FIFOMI
FIDEICOMISO DE FOMENTO MINERO

Informe de la Auditoría en materia Informática 2019

Noviembre, 2019

Índice de abreviaturas utilizadas

CNBV	Comisión Nacional Bancaria y de Valores
GESI	Grupo Estratégico de Seguridad de la Información
Disposiciones	Disposiciones de carácter general aplicables a los organismos de fomento y entidades de fomento
MAAGTICSI	Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información
GRP	Planificación de Recursos del Gobierno (Government Resource Planning)
CRM	Gestión de la relación con el cliente (Customer Relationship Management)
EDN	Estrategia digital nacional en materia de tecnologías de la información y comunicaciones y en la seguridad de la información
FIFOMI; Fideicomiso	Fideicomiso de Fomento Minero
TI	Tecnologías de la Información
SAP	Sistemas, Aplicaciones y Productos (Systems, Applications, Products in Data Processing)
SAP BASIS	Controles Generales de la Aplicación (Seguridad de la Información de la Aplicación)

Índice

Introducción

El objetivo del servicio de Auditoría en Materia Informática de los Ejercicios 2018 - 2019 definidos por el área de Auditoría Interna del Fideicomiso de Fomento Minero (FIFOMI), es identificar brechas de control en materia de sistemas informáticos y cumplir con las obligaciones que se encuentran descritas en las Disposiciones de carácter general aplicables a los organismos de fomento y entidades de fomento (Disposiciones) establecidas en el *artículo 166 fracciones III y IV.*

El servicio se desarrolla con base en nuestra metodología de revisión en donde se contemplan 3 fases principales: Exploración y Planteamiento, Supervisión y Ejecución, y Conclusiones y Cierre de Auditoría.
Para la exploración y planteamiento se basó en prácticas genéricas de administración de proyectos, donde se revisa el estado actual de la institución en conjunto con los reportes de auditoría entregados anteriormente y con esto se realiza un cronograma de trabajo. Para la supervisión y ejecución se elaboran los controles del sistema SAP (GRP/CRM), basados en las mejoras prácticas, así mismo, en conformidad con las Disposiciones emitidas por la Comisión Nacional Bancaria y de Valores (CNBV), la utilización de las mejores prácticas del Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGTICSI) publicado en el DOF de fecha 08-05-2014 y su última reforma el 23-07-2018, así como el Manual de Auditoría Interna del FIFOMI, , aprobado por el H. Comité de Auditoría el 29 de mayo según acuerdo CA/29MAY18.

Para la gestión y control de las actividades con la que se llevó acabo la auditoría, se utilizaron las herramientas Jira y Confluence, que han fungido como repositorio de documentación y tablero de control para llevar el cronograma de actividades donde se refieren las etapas comentadas anteriormente, descritas en la sección “procedimientos empleados para efectuar la revisión y evaluación” de este informe.

Antecedentes; fundamento legal y normativo

El FIFOMI es una entidad paraestatal, cuya cabeza de sector es la Secretaría de Economía, a la vez que forma parte del Sistema Bancario Mexicano, debido a que una de sus actividades preponderantes es otorgar financiamiento, por lo que su regulación y supervisión corresponde a la CNBV.

La CNBV establece en las Disposiciones, publicadas en el Diario Oficial de la Federación el 1 de diciembre de 2014 y sus diversas modificaciones, las funciones que, en materia de informática, está obligado a realizar el FIFOMI, en apego al contenido del artículo 166 fracciones III y IV.

Artículos 166.- El área de Auditoría Interna tendrá, entre otras, las funciones siguientes:

- *Fracción III.- Verificar que los sistemas informáticos, incluyendo los contables, operaciones de Cartera Crediticia, con valores o de cualquier otro tipo, cuenten con mecanismos para preservar la integridad, confidencialidad y disponibilidad de la información, que eviten su alteración y cumplan con los objetivos para los cuales fueron implementados o diseñados. Asimismo, vigilar dichos sistemas a fin de identificar fallas potenciales y verificar que estos generen información suficiente, consistente y que fluya adecuadamente.*
  En todo caso, deberá revisarse que el Organismo de Fomento o Entidad de Fomento cuente con planes de contingencia y medidas necesarias para evitar pérdidas de información, así como para, en su caso, su recuperación o rescate.
- *Fracción IV.- Cerciorarse de la calidad, suficiencia y oportunidad de la información financiera, así como, que sea confiable para la adecuada toma de decisiones, y tal información se proporcione en forma correcta y oportuna a las autoridades competentes.*

Adicionalmente, el FIFOMI, como parte de la Administración Pública Federal, da cumplimiento a las Disposiciones para la Estrategia Digital Nacional (EDN), en Materia de Tecnologías de Información y Comunicaciones, y en la Seguridad de la Información (MAAGTICSI), emitido por la Secretaría de la Función Pública.

Plan de Acción

Periodo de la revisión

El periodo de revisión de la auditoría en materia Informática comprenderá de octubre de 2018 a septiembre de 2019.

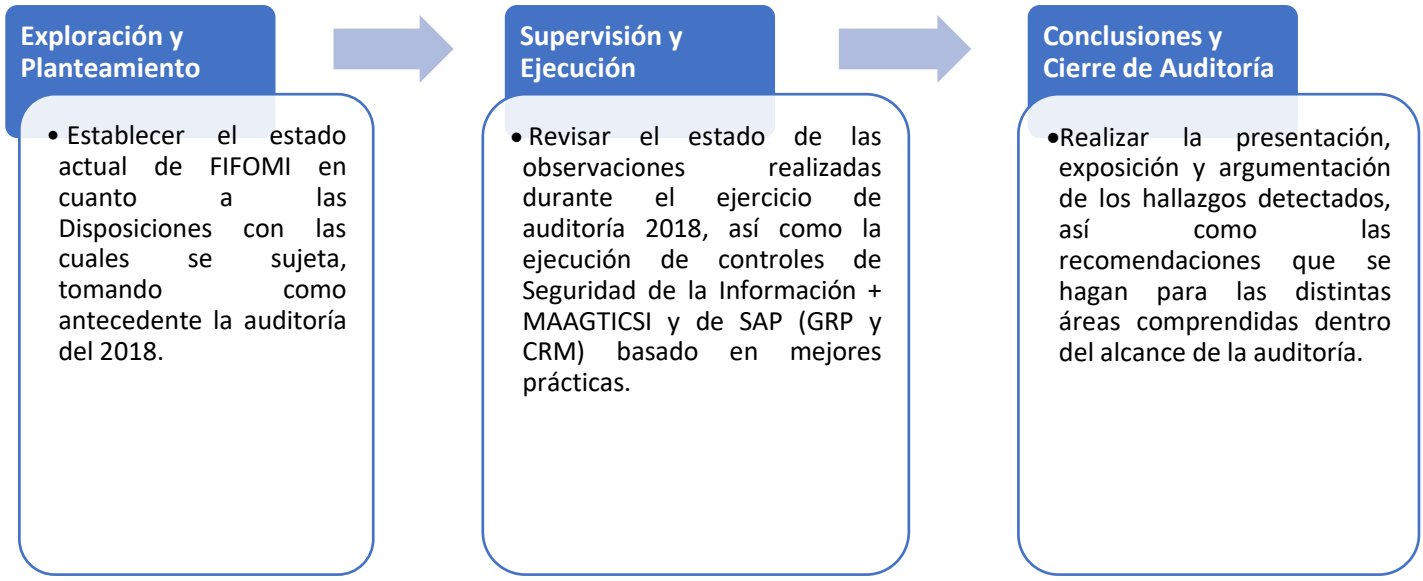
Objetivo de la revisión

Verificar que los sistemas informáticos, cuenten con mecanismos para preservar la integridad, confidencialidad y disponibilidad de la información, que eviten su alteración y cumplan con los objetivos para los cuales fueron implementados o diseñados. Así mismo, vigilar dichos sistemas a fin de identificar fallas potenciales y verificar que estos generen información suficiente, consistente y que fluya adecuadamente. Asimismo, que se cuente con planes de contingencia y medidas necesarias para evitar pérdidas de información, en su caso, su recuperación o rescate, y cerciorarse de la calidad, suficiencia y oportunidad de la información financiera, de tal manera que sea confiable para la adecuada toma de decisiones, y tal información se proporcione en forma correcta y oportuna a las autoridades competentes, sin soslayar lo relativo al riesgo tecnológico, de conformidad con lo establecido en el *artículo 166, fracciones III y IV, de las Disposiciones, emitidas por la CNBV, publicadas en el Diario Oficial de La Federación el 1 de diciembre de 2014*, y sus diversas modificaciones.

Alcance de la revisión y la evaluación

Llevar a cabo una revisión para evaluar y presentar un diagnóstico general de todo el entorno tecnológico del FIFOMI, que incluya los servicios tercerizados (la plataforma operativa de SAP se encuentra en un centro de datos tercerizado) y al personal de la Gerencia de Informática para determinar si la plataforma y sistema de operación central (SAP-GRP-CRM), cuenta con los mecanismos adecuados para preservar la integridad, confidencialidad y disponibilidad de la información, a la vez que permita identificar, en su caso, posibles fallas y proponer soluciones de remediación. La revisión deberá contemplar la ejecución de pruebas funcionales y técnicas, (detectar las brechas de seguridad sobre las implementaciones de control de acceso en cada módulo de SAP, como en los sistemas satelitales propietarios de SAP, cada hallazgo encontrado deberá ser debidamente reportado, así como la causa y la remediación propuesta para cada uno), que garanticen que se cumplen con los estándares y mejores prácticas de acuerdo a lo establecido en las Disposiciones y Marcos Normativos aplicables.

