concentración y el destino final.

Este cuadro general y catálogo de disposición documental tienen como objetivos:

- Contar con la estructura documental completa de la Institución, que sirva para clasificar e identificar los expedientes y documentos con una clave y título que derivan de la estructura y atribuciones de cada una de sus áreas.
- Facilitar el acceso y la consulta de la documentación desde su creación en las Unidades Administrativas hasta su recepción y resguardo en los Archivos de Trámite y Concentración, mediante la organización, descripción y vinculación de los documentos de archivo.

La estructura del Cuadro General de Clasificación Archivística está conformada de la siguiente manera:

Niveles de Archivo	Descripción
Fondo	La propia Institución
Subfondo	Dirección General y Direcciones Generales Adjuntas
Sección	Direcciones de Área y Direcciones Regionales
Subsección	Subdirecciones, Gerencias y Oficinas Estatales de Promoción
Serie	Conjunto de documentos producidos en el desarrollo de una misma atribución general
Subserie	Documentos que versan sobre una materia o asunto específico dentro de una serie

Los diferentes archivos de la Institución se ubican en instalaciones con seguridad en accesos, y en condiciones físicas adecuadas para su operación, con instrumentos que permiten la prevención y atención de siniestros reduciendo el impacto en el daño a los documentos, tales como:

- Control y administración del archivo documental a través de un sistema automatizado.
- Control y registro de acceso diario mediante esquema de identificación y grabación ante cámara de circuito cerrado.
- Registro y seguimiento de préstamo, consulta y devolución de expedientes.
- Catálogo de firmas de personal autorizado para ingreso específico al Acervo.
- Vigilancia las 24 horas, los 365 días del año.
- Sistema de circuito cerrado de televisión.
- Sistema y equipo contra de Hidrante para incendio con tablero de control central, con equipo eléctrico y de combustión.
- Programas permanentes de fumigación y mantenimiento.

- Instrumentos de medición de temperatura y humedad.

NAFIN tiene conformado un Sistema Institucional de Archivos que comprende el control total de todo el ciclo vital del documento, lo que permite identificar, registrar, clasificar, organizar y administrar la totalidad del acervo Institucional en donde se encuentre, ya sea en trámite, concentración, o inclusive, histórico, considerando en el mismo la información que contenga Datos personales.

En el **Anexo 2**, se presenta la relación de enlaces en materia de Transparencia y Archivo designados en NAFIN, quienes tienen la obligación de observar las medidas de seguridad que se establecen en los Criterios Específicos de Archivos. Dicho Anexo se actualizará cuando se requiera, debido a los movimientos de personal en la Institución.

1.2. Electrónicos

A continuación, se detalla el universo de los sistemas informáticos en los que el responsable identifica que contienen datos personales dentro de la Institución:

INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO	
Área administrativa responsable	Sistemas
Dirección de Canales Alternos	E - FILE
	E - CONTRACT
	NAFIN ELECTRÓNICO
Dirección Cadenas Productivas	SISTEMA DE GESTIÓN PROMOCIÓN Y VENTAS
Dirección de Administración Crediticia	SISTEMA INSTITUCIONAL DE RECUPERACIÓN Y ADMINISTRACIÓN DE CARTERA (SIRAC)
	BURÓ DE CRÉDITO (BNC)
	SISTEMA DE INFORMACIÓN DE CARTERA (SICAR)
	SISTEMA GUARDA VALORES (GVAL)
	MESA DE CONTROL DE CRÉDITO (MDC)
	SISTEMA INTEGRAL DE ADMINISTRACIÓN DE GARANTÍAS (SIAG)
Dirección de Crédito	CONSULTA A BURÓ DE CRÉDITO

INVENTARIO DE DATOS PERSONALES Y DE LOS SISTEMAS DE TRATAMIENTO	
Área administrativa responsable	Sistemas
Dirección de Seguimiento y Recuperación	SISTEMA DE SEGUIMIENTO DE CRÉDITO (SISEC)
	SISTEMA DE CALIFICACIÓN DE CARTERA BATCH ELECTRÓNICA (CCBE)
	SISTEMA DE CALIFICACIÓN DE CARTERA (SCC)
	SISTEMA DE RECUPERACIÓN Y SEGUIMIENTO (SIRYS)
Dirección de Recursos Humanos y Calidad	SISTEMA INTEGRAL PARA LA ADMINISTRACIÓN DE RECURSOS HUMANOS
Dirección de Desarrollo Empresarial y Asistencia Técnica	CAPASISTEC
	PLATAFORMA E-LEARNING PARA CAPACITACIÓN EMPRESARIAL EN LÍNEA (www.nafintecapacita.com) (*)
Dirección de Contraloría Interna	SISTEMA DE OPERACIONES RELEVANTES E INUSUALES (SORI)
Dirección Venta de Títulos en Directo al Público	SERVICIOS EN SITIO (*)
	CETESDIRECTO (*)

(*) Nota: La infraestructura tecnológica de estos sistemas informáticos no están hospedados en los centros de cómputo (primario y alterno) de NAFIN.

2. Especificación del tipo de Datos personales contenidos en los sistemas

2.1. Físicos

El Sistema Integral de Archivos administra la documentación conforme al Catálogo de Disposición Documental, el cual permite identificar aquellas series documentales que las Unidades Administrativas declararon contenían Datos personales, adicional a que cada expediente cuenta con su portada de identificación, lo que permite dar mayor seguridad a dicha información. Es obligación de los Responsables, administrar los Datos personales contenidos en sus expedientes, conforme a portada de expediente (**Anexo 3**).

Como se menciona en los Criterios específicos para la organización, clasificación, conservación, custodia y baja de los archivos de NAFIN, la guarda y custodia de los acervos documentales implica la integridad de los soportes y la confiabilidad de la información, para lo cual, los Responsables aseguran que, a través de sus Responsables designados de Archivos de Trámite, la documentación que generen esté debidamente custodiada.

Tanto los expedientes, documentos y mobiliario en donde se custodian los archivos documentales, se identifican por medio de etiqueta archivística (**Anexo 4**) de acuerdo a lo establecido por los presentes citados criterios. La custodia de los archivos no sólo corresponde al acceso y a su integridad, sino también a su conservación física, cuidando las condiciones mínimas de los repositorios.

La conservación documental se orienta tanto a la integridad física de la información documentada (el soporte) como a su integridad funcional (el material sustentado).

Todo expediente que se solicite en préstamo se devuelve a su lugar de origen con la documentación completa y sin alteraciones en el contenido de la información, para lo cual los Responsables designados de Archivos de Trámite y el área solicitante, tienen la obligación de cotejar la integridad de la documentación que contienen los expedientes al momento de la entrega y la recepción.

2.2. Electrónicos

Es obligación de los Responsables administrar los sistemas electrónicos de datos personales y su contenido, toda vez que son quienes controlan el uso y explotación de los mismos.

VII. Funciones y Obligaciones de las personas que traten Datos personales.

Con fundamento en lo dispuesto por los artículos 83 y 84, fracciones I y V de la LGPDPPSO, el Comité de Transparencia es la autoridad máxima en materia de protección de Datos personales y tiene entre sus funciones la de coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los Datos personales en NAFIN.

La Dirección Seguridad de la Información y la Coordinación General de Archivos como áreas reguladoras y administradoras de los sistemas de Datos personales electrónicos y físicos, respectivamente, proporcionarán la información que requiera el Comité de Transparencia.

Los Responsables deberán dar atención y aplicar las medidas que en materia de Datos personales establezca NAFIN.

Es obligación de los Responsables administrar sus sistemas de Datos personales técnicos y/o físicos y su contenido, toda vez que son quienes controlan el uso y explotación de los mismos.

Los Responsables deberán observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de Datos personales y Datos personales sensibles.

Todo Tratamiento de Datos personales que efectúen los Responsables deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.

Los Responsables podrán tratar Datos personales para finalidades distintas a aquellas establecidas en el Aviso de privacidad correspondiente, siempre y cuando cuenten con atribuciones conferidas en la ley y medie el consentimiento del Titular, salvo que sea una persona reportada como desaparecida, en los términos previstos en la LGPDPPSO y demás disposiciones que resulten aplicables en la materia.

Los Responsables no deberán obtener y tratar Datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del Titular y la expectativa razonable de privacidad.

Cuando no se actualicen algunas de las causales de excepción previstas en el artículo 22 de la LGPDPPSO, el Responsable deberá contar con el consentimiento previo del Titular para el Tratamiento de los Datos personales, el cual deberá otorgarse de forma:

- I. Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del Titular;
- II. Específica: Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el Tratamiento, e
- III. Informada: Que el Titular tenga conocimiento del Aviso de privacidad previo al Tratamiento a que serán sometidos sus Datos personales.



El consentimiento podrá manifestarse de forma expresa o tácita. Se deberá entender que el consentimiento es expreso cuando la voluntad del Titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.

El consentimiento será tácito cuando habiéndose puesto a disposición del Titular el Aviso de privacidad, éste no manifieste su voluntad en sentido contrario.

Por regla general será válido el consentimiento tácito, salvo que la ley o las disposiciones aplicables exijan que la voluntad del Titular se manifieste expresamente.

Tratándose de Datos personales sensibles el Responsable deberá obtener el consentimiento expreso y por escrito del Titular para su Tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en el artículo 22 de la LGPDPPSO.

Los Responsables deberán adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los Datos personales en su posesión, a fin de que no se altere la veracidad de éstos.

Toda Transferencia de Datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su Titular, salvo las excepciones previstas en los artículos 22, 66 y 70 de la LGPDPPSO.

1. Acceso a los sistemas de Datos personales en medios físicos:

Los Responsables deberán:

- Autorizar expresamente a través de un escrito, a los servidores públicos que fungirán como encargados y/o usuarios para el acceso a la documentación, en los casos en los que no exista un instrumento jurídico que los faculte para el desempeño de sus funciones. El escrito deberá enviarse a la Coordinación General de archivos y Unidad de Transparencia para formalizar la designación.
- Contar con una relación actualizada de las personas que tengan acceso a los expedientes que contengan Datos personales.
- Establecer las medidas de seguridad descritas en los Criterios Específicos y normatividad interna para el resguardo de los expedientes que contengan Datos personales, los cuales eviten la alteración, pérdida o acceso no autorizado.

- Informar sin dilación alguna al Comité de Transparencia de NAFIN, sobre la alteración o modificación; pérdida o destrucción; robo o extravío, copia, uso, acceso o tratamiento no autorizado a los Datos personales a su cargo, que afecte la seguridad de los mismas, señalando las acciones que se llevaron a cabo para contrarrestar sus efectos.
- Cuidar que los tipos de datos que se solicitan al Titular sean los estrictamente necesarios para el proceso al cual se refiere y así instruirlo al encargado y/o usuario.
- En caso de detectar la existencia de Datos personales inexactos, deberán corregirlos o actualizarlos a la brevedad posible, y en su caso obtener el respaldo documental que justifique dicha corrección o actualización, la cual deberá informar la modificación mediante oficio emitido por el Titular para su posterior información y autorización del Comité de Transparencia.
- Prever las acciones necesarias para que los Titulares puedan ejercer sus Derechos ARCO.
- Señalar a los encargados y/o usuarios su responsabilidad respecto de la confiabilidad y veracidad de los tipos de datos recabados.
- Informar al Comité de Transparencia de NAFIN, a través de la Unidad de Transparencia, sobre la creación, modificación sustancial o cancelación los sistemas de Datos personales, dentro de los quince días hábiles siguientes a que ocurra alguno de los supuestos mencionados.
- Cumplir las medidas de seguridad previstas por la Dirección de Seguridad de la Información y la Coordinación General de Archivos, necesarias para garantizar la integridad y control en el acceso a los expedientes con Datos Personales a su cargo.
- Garantizar que todas las personas que intervengan en cualquier fase del Tratamiento de los Datos personales, guarden confidencialidad respecto de éstos.
- Informar al Titular, a través del Aviso de privacidad, la existencia y características principales del Tratamiento al que serán sometidos sus Datos personales, a fin de que pueda tomar decisiones informadas al respecto.



- En la Transferencia de Datos personales, deberá garantizar la confidencialidad y únicamente los utilizará para los fines que fueron transferidos atendiendo a lo convenido en el Aviso de privacidad que le será comunicado por el Responsable.
- Establecer procedimientos sencillos que permitan el ejercicio de los Derechos ARCO, cuyo plazo de respuesta no deberá exceder de veinte días contados a partir del día siguiente a la recepción de la solicitud del Titular.

Los encargados y usuarios deberán:

- Acatar las medidas de seguridad previstas por la Dirección de Seguridad de la Información y la Coordinación General de Archivos para el resguardo de expedientes con Datos personales.
- Registrar en la bitácora correspondiente, los accesos al área de resguardo de los documentos físicos que contienen los Datos personales.
- Por ningún motivo deben retirar de las instalaciones de la Institución o difundir información sin la autorización expresa del Responsable del sistema de Datos personales.
- En caso de detectar alguna alteración, pérdida o acceso no autorizado al área de resguardo de los documentos, notificar de manera inmediata al Responsable del sistema.