A continuación, se exponen los objetivos de las etapas con la que se llevó a cabo la evaluación:



Metodologías aplicadas, marco de referencia, normas y procedimientos

La metodología de trabajo que llevó a cabo SYE Software para el cumplimiento del objetivo establecido en conjunto con el FIFOMI se divide en 3 etapas principales; para la revisión de los controles del sistema SAP GRP/CRM, se basó en las mejores prácticas de SAP incluidas en nuestro método de revisión, así mismo, de conformidad a las Disposiciones emitidas por la CNBV; y la utilización de las mejores prácticas del MAAGTICSI, así como el Manual de Auditoría interna de FIFOMI.

La planeación y control del presente proyecto se llevó a cabo bajo los estándares de FIFOMI.

Exploración y Planteamiento

Como primera etapa se realizó la recopilación de información, lo cual permitió identificar los controles a verificar, así como los documentos necesarios que justificaron y sustentaron la revisión.

Las actividades a realizar en la ***Exploración*** fueron las siguientes:

- Definición de requerimientos de información
- Solicitud formal de documentación relacionada
- Clasificación de información
- Identificación de responsables técnicos de los servicios
- Identificación de responsables funcionales

- Identificación de áreas involucradas

Las actividades realizadas en el ***Planteamiento*** fueron las siguientes:

- Integración de modelos normativos
- Entendimiento para el seguimiento de los hallazgos identificados en la auditoría 2018
- Diseño y construcción de matrices de verificación
- Generación de agenda de visita con responsables técnicos
- Generación de agenda de visita con responsables funcionales
- Integración Documental

Supervisión y Ejecución

Durante esta segunda etapa se ejecutaron las actividades de seguimiento a los hallazgos detectados durante la auditoría 2018, así como las evaluaciones técnicas necesarias a los servicios de TI contratados por el periodo que comprende la auditoría 2019 dentro del presente informe. Esta actividad se realizó con las matrices diseñadas previamente, en el nivel de cumplimiento de seguridad y normatividad de cada uno.

En lo correspondiente a la ***Supervisión*** se realizaron las siguientes actividades:

- Seguimiento de hallazgos de la auditoría 2018
- Ejecución de actividades de validación de hallazgos 2018
- Creación de cédulas de seguimiento
- Elaboración de informes preliminares

Para lo correspondiente a las actividades de ***Ejecución*** realizadas en esta etapa se desprenden las siguientes:

- Ejecución de las matrices de verificación (evaluación técnica)
- Pruebas de Funcionales
- Pruebas Técnicas
- Pruebas de Seguridad de la Información
- Pruebas de Acceso a la Información
- Pruebas de Segregación de Funciones
- Verificación Documental
- Elaboración de informes preliminares

Durante esta etapa se solicitó evidencia documental a los responsables técnicos y funcionales evaluados.

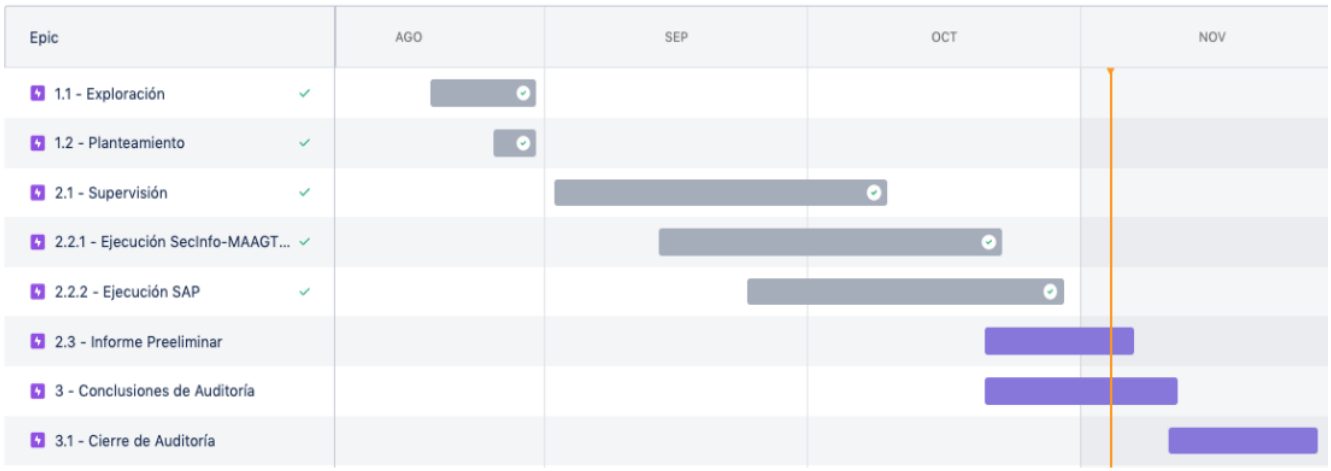
Cierre y Conclusiones

Durante la última etapa del proyecto, se llevó a cabo un análisis de los resultados obtenidos de las evaluaciones técnicas realizadas. Se generaron los informes preliminares y finales, así como la documentación de las cédulas de trabajo definidos como entregables de este proyecto.

Las actividades realizar en esta etapa fueron las siguientes:

- Análisis de resultados de la ejecución de las matrices de verificación
- Análisis de resultados de verificación documental (evidencias recabadas)
- Análisis general de resultados obtenidos
- Generación de Informe Preliminar
- Junta aclaración con las áreas auditadas para comentarios
- Generación de Informe Final con comentarios y aclaraciones de las áreas auditadas
- Reunión de cierre con el área de Auditoría Interna.

A continuación, se muestra la hoja de ruta en donde están marcadas las 3 etapas mencionadas, divididas en subetapas consideradas anteriormente.



Procedimientos

Con la finalidad de garantizar la adecuada revisión y evaluación se realizaron el equipo de trabajo se apoyó en la ejecución y prueba de las siguientes matrices de trabajo:

- **Matriz de Controles Seguridad de la Información y MAAGTICSI**: Consta en una matriz de casos de prueba y controles que garantizan el apego a las buenas prácticas, derivado de la evaluación de cumplimiento y de acuerdo a lo establecido en el *artículo 166 fracciones III y IV; de las Disposiciones*. Así, como parte de la Administración Pública Federal, da cumplimiento a las Disposiciones para la Estrategia Digital Nacional, en Materia de Tecnologías de Información y Comunicaciones, y en la Seguridad de la Información (MAAGTICSI), emitido por la Secretaría de la Función Pública.

- **Matriz de Controles SAP**: Consta de un conjunto de casos de prueba y controles de configuración y accesos (BASIS y Funcionales), organizados dentro de una matriz de prueba, el cual está basada en las mejores prácticas de SAP, de acuerdo a lo establecido en el *artículo 166 fracciones III y IV*, en conformidad a las Disposiciones, publicadas en el Diario Oficial de la Federación el 01 de diciembre de 2014, y sus diversas modificaciones.

Resultado final del seguimiento de las acciones y recomendaciones de la auditoría anterior (2018)

Derivado de los hallazgos detectados durante la auditoria en materia Informática 2018, la Gerencia de Informática del FIFOMI, definió un conjunto de acciones con el objetivo de remediar las observaciones y recomendaciones generadas durante dicha auditoría, para las cuales se corroboraron los avances e identificaron planes de trabajo para el seguimiento y cumplimiento definitivo de las mismas.

Como seguimiento de los resultados se identificó la creación del Grupo Estratégico de Seguridad de la Información (GESI) mismo que ha venido sesionando desde mediados del presente año. Dicho grupo interdisciplinario está conformado por miembros de distintas gerencias de la organización y que entre las principales funciones y avances en su conformación sobresalen los siguientes:

- Apoyo con la resolución de hallazgos de seguridad de la información y lo correspondiente a lo establecido dentro de MAAGTICSI.
- Desarrollo, revisión e implementación de políticas, procedimientos y formatos que facilitan la adopción de buenas prácticas en materia de seguridad de la información.
- Seguimiento a los planes de continuidad de negocio apoyando el desarrollo y pruebas anuales requeridas por la normatividad aplicable.

A su vez la Gerencia de Informática, con el interés de solventar y contribuir con la integridad del FIFOMI, ha llevado a cabo actividades que apoyaron a solventar y disminuir los riesgos inherentes propios del negocio, los cuales son:

- Monitoreo constante a través de reportes a las actividades críticas de seguridad de la información.
- Validación y monitoreo de usuarios con relación a la segregación de roles y funciones con el fin de garantizar que los permisos sean los adecuados para realizar sus funciones sin significar un riesgo alto en operaciones del negocio.
- Mantener las configuraciones adecuadas de los sistemas de acuerdo con las normas y políticas propias del Fideicomiso.
- Implementación y monitoreo de softwares que ayudan a mantener controles de seguridad tales como firewalls, análisis de vulnerabilidades, antivirus entre otros.