La Coordinación General de Archivos deberá:

- Integrar el Catálogo de firmas del personal autorizado para el préstamo y consulta de expedientes.
- Adoptar las medidas necesarias en caso de alteración, pérdida o acceso no autorizado a los expedientes que mantiene en resguardo.
- Difundir a los Responsables y suplentes designados la normatividad en materia de Archivos.
- A través del Programa Anual de Organización, Conservación y Depuración de Archivos, supervisar en cada Unidad Administrativa que los expedientes estén registrados con clasificación de información (reservada y/o confidencial) se encuentre debidamente localizada topográficamente, resguardada y bajo llave.

- Establecer los mecanismos necesarios que garanticen que los servidores públicos que causan baja o se separan de su empleo, cargo o comisión, devuelvan los expedientes que hayan solicitado al Archivo de Trámite, de Concentración, o en su caso histórico, mediante la liberación de la Constancia de no adeudo de expedientes; en caso que corresponda se integra dicho documento al Acta Entrega Recepción de sus funciones.

La Unidad de Transparencia tendrá, entre otras, las siguientes funciones:

- Integrar el catálogo de Responsables, Responsables designados, encargados y usuarios de los sistemas de Datos personales.
- Supervisar que la lista de Responsables, Responsables designados, encargados y usuarios de los sistemas de Datos personales se encuentre actualizada.
- Integrar y mantener actualizada la relación de personal en materia de Transparencia y Archivo designados por los Responsables en NAFIN.
- Adoptar las medidas necesarias en caso de alteración, pérdida o acceso no autorizado a los documentos que contienen la información de los Datos personales.
- Difundir a los Responsables y Responsables designados, Enlaces, encargados y usuarios la normatividad que se emita por parte del INAI.
- Implementar campañas de difusión hacia todo el personal de NAFIN respecto al tema de Protección de Datos Personales, normatividad aplicable y responsabilidades como servidores públicos.
- Coordinar con el Comité de Transparencia la implementación de acciones en materia de Protección de Datos Personales.
- Supervisar en cada Unidad Administrativa responsable de sistemas de Datos personales la total aplicación de medidas en materia de Protección de Datos Personales.
- Gestionar las solicitudes para el ejercicio de los derechos ARCO ante los Responsables.



- Establecer mecanismos para asegurar que los Datos personales solo se entreguen a su Titular o su representante debidamente acreditados.
- Informar al Titular o su representante el monto de los costos a cubrir por la reproducción y envío de los Datos personales, con base en lo establecido en las disposiciones normativas aplicables.
- Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO.
- Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO.
- Asesorar a las áreas adscritas al Responsable en materia de protección de datos personales.

El Comité de Transparencia tendrá, entre otras, las siguientes funciones:

- Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los Datos personales en NAFIN
- Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO.
- Supervisar, en coordinación con las Áreas o Unidades Administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el presente Documento de Seguridad.

2. Acceso a los sistemas de Datos personales en medios electrónicos:

La Dirección de Seguridad de la Información en conjunto con la Dirección de Informática tiene definidas e implementadas políticas, responsabilidades y mecanismos de seguridad lógica diseñados para asegurar la integridad, confidencialidad y disponibilidad de la información de los sistemas informáticos de la Institución, los cuales están alineados a las Disposiciones de Carácter General Aplicables a las Instituciones de Crédito (Circular Única de Bancos – CUB), emitidas por la CNBV y al Manual



Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información, MAAGTICSI.

Responsabilidades Generales

- Es responsabilidad de todos los empleados de la organización a todos los niveles, el apego irrestricto a los responsabilidades, políticas y estándares publicados en Intranafin, relacionados con la seguridad de la información y seguridad informática establecidos en los manuales respectivos.
- Es responsabilidad de todos los empleados de la organización, a todos los niveles, proteger la confidencialidad, integridad y autenticidad de la información bajo su cargo, porque conoce y cumple las políticas de seguridad establecidas.
- Cada sistema informático institucional cuenta con un administrador, quien es responsable de cumplir con las obligaciones establecidas para el administrador detalladas más adelante, además de las generales.
- La Dirección de Seguridad de la Información participará en la definición y verificará el continuo cumplimiento de las políticas y procedimientos de seguridad de la información establecidos en la Institución.
- Es responsabilidad de las Subdirecciones de Informática considerar el cumplimiento de los estándares técnicos y de seguridad vigentes, en el ámbito de sus responsabilidades y asignaciones dentro de la Institución.
- Es responsabilidad de la Dirección de Seguridad de la Información la verificación del continuo cumplimiento de los estándares técnicos y de seguridad vigentes.

Responsabilidades de los administradores de Sistemas Aplicativos Centrales

- Todo sistema cuenta con un usuario administrador responsable del mismo, y un suplente. Este usuario administrador y suplente serán servidores públicos de la Institución y serán designados por escrito ante la Dirección de Informática por el Responsable del área correspondiente, formalizados mediante convenio de niveles de servicio.

- El usuario administrador es el responsable de asignar y autorizar los perfiles de usuario y de administrar la información.
- Es responsabilidad del usuario administrador asegurar que todos los usuarios del sistema informático a su cargo cuenten con una clave solicitada por el procedimiento establecido.
- El usuario administrador es responsable de autorizar o en su caso rechazar las solicitudes de acceso a sistemas centrales de los usuarios finales.
- El usuario administrador es el responsable de solicitar a la Dirección de Informática las bajas que deban aplicarse en los sistemas de su responsabilidad por medio de la solicitud de “Claves de usuarios de sistemas centrales”, y para Servicios Centrales Web deberá revocar el acceso desde la PAU, asegurando que las cuentas activas son las que deben continuar vigentes.
- El usuario administrador es responsable de asegurar que las cuentas asignadas sean individuales y no existan cuentas de uso grupal o general que sean compartidas por usuarios distintos para los sistemas a su cargo.
- En caso de cambio de usuario administrador y/o suplente, el Responsable debe notificarlo por escrito a la Dirección de Informática.
- Todos los cambios informáticos a los sistemas aplicativos institucionales son aprobados por sus respectivos usuarios administradores de acuerdo al procedimiento de control de cambios vigente.
- El usuario administrador es el único facultado para solicitar y autorizar la generación de respaldos, copias o transferencias de la información contenida en los sistemas centrales en producción bajo el procedimiento vigente.
- El usuario administrador es el único facultado para solicitar a producción central ampliación de línea o apertura de línea bajo el procedimiento vigente.
- El Responsable tendrá la obligación de supervisar y asegurar el cumplimiento de las responsabilidades de los usuarios administradores.
- El Responsable y el administrador del sistema por ser los responsables de la información son los únicos que pueden solicitar a la Dirección de Informática la cancelación y/o baja de Producción del sistema aplicativo central, en la que indique los motivos por los cuales solicitan la baja.