Resultados finales derivados de la revisión y pruebas efectuadas a los procesos, y controles (2019)

Derivado de la evaluación de cumplimiento y de acuerdo a lo establecido en el *artículo 166 fracciones II y III de las Disposiciones*, publicadas en el Diario Oficial de la Federación, en fecha 1 de diciembre de 2014, y sus diversa modificaciones, así como el MAAGTICSI, se llevó a cabo la revisión de los mecanismos de control, así como la verificación de los sistemas informáticos a fin de preservar la integridad, confidencialidad y disponibilidad de la información, a efecto de evitar su alteración y cumplir con los objetivos, para los cuales fueron implementados, además de identificar las fallas potenciales de los sistemas.

Se verificó que los procesos de negocio, de acuerdo con la arquitectura funcional actual del SAP-GRP/CRM, se encuentren debidamente identificados y controlados (integridad de los procesos de negocio). Durante la auditoría se llevaron a cabo entrevistas de entendimiento con los distintos enlaces de las áreas del negocio, donde se identificaron los diferentes autores y flujos de información que conforman cada uno de los procesos, así como el registro de la información y su interacción con el sistema SAP.

De acuerdo con el organigrama 2019 de FIFOMI, las áreas recorridas fueron:

- Gerencia de Informática
- Gerencia de Presupuesto y Contabilidad
- Gerencia de Cartera
- Gerencia de Cumplimiento Normativo
- Subdirección Jurídica
- Gerencia de Recursos Materiales
- Gerencia de Tesorería
- Gerencia de Recursos Humanos
- Gerencia de Comunicación y Difusión
- Subdirección de Riesgos
- Subdirección Técnica
- Gerencia de Operación
- Gerencia de Seguimiento y Evaluación
- Gerencia de Crédito y Contratación

Con base en el recorrido y entendimiento a través de las entrevistas realizadas a las diferentes gerencias, se identificó que el sistema utilizado por el FIFOMI para sus procesos de negocio es SAP (CRM-GRP), a la vez que se verificó que la estructura del sistema SAP consiste de la siguiente manera:

Módulos del ambiente CRM:
- CML – Gestión Crediticia

Módulos del ambiente GRP:
- ATR - Activo Fijo
- GL - Contabilidad
- PUR - Compras
- AP - Cuentas por Pagar

- AR - Cuentas por Cobrar
- PY - Nómina
- MM - Inventarios
- TR - Tesorería
- TV - Gestión de Viajes
- TRM - Tesorería Avanzada
- CFM - Gestión de Riesgos
- CML - Gestión Crediticia
- CMS - Control de Garantía
- CO - Costos
- EP - Enterprise Portal
- FM - Presupuestos
- PA - Administración de Personal
- PD - Desarrollo de Personal

Derivado del entendimiento y ejecución de las matrices mencionadas en la sección ***Procedimientos*** del presente informe, se desprenden a manera de resumen los siguientes resultados:

a) Seguridad de la Información + MAAGTICSI

- En concordancia con el MAAGTICSI dentro de las políticas y disposiciones de la EDN, el trabajo realizado fue:
    - **Revisión de controles para los 9 procesos base del MAAGTICSI**: Se elaboró la "Matriz de Verificación de Seguridad de la Información" con 40 puntos de revisión, con los cuales se pudo verificar el nivel de apego que la Gerencia de Informática y áreas de apoyo tienen con los 9 procesos definidos en el manual.

b) Controles Generales de SAP BASIS CRM y GRP

- Con fundamento en el *artículo 166 fracción III de las Disposiciones*, y con el fin de asegurar que los sistemas informáticos, incluyendo los contables, operacionales de cartera crediticia, con valores o de cualquier otro tipo, cuenten con mecanismos para preservar la integridad, confidencialidad y disponibilidad de la información, que eviten su alteración y cumplan con los objetivos para los cuales fueron implementados o diseñados, el trabajo realizado fue:
    - **Revisión de la seguridad de la aplicación:** Este control constó en la elaboración de matrices de pruebas para SAP-BASIS GRP y SAP-BASIS CRM. Estas matrices se encuentran contenidas ambas en el archivo "Matriz de Control FIFOMI 2019 - Basis GRP y CRM" las cuales se utilizaron para determinar los niveles adecuados de permisos y accesos que se tienen a transacciones sensibles (valores tipo 01-Creación o Activación, 02-Modificación, 06-Borrado, perfiles SAP_ALL, entre otros, con el fin de identificar los niveles de seguridad e integridad de los accesos al sistema), propias que deben pertenecer a un área especializada como en este caso se considera a la Gerencia de Informática del Fideicomiso de Fomento Minero.
    - **Gestión y configuración de la seguridad de la aplicación:** Con el diseño de las matrices de prueba SAP-BASIS GRP y SAP-BASIS CRM se integraron controles específicos para la validación de parámetros dentro de los ambientes productivos, configuración de contraseñas, gestión de cambios a través de transportes, entre otros.

c) Controles Funcionales y Accesos SAP

- *Con fundamento en el artículo 166 fracciones III y IV de las Disposiciones,* y con la finalidad de verificar que los sistemas informáticos, incluyendo los contables, operacionales de cartera crediticia, con valores o de cualquier otro tipo, cuenten con mecanismos para preservar la integridad, confidencialidad y disponibilidad de la información, incluyendo también la posibilidad de cerciorarse de la calidad, suficiencia y oportunidad de la información, así como que sea confiable para la adecuada toma de decisiones, y tal información se proporcione en forma correcta y oportuna a las autoridades competentes, el trabajo realizado fue:
    - **Revisión del sistema SAP a los controles Funcionales del FIFOMI:** Se diseñaron matrices de prueba para los 18 módulos funcionales de SAP GRP y CRM, así como pruebas de segregación de roles y accesos.

Resultados finales de las cédulas de hallazgos, recomendaciones y observaciones finales (2019).

De acuerdo con el alcance definido a lo largo de este documento se presenta a manera resumen los siguientes resultados:

a) Hallazgos remediados durante la auditoría

Derivado de las acciones y actividades descritas en las primeras secciones de este documento, se listan a continuación los hallazgos remediados por parte de la Gerencia de Informática y áreas involucradas, durante el curso de la presente auditoría:

Número	Tipo de Hallazgo	Descripción	Remediación
1.1, 1.3, 1.4, 1.5, 1.6, 1.7, 1.8, 1.10, 1.11, 1.12, 1.13	Observación	Se identificó 1 usuario funcional en el sistema SAP CRM con permisos que no deberían de contar de acuerdo con sus funciones y área para las transacciones: • SU01, SU02, SU10-SU12, SUGR, PFCG • SE37, SE80, SMOD • OAB4, SM36, SM37 • SM49, SM69 • STMS, SCTS, SE03, SE06 • SCC4 • SE38, SE80 • RZ10 • SE14 • SM59 • SM50, SM51, SM66, SM12 *Referencia documental: SAP-BAS-001-CRM, SAP-BAS-006-CRM, SAP-BAS-008-CRM, SAP-BAS-009-*	La Gerencia de Informática vía correo electrónico con fecha de 07 de noviembre de 2019 envió evidencia remediando la observación de este punto, donde explica que se cambió el tipo de usuario de Dialogo a Comunicación para evitar el acceso al SAP GUI y solo puedan ingresar a SAP vía WEB.

		CRM, SAP-BAS-011-CRM, SAP-BAS-013-CRM, SAP-BAS-014-CRM, SAP-BAS-017-CRM, SAP-BAS-018-CRM, SAP-BAS-019-CRM, SAP-BAS-020-CR.	

1.2	Observación	Se identificaron usuarios funcionales con permisos en SAP-CRM con los que no deberían de contar de acuerdo con sus funciones y área para las transacciones siguientes:
		
		• Para la transacción SU24:
		  ○ 4 usuarios son nuevos generados en el 2019.
		• Para la transacción SU25 y AUTH_SWITCH_OBJECTS
		  ○ 1 usuario es nuevo generado en el 2019.
		
		Referencia documental: SAP-BAS-003-CRM
			La Gerencia de Informática vía correo electrónico con fecha de 07 de noviembre de 2019 envió evidencia remediando la observación de este punto, donde explica que se cambió el tipo de usuario de Dialogo a Comunicación para evitar el acceso al SAP GUI y solo puedan ingresar a SAP vía WEB.

1.9	Observación	Se identificó 1 usuario - FQUIROGA nuevo generado en el año 2019 con permisos que de acuerdo con sus funciones y área no deberían de contar para la transacción: SE38 del SAP GRP *Referencia documental: SAP-BAS-014-GRP*	La Gerencia de Informática vía correo electrónico con fecha de 05 de noviembre de 2019 envió evidencia remediando la observación de este punto, donde se puede observar que se retiraron los permisos al usuario FQUIROGA.
2	Recomendación	Se realizó una consulta de los parámetros de uso de contraseñas para SAP CRM de acuerdo al plan de prueba. Se identificó que los parámetros *login/min_password_specials* y *login/min_password_uppercase* no se encuentran con valores según las reglas de FIFOMI con respecto a la política interna perfil, mismos que se encuentran en valor 0 cuando deberían ser por lo menos el valor 1. *Referencia documental: SAP-BAS-002-CRM*	La Gerencia de Informática en el archivo EvidenciaObservaciónSAP-BAS-002.docx, se puede observar que se realizó el ajuste a los parámetros identificados, a su nuevo valor de uno (1). Por lo que se puede determinar que la Recomendación ha sido atendida
3.1 y 3.2	Observación	Se ingresó a la Tabla T000 para validar la configuración del ambiente productivo, encontrando que se encuentra parametrizado para permitir cambios directos sin necesidad de pasar por un	La Gerencia de Informática, a través de los reportes de vista Mandantes para el *100 Productivo CRM* y *100 Productivo FIFOMI,* ha realizado la configuración para

		sistema de transporte para SAP CRM y GRP. *Referencia documental: SAP-BAS-012-CRM*	restringir el parámetro de Autorización para actualizar objetos validos a su valor 3 (Sin modificación a objetos Repository y Customazing), el parámetro de Modificación y transporte objetos específicos mandantes a su valor 2 (no se permiten modificaciones) y el parámetro de Protección de programa para copiar mandantes y herramienta a su valor 1 (No se puede sobrescribir)
4.1 y 4.2	Recomendación	Se identificaron 7 usuarios en el sistema SAP CRM y 4 usuarios en el sistema SAP GRP que nunca han accedido o no lo han hecho en los últimos 3 meses. *Referencia documental: SAP-BAS-016-CRM*	La Gerencia de Informática, mediante el archivo *Usuarios bloqueados Sistema SAP por falta de uso en periodo de 90 días.pdf*, confirma la remoción de accesos y permisos a usuarios que no han ingresado al sistema o que tienen un periodo de inactividad mayor a 90 días.
5	Recomendación	Se ingresó al Sistema SAP GRP al Módulo de Cuentas por Pagar y a través de la tabla LFA1 se observa que los siguientes proveedores tienen habilitado el campo "Recepción Alternativo de pago", lo cual permite cambiar a un proveedor alternativo para efectuar el pago durante el procesamiento de la factura. *Referencia documental: SAP-AP-004*	La Gerencia de Informática vía correo electrónico con fecha de 07 de noviembre de 2019 envió evidencia remediando la recomendación de este punto, donde explica que se validó con el personal de Presupuesto y Contabilidad quienes comentaron que, para el caso de los empleados, anteriormente se estaban utilizando para realizar como pago a proveedores, sin embargo, hoy día este proceso ya no se realiza. Para el caso de las seis empresas (morales y físicas) fue pedido y dado de alta de esta forma, quedando igual y para futuras operaciones con el proveedor.
6	Recomendación	Se ingresó al Sistema SAP GRP al Módulo de GL a través de la tabla SKA1 para validar que las cuentas marcadas para borrado se encuentren bloqueadas para	La Gerencia de Informática vía correo electrónico con fecha de 05 de noviembre de 2019 envió evidencia remediando la

		evitar se realicen movimientos contables en dichas cuentas. Para las cuentas contables dentro del Plan de Cuentas FIFOMI - 1000 se observó que 22 cuentas contables marcadas en el campo "Marcadas para borrado" no se encontraban marcadas en el campo "Bloqueadas para Posteo", lo que permite que dichas en dichas cuentas contables puedan realizarse movimientos contables. *Referencia documental: SAP-GL-003*	recomendación de este punto, donde explica que el personal de Presupuesto y Contabilidad realizó el bloqueo de las cuentas identificadas que fueron marcadas para borrado. Así mismo, se comenta que ya fueron validadas y revisadas por parte de la Gerencia de Informática, se envió evidencia con la imagen del cambio. Ver Archivo Remediación Cédula SAP-GL-003.
7	Recomendación	El sistema SAP GRP está configurado para prevenir la afectación en diferentes periodos contables. Para validar dicha configuración se ingresó a la Tabla V_T001B y se observó que, a la fecha de la revisión, todos los periodos están abiertos para modificar en periodos contables diferentes al actual. Es decir, el único periodo contable abierto debería ser el 10 - octubre, sin embargo, los 16 periodos se encuentran abiertos, lo que permite que cualquier movimiento contable pueda aplicarse en cualquier fecha. *Referencia documental: SAP-GL-004*	La Gerencia de Informática vía correo electrónico con fecha de 04 de noviembre de 2019 envió evidencia remediando la recomendación de este punto, donde explica que el personal de Presupuesto y Contabilidad realizó la modificación de los periodos contables, dejando abiertos los periodos 10-octubre y 11-noviembre (fecha actual de la auditoría).

b) Hallazgos con plan de acción identificados durante la auditoría

Para lo correspondiente a los resultados del presente trabajo de auditoría en materia informática 2019, listamos a continuación los hallazgos que quedaron en proceso con plan de acción del cual la Gerencia de Informática son los responsables de su implementación y seguimiento:

Número	Tipo de Hallazgo	Descripción	Plan de acción
8	Recomendación	Derivado de la revisión del documento "IM957333 - Reporte Utilización Capacidad de VM.pdf", donde solamente se describe la medición de espacio que se está utilizando actualmente de cada uno de los servidores que e encuentran en el centro de datos (TRIARA), se determina que actualmente FIFOMI no cuenta con un programa de capacidad de su infraestructura y su monitoreo. 1. El MAAGTICSI solicita la elaboración del programa de capacidad, así como su monitoreo de acuerdo con lo descrito en la actividad ADS, en sus factores críticos, por ejemplo: a) Determinar el balance entre la demanda de los servicios de TIC y la capacidad de la infraestructura de TIC, para conocer la suficiencia de cada uno de sus componentes, b) Establecer escenarios para las diversas proyecciones de demanda de los servicios de TIC y considerar, de ser el caso, opciones respecto de los niveles y metas de servicio acordados, señalando invariablemente los riesgos que cada escenario conlleve. c) Determinar los componentes de la infraestructura de TIC que son necesarios para cumplir con los requerimientos de desempeño y disponibilidad de los servicios de TIC, tanto de los existentes como de los proyectados. d) Identificar los activos de TIC que requieren actualizarse, mejorarse o elaborar el programa de capacidad y realizar su monitoreo al menos trimestralmente apegados a lo descrito en la Actividad ADS 3	La Gerencia de Informática indicó que dentro del programa de consolidación de contratos para el año 2020 por parte de las Secretarías de Economía, se incluirá dentro del Proyecto “Suministro de equipo de cómputo”, mismo que en el alcance se integra el componente L. Monitoreo, de acuerdo a la evidencia proporcionada “Reporte de cartera de iniciativa y proyectos.pdf”; por lo que al cierre de la auditoría (noviembre 2019) no se cuenta con una fecha tentativa para el cumplimiento de este punto.

		del MAAGTICSI. inclusive, sustituirse, así como las fechas propuestas y los costos estimados en cada caso. 2. Verificar, al menos trimestralmente, la capacidad y rendimiento de la infraestructura de TIC, para determinar si es suficiente para prestar los servicios de TIC con los niveles de servicio acordados, etc. (*Disposiciones de Carácter General Aplicables a los Organismos de Fomento y Entidades de Fomento, artículo 169, fracción V, inciso f). Proceso ADS, Actividad 3 del MAAGTICSI.)* *Referencia documental: SI-34*	
9	Observación	Actualmente el FIFOMI no cuenta con un repositorio de configuraciones, en el que se integren las soluciones tecnológicas y sus componentes, así como la información funcional y técnica de los mismos y la relativa a los diversos ambientes y arquitecturas tecnológicas, como elementos de configuración (CI), con la finalidad de facilitar su acceso cuando así se requiera para la operación de los procesos. (*Disposiciones de Carácter General Aplicables a los Organismos de Fomento y Entidades de Fomento, artículo 169, fracción VI. Proceso ACNF, todas sus actividades del MAAGTICSI)* *Referencia documental: SI-36*	La Gerencia de Informática indicó que durante el Programa de Seguridad de la Información que se realizará con apoyo del proveedor a quien se adjudicó la licitación IA-010K2O001-E112-2019, entregará un proyecto al área de auditoría interna del FIFOMI donde describirá el proceso de integración de las soluciones tecnológicas y sus componentes para la creación del repositorio de configuraciones, con el fin de llevar acabo un mejor manejo en la operación de sus procesos. **Fecha compromiso:** 15 enero 2020
10	Observación	Actualmente el FIFOMI no cuenta con la Directriz de Análisis de Riesgos, con el objetivo de identificar, clasificar y priorizar los riesgos para evaluar su impacto sobre los procesos y los servicios de la Institución, de manera que se obtengan las matrices de análisis de riesgos, mismas que actualmente no han sido elaboradas. (*Disposiciones de Carácter General Aplicables a los Organismos de Fomento y Entidades de*	La Gerencia de Informática indicó que durante el Programa de Seguridad de la Información que se realizará con apoyo del proveedor a quien se adjudicó la licitación IA-010K2O001-E112-2019, entregará un proyecto al área de auditoría interna del FIFOMI donde describirá el proceso de creación y plan de