- La baja se formaliza mediante un acta denominada “Acta de Baja del Sistema”, en cuanto a la protección de los datos se indica el respaldo requerido, su vigencia y después del término de dicha vigencia el destino final de la información ya sea destrucción o envío de archivo muerto y posterior destrucción, esto se alinea a los procesos de cada área de negocio.

VIII. Medidas de Seguridad

1. Medidas de Seguridad Administrativas

NAFIN cuenta con políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel Institucional, la identificación, clasificación, y eliminación (borrado seguro) de la información, tales como:

- Manual Normativo de Políticas de Seguridad de la Información.
- Manual Operativo de Calidad Informática
- Manual Operativo de Desarrollo Aplicativo
- Manual Operativo de Desarrollo de Infraestructura
- Manual Operativo de Gestión Administrativa de Informática
- Manual Operativo de Infraestructura Distribuida y Telecomunicaciones
- Manual Operativo de Planeación Tecnológica
- Manual Operativo de Seguridad Informática
- Manual Operativo de Servicios de Producción Central
- Manual Operativo Administración Integral de Riesgos
- Políticas, Responsabilidades, Estándares y Lineamientos de Seguridad Informática
- Lineamientos para el control y uso de computadoras personales, periféricos, accesorios, programas de cómputo y archivos de información
- Lineamientos, políticas y estándares de Infraestructura de Cómputo personal
- Modelo de Gobierno de Seguridad de la Información
- Manual Operativo del Sistema Institucional de Archivos.

Los cuales tienen por objeto identificar los riesgos a los que se encuentran expuestos y que atentan contra la disponibilidad, integridad y confidencialidad de la información almacenada en Tecnologías de la Información, para proponer soluciones y definir políticas de seguridad, procurando su cumplimiento y contribuyendo a disminuir el impacto en la Institución.

Desde septiembre de 2019, NAFIN cuenta con la Dirección de Seguridad de la Información a cargo del Oficial en Jefe de Seguridad de la Información (CISO), cuyas funciones principales destacan:

- Participar en la definición y verificar la implementación y continuo cumplimiento de políticas y procedimientos de seguridad de la información dentro de la Institución.
- Proponer y coordinar los programas de capacitación y concientización en materia de seguridad de la información y evaluar la efectividad de los mismos.
- Asegurar la correcta implementación de regulación emitida por diferentes autoridades en materia de seguridad de la información.

2. Medidas de Seguridad Físicas

NAFIN cuenta con políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel Institucional, la identificación, clasificación y baja de documentos, tales como:

Criterios Específicos para la Organización, Clasificación, Conservación, Custodia y Baja de los Archivos de Nacional Financiera, S.N.C. (Criterios)

El Sistema Integral de Archivos administra la documentación conforme al Catálogo de Disposición Documental, el cual permite identificar aquellas series documentales que las Unidades Administrativas declararon contenían Datos personales, adicional a que cada expediente cuenta con su portada de identificación, lo que permite dar mayor seguridad a dicha información. Es responsabilidad de cada Titular de Unidad Administrativa, administrar los Datos personales contenidos en sus expedientes.

De conformidad con los Criterios, la guarda y custodia de los acervos documentales implica la integridad de los soportes y la confiabilidad de la información, para lo cual los Titulares de las Unidades Administrativas aseguran que, a través de sus Responsables de Archivos de Trámite la documentación que generen esté debidamente custodiada. Para ello la Institución tiene adoptadas las siguientes medidas de seguridad:

- Niveles de conservación. El mobiliario (archiveros metálicos con medidas estándar) utilizado en las oficinas de la Institución protege los soportes físicos de luz solar y polvo y mantiene los documentos bajo llave. En cuanto al Archivo de Concentración la documentación se resguarda en contenedores especiales, los cuales se encuentran colocados en racks y estantería dentro de los depósitos con las medidas de seguridad adecuadas.

- El mobiliario en donde se custodian los archivos documentales, se identifican por medio de etiqueta archivística que contiene el logotipo de NAFIN, la leyenda “Coordinación General de Archivos”, el nombre de la Unidad Administrativa y el número de archivero.
- En caso de que existan expedientes parcialmente clasificados como reservados y/o confidenciales, las Unidades Administrativas se cercioran de que los expedientes que se soliciten en préstamo sean las versiones públicas de los mismos.
- Todo expediente que se solicite en préstamo se devuelve a su lugar de origen con la documentación completa y sin alteraciones en el contenido de la información, para lo cual los Responsables de Archivos de Trámite y el área solicitante, tienen la obligación de cotejar la integridad de la documentación que contienen los expedientes al momento de la entrega y la recepción.
- Los expedientes clasificados como reservados y/o confidenciales se resguardan en lugares seguros y bajo llave.
- Seguridad física. Las zonas de acceso restringido cuentan con un sistema de vigilancia de circuito cerrado al interior del inmueble. Dicho sistema realiza grabaciones las 24 hrs. del día los 7 días de la semana acumulando soportes en medios digitales por un periodo de hasta 90 días.
- Modelo de control de acceso. Es obligatorio el acreditar la identidad en individuos y etiquetar los equipos de cómputo que permanecerán temporalmente en las instalaciones.

Bitácoras para accesos y operación cotidiana

En cuanto al Archivo de Concentración, se cuenta con una bitácora de acceso, Catálogo de firmas para el personal autorizado para el préstamo, consulta y devolución de expedientes, así como control y seguimiento de las solicitudes, a través del formato “vale de préstamos”, el cual cumple con el procedimiento y los elementos establecidos en las Disposiciones Generales en las materias de Archivos y de Gobierno Abierto para la Administración Pública Federal y su Anexo Único.

Registro de incidentes

El Responsable, llevará un registro de incidentes en el que se consigne los procedimientos realizados para la consulta, los Datos personales comprometidos y en



su caso, recuperación de acervos para permitir una disponibilidad de la información, indicando la persona que resolvió el incidente, la metodología aplicada, los datos recuperados y, en su caso, que datos ha sido necesario grabar manualmente en el proceso de recuperación.

3. Medidas de Seguridad Técnicas

La administración de los sistemas de Datos personales y su contenido, son responsabilidad de los Titulares de las Unidades Administrativas, quienes controlan el uso y explotación de los mismos.

La Dirección de Informática cuenta con procedimientos y controles para asegurar que las Bases de datos se administren únicamente por el personal autorizado. Adicionalmente, se cuenta con herramientas de protección para el monitoreo, con la finalidad de identificar en forma oportuna accesos no autorizados a la información contenida en ellas.