		Fomento, artículo 166, fracción VIII. Proceso ASI, actividad 5 del MAAGTICSI.) *Referencia documental: SI-40*	implementación de la Directriz de Análisis de Riesgos que servirá para identificar, clasificar y priorizar los riesgos y evaluar el impacto en los procesos de la seguridad de la información. **Fecha compromiso:** 15 enero 2020
11	Recomendación	Derivado de la revisión de la información otorgada por la Gerencia de Informática y la Gerencia de Recursos Materiales, así como las entrevistas que se tuvieron con dichas áreas, se concluye que actualmente FIFOMI tiene implementados diferentes controles para el ingreso y salida de activos de información. Sin embargo, no se cuentan con políticas y procedimientos documentados que incluyan los controles que se practican hoy en día para el manejo (entradas y salidas) de los activos de información. (*Disposiciones de Carácter General Aplicables a los Organismos de Fomento y Entidades de Fomento, artículo 169, fracción VI, inciso e). Proceso ASI, Actividad 6, Factor Crítico 1 inciso d) del MAAGTICSI.)* *Referencia documental: SI-35*	La Gerencia de Informática indicó que durante el Programa de Seguridad de la Información que se realizará con apoyo del proveedor a quien se adjudicó la licitación IA-010K2O001-E112-2019, entregará al área de auditoría interna del FIFOMI la descripción y el plan de implementación de la política y su procedimiento que corresponde a las entradas y salidas de activos de información del Fideicomiso. **Fecha compromiso:** 15 enero 2020
12	Recomendación	No se encuentra autorizado el programa “Política de respaldo, recuperación y borrado seguro de la información”. Mismo que se espera sea aprobado por el GESI en la próxima sesión con fecha del 14-nov-2019. (*MAAGTICSI Proceso "ASI 6 Integrar al SGSI los controles mínimos de seguridad de la información." e) El borrado seguro de dispositivos de almacenamiento que por algún motivo necesiten ser reparados, reemplazados o asignados a otro usuario; y mantener evidencia auditable del proceso.)* *Referencia documental: SI-6*	La Gerencia de Informática indicó que durante el Programa de Seguridad de la Información que se realizará con apoyo del proveedor a quien se adjudicó la licitación IA-010K2O001-E112-2019, entregará al área de auditoría interna del FIFOMI el programa actualizado y fecha de autorización de la “Política de respaldo, recuperación y borrado seguro de la información” **Fecha compromiso:** 15 enero 2020

13	Recomendación	Derivado del recorrido del site, se realiza la recomendación de peinar, etiquetar y organizar el cableado estructurado de los equipos de comunicaciones que se encuentran en el rack, con el objetivo de mantener la seguridad de las conexiones de los equipos y continuidad de los servicios, una mejor identificación del cableado para que en caso de realizar algún cambio o incidente se realice de manera organizada e identificada. (*Disposiciones de Carácter General Aplicables a los Organismos de Fomento y Entidades de Fomento, artículo 169, fracción V, inciso f) y artículo 172, fracción V. Proceso AOP, Actividad 4, Factor Crítico 1 del MAAGTICSI)* *Referencia documental: SI-21*	La Gerencia de Informática indicó que dentro del programa de consolidación de contratos para el año 2020 por parte de las Secretarías de Economía, se incluirá dentro del Proyecto "Suministro de equipo de cómputo", mismo que en el alcance se integra el componente L. Monitoreo, de acuerdo a la evidencia proporcionada "Reporte de cartera de iniciativa y proyectos.pdf"; por lo que al cierre de la auditoría (noviembre 2019) no se cuenta con una fecha tentativa para el cumplimiento de este punto.
14	Recomendación	Conforme a la información revisada, se confirma que los documentos de Continuidad del Negocio se encuentran apegados a la normatividad aplicable. Sin embargo, es necesario que dicho plan cuente con pruebas y revisiones anuales para verificar la efectividad del plan y garantizar que se tomen en cuenta cambios o actualizaciones en los procesos de negocio, ya que los documentos se desarrollaron en septiembre 2018 y a la fecha de la auditoría no se ha realizado la actualización y pruebas anual. (*Disposiciones de Carácter General Aplicables a los Organismos de Fomento y Entidades de Fomento, artículo 161, fracción IV; artículo 163, fracción VI, inciso g), artículo 169, fracción I. y artículo 170, fracción VI, inciso e) y su anexo 42. Proceso ADS, Actividad 4 del MAAGTICSI.)* *Referencia documental: SI-35*	La Gerencia de Cumplimiento Normativo informó que las pruebas al Plan de Continuidad del Negocio (PCN) se llevaron a cabo el 20 de noviembre del 2019, conforme a lo acordado en la reunión del GESI, misma en la que se presentó el "2.- Programa de Difusión y Capacitación PCN aprobado GESI.xlsx", en el cual se describe el plan de trabajo con las actividades planeadas tanto para la capacitación y difusión del plan, como para las revisiones que se realizarán con la finalidad de la actualización de los 36 procedimientos. Se anexa el acta de la última sesión "Acta de la 4a sesión ordinaria del GESI.pdf". En seguimiento a los acuerdos y al programa mencionado anteriormente, la Gerencia de Cumplimiento Normativo, ha realizado diversas acciones de

			las cuales se presentan las siguientes evidencias: "1.- Atalait FIFOMI 201119 CONFIRMACION.pdf", "4.- Evidencia del envío de alertamiento para prueba del PCN.pdf" y "Notificación prueba PCN.pdf" Así mismo, la documentación de dichas pruebas será entregadas al área de auditoría interna del FIFOMI, **el próximo martes 26 de noviembre de 2019.**
15	Recomendación	La Gerencia de Informática cuenta con procedimientos y lineamientos para la capacitación y divulgación de la Seguridad de la Información de FIFOMI, no obstante, para el periodo revisado (octubre 2018 a septiembre 2019) no se cuenta con la evidencia de la aplicación del procedimiento. Sin embargo, se cuenta con el proyecto de implementación del Programa de Seguridad de la Información del FIFOMI para este último trimestre del año, donde se contempla todo el tema de capacitación y divulgación. Así mismo, se cuentan con políticas y procedimientos en materia de seguridad de la información que no se encuentran actualizados y totalmente implementados, como lo son: • Procedimiento de Seguridad de Infraestructura de TIC (Proc. Mantenimiento y Accesos a Centro de Datos); • Procedimiento de Gestión de Riesgos (Análisis de costo-beneficio de controles de seguridad); • Sistema de Gestión de Seguridad de la información; • Procedimiento de Incidentes;	La Gerencia de Informática indicó que durante el Programa de Seguridad de la Información que se realizará con apoyo del proveedor a quien se adjudicó la licitación IA-010K2O001-E112-2019, entregará al área de auditoría interna del FIFOMI el temario y listas de asistencia del curso ya realizado a todos los empleados del Fideicomiso con relación a la concientización, capacitación y divulgación de la Seguridad de la Información. **Fecha compromiso:** 31 de diciembre de 2019 Con relación a la actualización de las políticas y procedimientos descritos en el hallazgo, la Gerencia de Informática indicó que, durante el Programa de Seguridad de la Información mencionado anteriormente, entregará el proyecto de actualización y fecha de cada una de ellas. **Fecha compromiso:** 15 enero 2020

		• Procedimiento de Divulgación y capacitación de seguridad de la información; • Política de Seguridad de la Información; • Procedimiento de Monitoreo del Desempeño y Capacidad de la infraestructura Tecnológica y de Telecomunicaciones (monitoreo de manera visual y no se utilizan bitácora y seguimiento); Procedimiento de Riesgos. *(Disposiciones de Carácter General Aplicables a los Organismos y Entidades de Fomento, artículo 172 fracción V. Proceso ASI, actividad 3 Diseño del SGSI del MAAGTICSI)* *Referencia documental: SI-38*	
16	Recomendación	Actualmente el FIFOMI, cuenta con un listado de Infraestructuras de información críticas y/o esenciales y activos críticos, dentro del documento "BIA Procesos Críticos de la GI.pdf". Sin embargo, el documento data de mayo del 2018 y este debe ser revisado al menos una vez al año de acuerdo a lo establecido en el factor crítico 14, adicional a que no se encuentra evidencia de la autorización del Titular de FIFOMI. (*Disposiciones de Carácter General Aplicables a los Organismos de Fomento y Entidades de Fomento, artículo 169, fracción VI, inciso f). Proceso ASI, Actividad 4 del MAAGTICSI)* *Referencia documental: SI-39*	La Gerencia de Informática indicó que durante el Programa de Seguridad de la Información que se realizará con apoyo del proveedor a quien se adjudicó la licitación IA-010K2O001-E112-2019, entregará al área de auditoría interna del FIFOMI la actualización de la lista de infraestructuras de información críticas y/o esenciales, así como su autorización por parte del Titular del FIFOMI. **Fecha compromiso:** 15 enero 2020

Conclusiones

Derivado de lo realizado durante la auditoría en materia Informática 2019, de haber sostenido entrevistas con las áreas involucradas, revisar documentación compartida por parte de la Gerencia de Informática y haber ejecutado las pruebas y controles, se llegan a las siguientes conclusiones:

- Mediante las distintas pruebas realizadas a los sistemas SAP para evaluar su integración con los procesos del negocio, se estima necesario realizar una evaluación de los roles y perfiles de usuarios asociados a los distintos módulos, debido a que su implementación inicial data a mediados del 2012 y al día de hoy, no se detectan ajustes y actualizaciones de las matrices de roles y funciones de acuerdo a la realidad actual del negocio.
- Se requiere implementar prácticas de gestión de necesidades de negocio, con la finalidad de poder realizar mejoras y ajustes a las configuraciones sin impactar la operación de los sistemas previo a cualquier trabajo de mejora considerado para las herramientas.
- Se identificó que el personal de la Gerencia de Informática hace todo lo que está a su alcance para garantizar que el riesgo tecnológico permanezca bajo en las medidas de sus posibilidades, lo que podría apoyarse con un análisis profundo de sus capacidades y considerando la integración de talento clave para el apoyo de sus actividades, tanto documentales como operativas.