- **Generar privilegios o perfiles de acceso a los Datos personales en función de las atribuciones y funciones de cada usuario.** Los sistemas informáticos institucionales, cuentan con mecanismos de acceso orientados a la identificación de los usuarios y a la capacidad de operación que tienen dentro de los mismos, de tal manera que, mediante la definición de roles, perfiles y permisos, se segmenta la operación de los sistemas.
- **Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información.** Los Centros de Datos en los que se procesan los sistemas informáticos, se encuentran certificados en el nivel III de la norma ICREA emitida por International Computer Room Experts Association CREA, por lo que cuentan con las medidas de seguridad física que aseguran que la información se encuentra plenamente resguardada.
- **Revisar la configuración de seguridad del software y hardware.** La Dirección de Informática cuenta con procedimientos y controles para asegurar la administración del software y hardware instalado en la plataforma tecnológica de la Institución. Asimismo, se cuenta con procedimientos de monitoreo en línea que permiten la identificación oportuna de eventos que pudieran constituir un riesgo a la misma. La Dirección de Seguridad de la Información participa en la validación del cumplimiento de las políticas de seguridad establecidas, dentro de los



procedimientos correspondientes para el software o hardware de la Institución o su contratación por terceros

- **Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de Datos personales.** La Dirección de Informática, gestiona y administra las comunicaciones, la operación de TIC y los medios de almacenamiento de los sistemas informáticos de la Institución.

3.1. Borrado de la información contenida en los sistemas informáticos

Respecto de la información contenida en la plataforma tecnológica y en los sistemas informáticos institucionales, es necesario comentar que las áreas de negocio son las propietarias de la información y que la Dirección de Informática la tiene en custodia para ponerla disponible para su operación a través de los sistemas informáticos; por lo tanto, la información únicamente puede ser borrada por el personal designado para tal fin, mediante un rol definido para ello.

En relación con la información contenida en los medios de almacenamiento de respaldo, esta es gestionada mediante el sistema de administración de archivos electrónicos, el cual se ha desarrollado para dar cumplimiento a las medidas definidas en la Ley General de Archivos.

IX. Análisis de Riesgos

Lineamientos Generales

La Metodología utilizada es la aprobada por el Comité de Administración Integral de Riesgos (CAIR) a través de los diferentes Dictámenes Técnicos de Riesgo Operacional que la Subdirección de Riesgo Operacional aplica.

Fase I para la Identificación de Riesgos

- La Subdirección de Riesgo Operacional, en comunicación constante con las diferentes áreas tanto escrita como verbal, apoyó en la identificación de riesgos respecto de los tratamientos intensivos o relevantes de Datos personales.
- Los Responsables de los sistemas de Datos personales respondieron con calidad, integridad y oportunidad el cuestionario proporcionado y/o las preguntas realizadas durante los talleres a fin de identificar los riesgos inherentes.
- La clasificación de los riesgos está basada en la “Taxonomía de Riesgos de la CNBV”.

Fase II para la Medición de Riesgos

- Los Responsables de los sistemas de Datos personales evaluaron el riesgo identificado con base en los impactos* y su frecuencia a partir de lo siguiente:

ESCALA DE RIESGO	
1	MUY BAJO
2	BAJO
3	MEDIO
4	ALTO
5	MUY ALTO

En caso de materializarse el riesgo, ¿Cuál sería el posible Impacto Económico?

- 1) Sin impacto o hasta 60M MXN por evento
- 2) Más de 60M y hasta 100M MXN por evento
- 3) Más de 100M y hasta 300M MXN por evento
- 4) Más de 300M y hasta 600M MXN por evento
- 5) Más de 600M MXN por evento

¿Con qué Factibilidad / Frecuencia consideras que podría materialice el riesgo?

- 1) Podría ocurrir un evento en 5 años
- 2) Al menos un evento en 2-4 años
- 3) Al menos un evento, en los últimos 2 años
- 4) Entre 1 y 10 eventos al año
- 5) Más de 10 eventos al año

*Impactos = Σ (25% *Económico) + (25%*Legal) + (25%*Nivel de Servicio) + (25%*Reputacional)

Fase III para la Evaluación del Control

Los Responsables de los sistemas de Datos personales especificaron y describieron el control, el tipo de control, la frecuencia y el responsable de la ejecución del Punto de Control a fin de que el CISO tenga elementos suficientes para el análisis de brecha.

Resultado Perfil de Riesgo Tecnológico

De acuerdo a la Metodología que tiene desarrollada la Subdirección de Riesgo Operacional aplicable en los Dictámenes Técnicos de Riesgo Operacional y que se encuentra aprobada por el Comité de Administración Integral de Riesgos, se tiene lo siguiente:

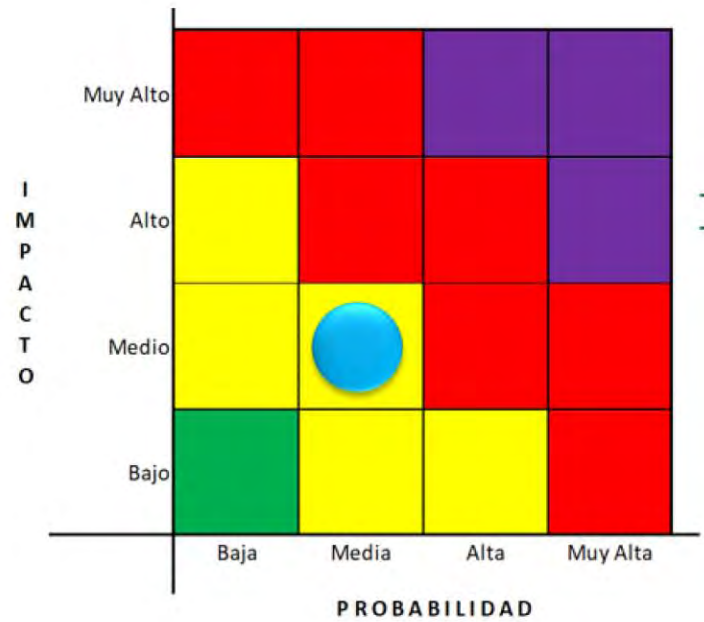
Se realizó la evaluación de cumplimiento de controles de riesgos relativos con el riesgo de "Seguridad de la información".

Riesgo	Nivel de Cumplimiento de Controles de Riesgos	Porcentaje de Cumplimiento de Controles de Riesgos
Seguridad de la información	Medio	66%

Con base en lo anterior, se evaluó la probabilidad de ocurrencia del riesgo, así como su impacto.