En adición a la revisión se detectó que la Gerencia de Informática cuenta una estrategia de actualización de la plataforma SAP (2020-2021) la cual trata de la migración de la infraestructura actual a la nube SAP HANA, por lo que es conveniente que durante este proyecto se habilite el parámetro rec/client (huellas de auditoría), así como llevar a cabo un análisis profundo para evaluar y en su caso restructurar la matriz de autorizaciones (Roles SAP 2019) que contienen los roles y perfiles definidos desde su origen (año 2012), y con ello poder disminuir los riesgos a través de una adecuada segregación de funciones.

FIFOMI
FIDEICOMISO DE FOMENTO MINERO

Informe sobre el Riesgo Tecnológico de la auditoría en materia Informática 2019

Noviembre, 2019

Índice de abreviaturas utilizadas

CNBV	Comisión Nacional Bancaria y de Valores.
Disposiciones	Disposiciones de carácter general aplicables a los organismos de fomento y entidades de fomento
FIFOMI; Fideicomiso	Fideicomiso de Fomento Minero.
GESI	Grupo Estratégico de Seguridad de la Información.
SAP	Sistemas, Aplicaciones y Productos (Systems, Applications, Products in Data Processing)
SAP BASIS	Controles Generales de la Aplicación (Seguridad de la Información de la Aplicación)
GRP	Planificación de Recursos del Gobierno (Government Resource Planning)
CRM	Gestión de la relación con el cliente (Customer Relationship Management).
ID	Identificador.
MAAGTICSI	Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información.
TI	Tecnologías de la Información

Índice

Introducción

El informe de riesgo tecnológico del Fideicomiso de Fomento Minero (FIFOMI) del periodo 2019 toma como referencia los resultados finales del servicio de Auditoría en Materia Informática realizada para dicho periodo, con la finalidad de identificar brechas de control en materia de sistemas informáticos y cumplir con las obligaciones que se encuentran descritas en las "Disposiciones de carácter general aplicables a los organismos de fomento y entidades de fomento" (en adelante Disposiciones) emitidas por la Comisión Nacional Bancaria y de Valores (en adelante CNBV) y verificar las establecidas en el *artículo 79 fracción II inciso b).*

Antecedentes; fundamento legal y normativo

El FIFOMI es una entidad paraestatal, cuya cabeza de sector es la Secretaría de Economía, a la vez que forma parte del Sistema Financiero Mexicano, debido a que una de sus actividades preponderantes es otorgar financiamiento, por lo que su regulación y supervisión corresponde a CNBV.

La CNBV establece en las Disposiciones publicadas en el Diario Oficial de la Federación el 1 de diciembre de 2014 y sus diversas modificaciones, las funciones que, en materia de riesgo tecnológico, está obligado a realizar el FIFOMI, en apego al contenido del artículo 79 fracción II, inciso b).

Artículo 79.- *En materia de riesgos cuantificables no discrecionales los Organismos de Fomento y Entidades de Fomento se sujetarán a lo siguiente:*

b) La administración del riesgo tecnológico:

1. Evaluar la vulnerabilidad en el hardware, software, sistemas, aplicaciones, seguridad, recuperación de información y redes, por errores de procesamiento u operativos, fallas en procedimientos, capacidades inadecuadas e insuficiencias de los controles instalados, entre otros.

2. Considerar en la implementación de controles internos, respecto del hardware, software, sistemas, aplicaciones, seguridad, recuperación de información y redes del Organismo de Fomento o de la Entidad de Fomento, cuando menos, los aspectos siguientes:

i. Mantener políticas y procedimientos que aseguren en todo momento el nivel de calidad del servicio y la seguridad e integridad de la información; lo anterior, con especial énfasis cuando los Organismos de Fomento y Entidades de Fomento contraten la prestación de servicios por parte de proveedores externos para el procesamiento y almacenamiento de dicha información.

ii. Asegurar que cada operación o actividad realizada por los usuarios deje constancia electrónica que conforme registros de auditoría.

iii. Implementar mecanismos que midan y aseguren niveles de disponibilidad y tiempos de respuesta, que garanticen la adecuada ejecución de las operaciones y servicios realizados.

3. En caso de mantener canales de distribución para operaciones con clientes y derechohabientes realizadas a través de la red electrónica mundial denominada Internet, vía telefónica y oficinas, entre otros, deberán en lo conducente:

i. Establecer medidas y controles necesarios que permitan asegurar confidencialidad en la generación, almacenamiento, transmisión y recepción de las claves de identificación y acceso para los usuarios.

ii. Implementar medidas de control que garanticen la protección, seguridad y confidencialidad de la información generada por la realización de operaciones a través de cualquier medio tecnológico.

iii. Contar con esquemas de control y políticas de operación, autorización y acceso a los sistemas, bases de datos y aplicaciones implementadas para la realización de operaciones a través de cualquier medio tecnológico.

iv. Incorporar los medios adecuados para respaldar y, en su caso, recuperar la información que se genere respecto de las operaciones que se realicen a través de cualquier medio tecnológico.

v. Diseñar planes de contingencia, a fin de asegurar la capacidad y continuidad de los sistemas implementados para la celebración de operaciones, a través de cualquier medio tecnológico. Dichos planes deberán comprender, además, las medidas necesarias que permitan minimizar y reparar los efectos generados por eventualidades que, en su caso, llegaren a afectar el continuo y permanente funcionamiento de los servicios.

vi. Establecer mecanismos para la identificación y resolución de aquellos actos o eventos que puedan generarle al Organismo de Fomento o la Entidad de Fomento, riesgos derivados de:
vi.i Comisión de hechos, actos u operaciones fraudulentas a través de medios tecnológicos.
vi.ii Contingencias generadas en los sistemas relacionados con los servicios prestados y operaciones celebradas a través de cualquier medio tecnológico.
vi.iii El uso inadecuado por parte de los usuarios de los canales de distribución antes mencionados, para operar con el Organismo de Fomento o la Entidad de Fomento, a través de los medios citados en el presente artículo.

Los Organismos de Fomento y Entidades de Fomento deberán evaluar las circunstancias que en materia de riesgo tecnológico pudieran influir en su operación ordinaria, las cuales se sujetarán a vigilancia permanente a fin de verificar el desempeño del proceso de Administración Integral de Riesgos.

Adicionalmente, el FIFOMI, como parte de la Administración Pública Federal, da cumplimiento a las Disposiciones para la Estrategia Digital Nacional, en Materia de Tecnologías de Información y Comunicaciones, y en la Seguridad de la Información (MAAGTICSI), emitido por la Secretaría de la Función Pública.

Resultados finales

Derivado de la evaluación de cumplimiento y de acuerdo a lo establecido en las Disposiciones, emitidas por la CNBV, así como lo regulado por el MAAGTICSI, se llevó a cabo la revisión de los mecanismos de control, así como la verificación de los sistemas informáticos a fin de preservar la integridad, confidencialidad y disponibilidad de la información, a efecto de evitar su alteración y cumplir con los objetivos, para los cuales fueron implementados, además de identificar las fallas potenciales de los sistemas.

Se verificó que los procesos de negocio, de acuerdo con la arquitectura funcional actual del SAP-GRP-CRM, se encuentren debidamente identificados y controlados (integridad de los procesos de negocio). Durante la auditoría se llevaron a cabo sesiones de entendimiento con los distintos enlaces de las áreas del negocio, donde identificamos a los diferentes autores y flujos de información que conforman cada uno de los procesos, así como el registro de la información y la interacción con el sistema SAP.

De acuerdo con el organigrama 2019 de FIFOMI, las áreas recorridas fueron:

- Gerencia de Informática
- Gerencia de Presupuesto y Contabilidad
- Gerencia de Cartera
- Gerencia de Cumplimiento Normativo
- Subdirección Jurídica
- Gerencia de Recursos Materiales
- Gerencia de Tesorería
- Gerencia de Recursos Humanos
- Gerencia de Comunicación y Difusión
- Subdirección de Riesgos
- Subdirección Técnica
- Gerencia de Operación
- Gerencia de Seguimiento y Evaluación
- Gerencia de Crédito y Contratación

a) Seguridad de la Información + MAAGTICSI

En concordancia con el MAAGTICSI dentro de las políticas y disposiciones para la Estrategia Digital Nacional en materia de tecnologías de la información y comunicaciones y en la seguridad de la información se realizó la **revisión de controles para los 9 procesos base del marco normativo MAAGTICSI**, donde se pudo verificar el nivel de apego que la Gerencia de Informática y áreas de apoyo tienen.

b) Controles Generales de SAP BASIS CRM y GRP

Con fundamento en las *Disposiciones* y con el fin de asegurar que los sistemas informáticos, incluyendo los contables, operacionales de cartera crediticia, con valores o de cualquier otro tipo, cuenten con mecanismos para preservar la

integridad, confidencialidad y disponibilidad de la información, que eviten su alteración y cumplan con los objetivos para los cuales fueron implementados o diseñados, se llevó a cabo la **revisión de la seguridad de la aplicación,** donde se determinan los parámetros adecuados de permisos y accesos que se tienen a transacciones sensibles, con el fin de identificar los niveles de seguridad e integridad de los accesos al sistema, propias que deben pertenecer a un área especializada como en este caso se considera a la Gerencia de Informática. Adicionalmente, se evaluó la **gestión y configuración con la que opera el FIFOMI a través de la aplicación,** evaluando diversos controles específicos para la validación dentro de los ambientes productivos, configuración de contraseñas, gestión de cambios a través de transportes, entre otros.

c) Controles Funcionales y Accesos SAP

Con fundamento en las *Disposiciones* y con la finalidad de verificar que los sistemas informáticos, incluyendo los contables, operacionales de Cartera Crediticia, con valores o de cualquier otro tipo, cuenten con mecanismos para preservar la integridad, confidencialidad y disponibilidad de la información, incluyendo también la posibilidad de cerciorarse de la calidad, suficiencia y oportunidad de la información, así como que sea confiable para la adecuada toma de decisiones, y tal información se proporcione en forma correcta y oportuna a las autoridades competentes, se evaluó la **gestión y configuración con la que opera el FIFOMI,** probando diversos controles a lo largo de los 18 módulos de SAP GRP y CRM, así como la segregación de roles y accesos, con las cuales se pudo llevar a cabo las verificaciones de los controles propios de los módulos funcionales de SAP.

Riesgos detectados en la auditoría en materia informática.

Con base en el **artículo 79** de las Disposiciones de la CNBV para la administración del riesgo tecnológico en el que indica que, en materia de riesgos cuantificables no discrecionales, los Organismos de Fomento y Entidades de Fomento se sujetarán a las actividades descritas en la **fracción II y su inciso b),** determina:

1. Evaluar la vulnerabilidad en el hardware, software, sistemas, aplicaciones, seguridad, recuperación de información y redes, por errores de procesamiento u operativos, fallas en procedimientos, capacidades inadecuadas e insuficiencias de los controles instalados, entre otros.

Conforme a este requerimiento podemos determinar que FIFOMI se encuentra en proceso de fortalecimiento de los controles implementados con el fin de mitigar los riesgos tecnológicos que se pueden presentar en las tecnologías de la información y comunicaciones por las causas descritas.

Es importante mencionar que se identificaron diferentes hallazgos en la auditoría en materia informática 2019, los cuales fueron remediados durante la misma, es decir llevaron a cabo las acciones correctivas necesarias para eliminar la fuente del riesgo de cada una de ellas, tomando en cuenta las acciones a realizar recomendadas por los auditores. Estos hallazgos se presentan a continuación:

ID	*Descripción*	*Impacto*	*Nivel de Riesgo*
1.1	Se identificó 1 usuario funcional en el periodo 2019 con permisos con los que no deberían de contar de acuerdo con sus funciones y área para las transacciones SU01, SU02, SU10-SU12, SUGR, PFCG del sistema SAP CRM.	1 usuario funcional que puede incurrir sin consentimiento a los siguientes ajustes en el sistema: • Creación de Usuarios, • Mantenimiento de Perfiles, • Mantenimiento Masivo de Perfiles, • Mantenimiento de Roles,	Medio

ID	Descripción	Impacto	Nivel de Riesgo
		• Mantenimiento de Grupo de Usuarios.	
1.2	Se identificaron usuarios funcionales con permisos con los que no deberían de contar de acuerdo con sus funciones y área para las transacciones siguientes: Para la transacción SU24: • 4 usuarios son nuevos generados en el 2019. Para la transacción SU25 y AUTH_SWITCH_OBJECTS • 1 usuario es nuevo generado en el 2019.	Usuarios funcionales que pueden incurrir sin consentimiento a los siguientes ajustes en el sistema: Autorización al Mantenimiento de Objetos, Generación de Perfiles, Autorización de Cambio de objetos On/Off de las transacciones: SU24, SU25, AUTH_SWITCH_OBJECTS.	Medio
1.3	Se identificó 1 usuario funcional con permisos con los que no deberían de contar de acuerdo con sus funciones y área para las transacciones siguientes: SE37, SE80, SMOD.	1 usuario funcional que puede incurrir sin consentimiento a los siguientes ajustes en el sistema: Módulo de funciones ABAP, Navegador de Objetos, Gestión de Mejoras SAP de las transacciones: SE37, SE80, SMOD.	Medio
1.4	Se identificó 1 usuario funcional generado en el año 2019 con permisos con los que no deberían de contar de acuerdo con sus funciones y área para las transacciones siguientes: OAB4, SM36, SM37.	1 usuario funcional generado en el año 2019 que pueden incurrir sin consentimiento a los siguientes ajustes en el sistema: Creación de trabajos por lote SAP, Programar trabajos en segundo plano, Selección de vistas generales de las transacciones: OAB4, SM36, SM37.	Alto
1.5	Se identificó 1 usuario funcional nuevo generado en el año 2019 con permisos con los que no deberían de contar de acuerdo con sus funciones y área para las transacciones siguientes: SM49, SM69.	1 usuario funcional nuevo generado en el año 2019 que pueden incurrir sin consentimiento a los siguientes ajustes en el sistema: Ejecución de comandos externos OS, Mantenimiento de comandos externos OS de las transacciones: SM49, SM69	Alto
1.6	Se identificó 1 usuario funcional nuevo generado en el año 2019 con permisos con los que no deberían de contar de acuerdo con sus funciones y área para las transacciones siguientes: STMS, SCTS, SE03, SE06.	Un usuario funcional que puede incurrir sin consentimiento a los siguientes ajustes en el sistema: Sistema de Gestión de Transporte, Opción de Cambio System RSWBO004, Herramientas Organizador de Transporte, Configuración Organizador de Transporte de las transacciones: STMS, SCTS, SE03, SE06.	Medio
1.7	Se identificó un usuario funcional con permisos que de acuerdo con sus funciones y área no deberían de contar para la transacción: SCC4.	Un usuario funcional que puede incurrir sin consentimiento a los siguientes ajustes en el sistema: Administración de Clientes de la transacción - SCC4.	Medio
1.8	Se identificó un usuario funcional con permisos que de acuerdo con sus funciones y área no deberían de contar para las transacciones: SE38, SE80.	Un usuario funcional que puede incurrir sin consentimiento a los siguientes ajustes en el sistema: Editor ABAP, Navegador de Objetos de las transacciones.	Medio
1.9	Se identificó 1 usuario - FQUIROGA nuevo generado en el año 2019 con permisos que de acuerdo con sus funciones y área no	1 usuario funcional generados en el año 2019 que puede incurrir sin consentimiento a los siguientes ajustes en el sistema: Editor ABAP de la transacción - SE38.	Medio

ID	Descripción	Impacto	Nivel de Riesgo
	deberían de contar para la transacción: SE38.		
1.10	Se identificó un usuario funcional con permisos, que de acuerdo con sus funciones y área no deberían de contar para la transacción: RZ10.	Un usuario funcional que puede incurrir sin consentimiento a los siguientes ajustes en el sistema: Mantenimiento de parámetros de perfiles de la transacción: RZ10.	Medio
1.11	Se identificó un usuario funcional con permisos, que de acuerdo con sus funciones y área no deberían de contar para la transacción: SE14.	Un usuario funcional que puede incurrir sin consentimiento a los siguientes ajustes en el sistema: Utilerías para Tablas de Diccionarios de la transacción - SE14.	Medio
1.12	Se identificó un usuario funcional con permisos, que de acuerdo con sus funciones y área no deberían de contar para la transacción: SM59.	Un usuario funcional que puede incurrir sin consentimiento a los siguientes ajustes en el sistema: RFC - Destinations de la transacción - SM59.	Medio
1.13	Se identificó un usuario funcional con permisos, que de acuerdo con sus funciones y área no deberían de contar para las transacciones: SM50, SM51, SM66, SM12.	Un usuario funcional que puede incurrir sin consentimiento a los siguientes ajustes en el sistema: Proceso de Trabajo OverView, Lista de Sistema SAP, Proceso de Trabajo Systemwide, Borrado de Bloqueos de Objetos de las transacciones - SM50, SM51, SM66, SM12.	Medio
2	Se realizó una consulta de los parámetros de uso de contraseñas para SAP CRM de acuerdo al plan de prueba. Se identificó que los parámetros *login/min_password_specials* y *login/min_password_uppercase* no se encuentran con valores según las reglas de FIFOMI con respecto a la política interna perfil, mismos que se encuentran en valor 0 cuando deberían ser por lo menos el valor 1.	Al no respetar las políticas de seguridad de la información en lo relacionado con el control de las contraseñas, podría facilitarse la suplantación de identidades o el manejo indebido de las credenciales por parte de terceros.	Bajo

2. Considerar en la implementación de controles internos, respecto del hardware, software, sistemas, aplicaciones, seguridad, recuperación de información y redes del Organismo de Fomento o de la Entidad de Fomento, cuando menos, los aspectos siguientes:

i. Mantener políticas y procedimientos que aseguren en todo momento el nivel de calidad del servicio y la seguridad e integridad de la información; lo anterior, con especial énfasis cuando los Organismos de Fomento y Entidades de Fomento contraten la prestación de servicios por parte de proveedores externos para el procesamiento y almacenamiento de dicha información.