ID R	ID R	Riesgo	Probabilidad	Impacto Inherente	Impacto Residual	Riesgo Inherente	Riesgo Residual
2.1.1	A2-SA1-R3	Seguridad de la información	Bajo	Muy Alto	Alto	Alto	Medio

Finalmente, se ubica el riesgo en el mapa, en donde se aprecia que se encuentra dentro del nivel de tolerancia establecido en la Institución:



Resultado Análisis de Riesgo

ID.	Nombre del sistema / área con manejo de Datos personales	Riesgo / Amenaza tipo de riesgo operacional CNBV (nivel 3)	Factor de Riesgo	Clasificación de Factor	Control del Factor	Impacto Probabilidad de que Ocurra	Valor
1	E-Contract, E-File y Nafin Electrónico						
2	Dirección de Admón. de Mercados y Tesorería.						
3	Sociedad de Información Crediticia (Buró de Crédito)						
4	Dirección de Proyectos Sustentables						



ID.	Nombre del sistema / área con manejo de Datos personales	Riesgo / Amenaza tipo de riesgo operacional CNBV (nivel 3)	Factor de Riesgo	Clasificación de Factor	Control del Factor	Impacto Probabilidad de que Ocurra	Valor
5	TAS/MECA/SIDECA						
6	TAS/MECA/SIDECA						
7	SIGA						



ID.	Nombre del sistema / área con manejo de Datos personales	Riesgo / Amenaza tipo de riesgo operacional CNBV (nivel 3)	Factor de Riesgo	Clasificación de Factor	Control del Factor	Impacto Probabilidad de que Ocurra	Valor
8	TAS/MECA/SIDECA						
9	Dirección de Intermediarios Financieros y Microcréditos						
10	Dirección de Intermediarios Financieros y Microcréditos						



ID.	Nombre del sistema / área con manejo de Datos personales	Riesgo / Amenaza tipo de riesgo operacional CNBV (nivel 3)	Factor de Riesgo	Clasificación de Factor	Control del Factor	Impacto Probabilidad de que Ocurra	Valor
11	Cetes Directo						
12	Servicios en Sitio						
13	Dirección Fiduciaria						
14	Dirección Fiduciaria						



ID.	Nombre del sistema / área con manejo de Datos personales	Riesgo / Amenaza tipo de riesgo operacional CNBV (nivel 3)	Factor de Riesgo	Clasificación de Factor	Control del Factor	Impacto Probabilidad de que Ocurra	Valor
15	Información almacenada en SIRAC						
16	SIRYS (Sistema Integral de Recuperación y Seguimiento)						



ID.	Nombre del sistema / área con manejo de Datos personales	Riesgo / Amenaza tipo de riesgo operacional CNBV (nivel 3)	Factor de Riesgo	Clasificación de Factor	Control del Factor	Impacto Probabilidad de que Ocurra	Valor
17	SIAG (Administrado y reportado por la Dirección de Administración Crediticia)						
18	SISEC, SCC, CCBE						
19	Dirección de Financiamiento Corporativo						
20	Dirección General Adjunta Banca de Empresas						



ID.	Nombre del sistema / área con manejo de Datos personales	Riesgo / Amenaza tipo de riesgo operacional CNBV (nivel 3)	Factor de Riesgo	Clasificación de Factor	Control del Factor	Impacto Probabilidad de que Ocurra	Valor
21	SISTEMA DE GESTIÓN PROMOCIÓN Y VENTAS						
22	Dirección de Adquisiciones y Servicios						
23	Dirección de Adquisiciones y Servicios						



ID.	Nombre del sistema / área con manejo de Datos personales	Riesgo / Amenaza tipo de riesgo operacional CNBV (nivel 3)	Factor de Riesgo	Clasificación de Factor	Control del Factor	Impacto Probabilidad de que Ocurra	Valor
24	Sistema de Operaciones Relevantes e Inusuales SORI						
25	Dirección de Adquisiciones y Servicios						
26	CFD – Comprobantes Fiscales Digitales						
27	Sistema de Operaciones Relevantes e Inusuales SORI						
28	SIAL						



ID.	Nombre del sistema / área con manejo de Datos personales	Riesgo / Amenaza tipo de riesgo operacional CNBV (nivel 3)	Factor de Riesgo	Clasificación de Factor	Control del Factor	Impacto Probabilidad de que Ocurra	Valor
29	Dirección de Desarrollo Empresarial						
30	Secretaria del Consejo						
31	Secretaria del Consejo						
32	Secretaria del Consejo						



X. Análisis de Brecha.

Lineamientos Generales Análisis de Brecha

- La Metodología se realizó por la Dirección de Seguridad de la Información.
- La Metodología en sus tres fases fue aplicada por la Dirección de Seguridad de la Información en el ámbito de sus competencias al Responsable del sistema de Datos personales.
- Los Responsables, a través de la Metodología, identificaron las brechas de los sistemas de Datos personales y evaluaron el cumplimiento de los controles, en su caso, acciones suficientes para responder a éstos y asegurar de manera razonable el logro de los objetivos institucionales y el cumplimiento normativo, logro de los objetivos institucionales y el cumplimiento normativo.

Identificación de Brecha

- La Dirección de Seguridad de la Información, realizó la identificación de brecha a través de cuestionario de autoevaluación (Método de Soporte, Entrevista estructurada o semiestructurada y Técnica estructurada "What if"), apoyo en la identificación de riesgos respecto de los tratamientos intensivos o relevantes de Datos personales.
- Los Responsable de los sistemas de Datos personales respondieron con calidad, integridad y oportunidad el cuestionario proporcionado y/o las preguntas realizadas a fin de identificar las brechas.
- La clasificación de brechas está basada en la ISO/IEC 29100, que se ha convertido en la referencia de privacidad utilizada por la norma ISO 27001.

Medición de Brecha



Las áreas de la Institución que manejan Datos personales, evaluaron de brechas identificado con base en el cumplimiento de los controles de tratamientos de Datos personales y del tiempo de atención:

Escala de Brechas	Atención
BAJO	A Largo Plazo "Más de 6 meses"
MEDIO	A Mediano Plazo "6 meses"
ALTO	A Corto Plazo "3 meses"
MUY ALTO	Inmediata "1 mes"

Para los Planes de Remediación

- Los Responsables a cargo de Datos personales especificaron y describieron el plan de remediación, el tipo de control, el periodo de atención y el responsable de la ejecución del Punto de Control a fin de que el CISO minimice la brecha.
- Considerando que, en caso de no poderse atender el plan de remediación en el periodo estimado, el dueño del proceso firma una carta de aceptación del riesgo.

Metodología

La metodología empleada en este análisis de Brechas se divide en las etapas que se presentan a continuación.

- Levantamiento de información: se recopila la información publicada que se relacione con el cumplimiento de los riesgos establecidos.
- Verificación de la información: Se entrevista al responsable para verificar la información recopilada y obtener más información.
- Identificación de Brechas: se analiza la información anterior buscando identificar las brechas existentes.
- Evaluación de situación actual: se califica de acuerdo a los riesgos identificados.



La evaluación considera la condición de acuerdo a la factibilidad de mitigar los riesgos. Para esto se utiliza el siguiente criterio de evaluación.

CLAVE	CRITERIO	DESCRIPCIÓN
A	LOGRADO	IMPLEMENTADO.
B	INCOMPLETO	IMPLEMENTADO PARCIALMENTE.
C	VIABLE	FALTA IMPLEMENTAR.
D	INVIABLE	NO ES VIABLE IMPLEMENTAR.

Categoría de Análisis de Brecha

Para la realización del análisis de brecha, se consideran las siguientes categorías:

Estado	Significado
No Cumple	No se lleva a cabo algún control en la gestión del activo.
Cumple Parcial	Las actividades existen, pero no se gestionan y/o no existe un proceso formal para realizarlas. Su éxito depende de la intuición y de tener personal de alta calidad.
Cumple	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.

Resultados de Análisis de Brecha

Identificador	Nombre del Sistema / área con manejo de Datos personales	IDA	Pregunta	Respuesta	Brecha %	Brecha
1	E-Contract, E-File y Nafin Electrónico	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
2	Dirección de Admón. de Mercados y Tesorería	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			



Identificador	Nombre del Sistema / área con manejo de Datos personales	IDA	Pregunta	Respuesta	Brecha %	Brecha
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
3	Sociedad de Información Crediticia (Buró de Crédito)	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
4	Dirección de Proyectos Sustentables	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			



Identificador	Nombre del Sistema / área con manejo de Datos personales	IDA	Pregunta	Respuesta	Brecha %	Brecha
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
5	TAS/MECA/SIDECA	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
6	TAS/MECA/SIDECA	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			



Identificador	Nombre del Sistema / área con manejo de Datos personales	IDA	Pregunta	Respuesta	Brecha %	Brecha
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
7	SIGA	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
8	TAS/MECA/SIDCA	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			



Identificador	Nombre del Sistema / área con manejo de Datos personales	IDA	Pregunta	Respuesta	Brecha %	Brecha
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
9	Dirección de Intermediarios Financieros y Microcrédito	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
10	Dirección de. Intermediarios Financieros y Microcrédito	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			



Identificador	Nombre del Sistema / área con manejo de Datos personales	IDA	Pregunta	Respuesta	Brecha %	Brecha
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
11	Cetes Directo	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
12	Servicios en Sitio	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			



Identificador	Nombre del Sistema / área con manejo de Datos personales	IDA	Pregunta	Respuesta	Brecha %	Brecha
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
13	Dirección Fiduciaria	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
14	Dirección Fiduciaria	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			



Identificador	Nombre del Sistema / área con manejo de Datos personales	IDA	Pregunta	Respuesta	Brecha %	Brecha
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
15	Información almacenada en SIRAC	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
16	SIRYS (Sistema Integral de Recuperación y Seguimiento)	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			



Identificador	Nombre del Sistema / área con manejo de Datos personales	IDA	Pregunta	Respuesta	Brecha %	Brecha
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
17	SIAG (Administrado y reportado por la Dirección de Administración Crediticia)	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
18	SISEC, SCC, CCBE	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			



Identificador	Nombre del Sistema / área con manejo de Datos personales	IDA	Pregunta	Respuesta	Brecha %	Brecha
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
19	Dirección de Financiamiento Corporativo	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
20	Dirección General Adjunta Banca de Empresas	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			



Identificador	Nombre del Sistema / área con manejo de Datos personales	IDA	Pregunta	Respuesta	Brecha %	Brecha
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
21	SISTEMA DE GESTIÓN PROMOCIÓN Y VENTAS	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
22	Dirección de Adquisiciones y Servicios	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			



Identificador	Nombre del Sistema / área con manejo de Datos personales	IDA	Pregunta	Respuesta	Brecha %	Brecha
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
23	Dirección de Adquisiciones y Servicios	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
24	Sistema Integral de Operaciones Reportables (SIOR)	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			



Identificador	Nombre del Sistema / área con manejo de Datos personales	IDA	Pregunta	Respuesta	Brecha %	Brecha
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
25	Dirección de Adquisiciones y Servicios	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
26	CFD- Comprobantes Fiscales Digitales	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			



Identificador	Nombre del Sistema / área con manejo de Datos personales	IDA	Pregunta	Respuesta	Brecha %	Brecha
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
27	Sistema de Operaciones Relevantes e Inusuales SORI	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
28	SIAL	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			



Identificador	Nombre del Sistema / área con manejo de Datos personales	IDA	Pregunta	Respuesta	Brecha %	Brecha
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
29	Dirección de Desarrollo Empresarial y Asist. Técnica	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
30	Secretaría del Consejo	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			



Identificador	Nombre del Sistema / área con manejo de Datos personales	IDA	Pregunta	Respuesta	Brecha %	Brecha
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
31	Secretaria del Consejo	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			
32	Secretaria del Consejo	1	¿En tu área existen mecanismo para instruir al personal en el manejo de información de carácter personal?			
		2	¿Hay un responsable de privacidad de Datos personales en la el área?			
		3	¿Son los usuarios responsables conocedores de la información de carácter personal que es recopilado, procesado y almacenados en el área?			



Identificador	Nombre del Sistema / área con manejo de Datos personales	IDA	Pregunta	Respuesta	Brecha %	Brecha
		4	¿Se cuenta con controles de acceso a información de carácter personal?			
		5	¿Se conocen el nivel de acceso y roles (del personal del área) que tienen acceso a activos de información personal?			



XI. Plan de Trabajo.

A fin de implementar las medidas de seguridad faltantes, resultado del análisis de brecha realizado a continuación se lista el plan de trabajo, priorizando la atención de estas de acuerdo al nivel de atención resultado del análisis realizado.

ID	Nombre del Sistema / área con manejo de Datos personales	Brecha	Atención	Acciones de remediación
1	E-Contract, E-File y Nafin Electrónico			
2	Dirección de Admón. de Mercados y Tesorería			
3	Sociedad de Información Crediticia (Buró de Crédito)			
4	Dirección de Proyectos Sustentables			
5	TAS/MECA/SIDECA			
6	TAS/MECA/SIDECA			
7	SIGA			
8	TAS/MECA/SIDECA			



ID	Nombre del Sistema / área con manejo de Datos personales	Brecha	Atención	Acciones de remediación
9	Dirección de Intermediarios Financieros y Microcrédito			
10	Dirección de. Intermediarios Financieros y Microcrédito			
11	Cetes directo			
12	Servicios en Sitio			
13	Dirección Fiduciaria			
14	Dirección. Fiduciaria			
15	Información almacenada en SIRAC			
16	SIRYS (Sistema Integral de Recuperación y Seguimiento)			
17	SIAG (Administrado y reportado por la Dirección de Administración Crediticia)			
18	SISEC, SCC, CCBE			



ID	Nombre del Sistema / área con manejo de Datos personales	Brecha	Atención	Acciones de remediación
19	Dirección de Financiamiento Corporativo			
20	Dirección General Adjunta Banca de Empresas			
21	SISTEMA DE GESTIÓN PROMOCIÓN Y VENTAS			
22	Dirección de Adquisiciones y Servicios			
23	Dirección de Adquisiciones y Servicios			
24	Sistema Integral de Operaciones Reportables (SIOR)			
25	Dirección de Adquisiciones y Servicios			
26	CFD- Comprobantes Fiscales Digitales			
27	Sistema de Operaciones Relevantes e Inusuales SORI			
28	SIAL			



ID	Nombre del Sistema / área con manejo de Datos personales	Brecha	Atención	Acciones de remediación
29	Dirección de Desarrollo Empresarial y Asist. Técnica			
30	Secretaría del Consejo			
31	Secretaría del Consejo			
32	Secretaría del Consejo			

XII. Mecanismos de Monitoreo y Revisión de las medidas de seguridad.

Identificador	Nombre del Sistema / área con manejo de Datos personales	Medidas de Seguridad Actuales	Brecha
1	E-Contract, E-File y Nafin Electrónico		
2	Dirección de Admón. de Mercados y Tesorería		
3	Sociedad de Información Crediticia (Buró de Crédito)		
4	Dirección de Proyectos Sustentables		

Identificador	Nombre del Sistema / área con manejo de Datos personales	Medidas de Seguridad Actuales	Brecha
5	TAS/MECA/SIDCA		
6	TAS/MECA/SIDCA		
7	SIGA		
8	TAS/MECA/SIDCA		
9	Dirección de Intermediarios Financieros y Microcrédito		
10	Dirección de Intermediarios Financieros y Microcrédito		
11	Cetes directo		
12	Servicios en Sitio		
13	Dirección Fiduciaria		
14	Dirección Fiduciaria		
15	Información almacenada en SIRAC		
16	SIRYS (Sistema Integral de Recuperación y Seguimiento)		
17	SIAG (Administrado y reportado por la Dirección de Administración Crediticia)		
18	SISEC, SCC, CCBE		

Identificador	Nombre del Sistema / área con manejo de Datos personales	Medidas de Seguridad Actuales	Brecha
19	Dirección de Financiamiento Corporativo		
20	Dirección General Adjunta Banca de Empresas		
21	SISTEMA DE GESTIÓN PROMOCIÓN Y VENTAS		
22	Dirección de Adquisiciones y Servicios		
23	Dirección de Adquisiciones y Servicios		
24	Sistema Integral de Operaciones Reportables (SIOR)		
25	Dirección de Adquisiciones y Servicios		
26	CFD- Comprobantes Fiscales Digitales		
27	Sistema de Operaciones Relevantes e Inusuales SORI		
28	SIAL		
29	Dirección de Desarrollo Empresarial y Asist. Técnica		
30	Secretaria del Consejo		
31	Secretaria del Consejo		
32	Secretaria del Consejo		



XIII. Programa General de Capacitación.

Entre las obligaciones de NAFIN, se encuentra la de proporcionar capacitación continua y especializada al personal que forma parte del Comité y la Unidad de Transparencia.

A su vez, el Comité de Transparencia tiene entre sus atribuciones en materia de protección de Datos personales, establecer programas de capacitación y actualización para los servidores públicos de la Institución.

Derivado de lo anterior, la Unidad de Transparencia presenta al Comité de Transparencia en el mes de febrero de cada año, el Programa Anual de Capacitación, con el propósito de capacitar en materia de transparencia, acceso a la información, accesibilidad y protección de Datos personales, a los servidores públicos de la Institución cuyas actividades tienen relación directa con estos temas, sin perjuicio de otras actividades de capacitación interna en relación con temas específicos que se coordinan con la Dirección de Recursos Humanos y Calidad de NAFIN. Se adjunta como **Anexo 5** el Plan Anual de Capacitación para 2020.

Dichos Programas se sustentan en las acciones de capacitación y programa que propone el INAI para impartir cada año.

Asimismo, el Comité de Transparencia tiene la facultad para diseñar y aplicar diferentes niveles de capacitación del personal de NAFIN, dependiendo de sus roles y responsabilidades respecto del tratamiento de los Datos personales, según la detección de necesidades de las áreas.

Cabe destacar que, como parte del Programa General de Capacitación, en 2019, la Unidad de Transparencia, en coordinación con la Dirección de Recursos Humanos y Calidad, convocaron a todo el personal de la Institución para realizar la capacitación en los siguientes cursos: i) “Introducción a la Ley Federal de Transparencia y Acceso a la Información Pública” y ii) “Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados”. Al cierre de 2019, se logró capacitar a **439** funcionarios y **420** empleados. Derivado de lo anterior, mediante oficio INAI/RMC/85/2019 de fecha 18 de diciembre de 2019, el Instituto Nacional de Transparencia, Acceso a la Información y



Protección de Datos Personales notificó a NAFIN que se hizo acreedor al **Reconocimiento de Institución 100% capacitada** que otorga ese Instituto.

Para el año 2020, y también como parte del Programa General de Capacitación, NAFIN buscará obtener el Refrendo correspondiente ante el INAI.

XIV. Actualizaciones.

Conforme a lo previsto en el artículo 36 de la LGPDPPSO, el Documento de Seguridad se deberá actualizar cuando ocurra alguno de los siguientes eventos:

- Se produzcan modificaciones sustanciales al tratamiento de Datos personales que deriven en un cambio en el nivel de riesgo;
- Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
- Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y
- Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

En caso de que no ocurra ninguno de los eventos antes mencionados, la revisión y en su caso actualización del presente Documento de Seguridad será cada dos años, contados a partir de la aprobación del Comité de Transparencia del presente Documento.

Cada vez que ocurra una actualización, el Documento de Seguridad deberá ser sometido nuevamente para aprobación del Comité de Transparencia.



XV. Elaborado por

El presente documento fue elaborado en colaboración por las siguientes áreas de NAFIN.

Act. Aurora Cbeta Moreno Cortés
Directora Administración de Riesgos

L.C. Martha Lucia Contreras Gomez
Directora Adquisiciones y Servicios

Lic. Cynthia Medina Chapa
Directora Normatividad Gubernamental

Lic. Ricardo Jimenez Vargas
Director de Informática

Ing. José Antonio Martínez Sánchez
Oficial en Jefe de Seguridad de la Información