De acuerdo a la evaluación del apartado anterior, se determinaron los siguientes hallazgos, mismos que fueron remediados durante la auditoría:

ID	Hallazgo	Impacto	Nivel de riesgo
3.1	Se ingresó a la Tabla T000 para validar la configuración del ambiente productivo, encontrando que se encuentra parametrizado para permitir cambios directos sin necesidad de pasar por un sistema de transporte del sistema CRM.	La configuración en el ambiente productivo se encuentra parametrizado para permitir cambios directos en el sistema sin necesidad de pasar por un sistema de transporte. Los usuarios que cuenten con estos permisos podrían incurrir, sin consentimiento, a realizar cambios dentro del ambiente productivo, lo cual conforma un riesgo al no contar con un control que proteja la información ni tampoco un mecanismo confiable que permita realizar cambios que sean probados antes de ser implementados mediante un mecanismo de control de cambios.	Alto
3.2	Se ingresó a la Tabla T000 para validar la configuración del ambiente productivo, encontrando que se encuentra parametrizado para permitir cambios directos sin necesidad de pasar por un sistema de transporte del sistema GRP.		Alto
4.1	Se identificaron 7 usuarios que nunca han accedido en el sistema CRM o que no han accedido en los últimos 3 meses.	Contar con usuarios activos que no han accedido y que tienen estas características conlleva un riesgo en la información y en la integridad del sistema.	Bajo
4.2	Se identificaron 4 usuarios que nunca han accedido en el sistema GRP o que no han accedido en los últimos 3 meses.	Contar con usuarios activos que no han accedido y que tienen estas características conlleva un riesgo en la información y en la integridad del sistema.	Bajo
5	A través de la tabla LFA1 se observó que los siguientes proveedores tienen habilitado el campo "Recepción Alternativo de pago", lo cual permite cambiar a un proveedor alternativo para efectuar el pago durante el procesamiento de la factura.	Existen 14 proveedores con el campo "Receptor Alternativo de Pago" habilitado, lo cual permite cambiar a un proveedor alternativo para efectuar el pago durante el procesamiento de la factura.	Medio
6	Para las cuentas contables dentro del Plan de Cuentas FIFOMI - 1000 se observó que 22 cuentas contables marcadas en el campo “Marcadas para borrado” no se encontraban marcadas en el campo “Bloqueadas para Posteo”, lo que permite que dichas en dichas cuentas contables puedan realizarse movimientos contables.	Las cuentas marcadas para borrado no se encuentran bloqueadas, lo que permite seguir realizando movimientos contables en dichas cuentas.	Medio
7	Para validar dicha configuración se ingresó a la Tabla V_T001B y se observó que, a la fecha de nuestra revisión, todos los periodos están abiertos para modificar en periodos contables diferentes al actual. Es decir, el único periodo contable abierto debería ser el 10 - octubre, sin embargo, los 16 periodos se encuentran abiertos, lo que permite que cualquier movimiento contable pueda aplicarse en cualquier fecha.	Todos los periodos están abiertos para modificar en periodos contables diferentes al actual, lo que permite que cualquier movimiento contable pueda aplicarse en cualquier fecha.	Medio

Así mismo, se identificaron hallazgos adicionales que se encuentran con un plan de acción, mismo que es responsabilidad de la Gerencia de Informática su implementación y el área de auditoría interna confirmará su cumplimiento de acuerdo a lo comprometido, los cuales se describen a continuación:

ID	*Hallazgo*	*Impacto*	*Nivel de riesgo*
10	No se cuenta con la Directriz de Análisis de Riesgos, con el objetivo de identificar, clasificar y priorizar los riesgos para evaluar su impacto sobre los procesos y los servicios de la Institución.	Existe la posibilidad de que se presenten y materialicen riesgos tecnológicos y de seguridad de la información por falta de identificación, tratamiento y control preventivo.	Alto
11	No se cuentan con políticas y procedimientos documentados que incluyan los controles que se practican hoy en día para el manejo (entradas y salidas) de los activos de información.	Es importante que se documenten los controles referentes a la entrada y salida de activos de información con el objetivo que se lleven a cabo de manera sistemática y verificar su cumplimiento y garantizar la confidencialidad, integridad y disponibilidad de la información.	Medio
12	No se encuentra autorizado el programa "Política de respaldo, recuperación y borrado seguro de la información". Mismo que se espera sea aprobado por el GESI.	La información contenida en medios magnéticos ya sea de computadoras de escritorio, laptops o servidores; contienen información propiedad del FIFOMI que puede ser confidencial o de uso exclusivo de ciertas áreas. Al no contar con un procedimiento establecido de borrado, puede no llevarse a cabo esta actividad o llevarse a cabo de manera no segura.	Medio
15	Se cuenta con procedimientos y lineamientos para la capacitación y divulgación de la Seguridad de la Información, no obstante, para el periodo revisado no se cuenta con la evidencia de la aplicación del procedimiento. Así mismo, se cuentan con políticas y procedimientos en materia de seguridad de la información que no se encuentran actualizados y totalmente implementados.	El personal de FIFOMI no está actualizado en las medidas de seguridad de la información, así como de las recomendaciones que el GESI pueda aportar, por lo que es un riesgo para la confidencialidad, integridad y disponibilidad de la información del Fideicomiso.	Medio

ii. Asegurar que cada operación o actividad realizada por los usuarios deje constancia electrónica que conforme registros de auditoría.

De acuerdo a lo requerido a esta disposición, durante la auditoría en materia informática se detectó que la Gerencia de Informática cuenta una estrategia de actualización de la plataforma SAP (2020-2021) la cual trata de la migración de la infraestructura actual a la nube SAP HANA, por lo que es conveniente que durante este proyecto se habilite parámetro rec/client (huellas de auditoría), con el objetivo de velar por la seguridad que proteja la información, así como el acceso que garantice la integridad del sistema y la información generada, almacenada y/o transmitida.

iii. Implementar mecanismos que midan y aseguren niveles de disponibilidad y tiempos de respuesta, que garanticen la adecuada ejecución de las operaciones y servicios realizados.

Conforme a la disposición declarada anteriormente, como resultado de la auditoría en materia informática, se identificaron los siguientes hallazgos que pudieran afectar los niveles de disponibilidad y tiempos de respuesta de los servicios tecnológicos y que afecten a la operación de la entidad, mismos que son detallados a continuación y cuentan con un plan de acción correctivo para mitigar dichos riesgos:

ID	Hallazgo	Impacto	Nivel de riesgo
8	No se cuenta con el programa de capacidad y su monitoreo.	Falta de planeación y definición de acciones preventivas para asegurar la disponibilidad de la infraestructura que soporta la operación de los servicios.	Medio
9	No se cuenta con un repositorio de configuraciones, en el que se integren las soluciones tecnológicas y sus componentes.	Falta de planeación y definición de estrategias para la continuidad de las operaciones de FIFOMI ante un evento que afecte la disponibilidad e integridad de la información, así como que la capacidad de reacción de la Institución se comprometa.	Bajo
13	Organizar, clasificar e identificar el cableado estructurado de los equipos de comunicaciones que se encuentran en el site.	Desconexiones no previstas o accidentales, no tener identificado el cableado estructurado para que, en caso de presentarse algún cambio de equipo, se presenten deficiencias.	Bajo
14	Es necesario que el Plan de Continuidad del Negocio cuente con pruebas y revisiones anuales para verificar la efectividad del plan y garantizar que se tomen en cuenta cambios o actualizaciones en los procesos de negocio.	No identificar algún cambio o mejora en la definición de las estrategias para la continuidad de las operaciones de FIFOMI ante un evento que afecte la disponibilidad e integridad de la información, así como que la capacidad de reacción de la Institución se comprometa.	Alto
16	Se cuenta con un listado de Infraestructuras de información críticas y/o esenciales y activos críticos. Sin embargo, el documento data de mayo del 2018 y este debe ser revisado al menos una vez al año, adicional a que no se encuentra evidencia de la autorización del Titular de FIFOMI.	No identificar algún activo o infraestructura crítica por cambios o actualización en los procesos de FIFOMI para establecer los controles necesarios para los riesgos asociados a estos.	Medio

3. En caso de mantener canales de distribución para operaciones con clientes y derechohabientes realizadas a través de la red electrónica mundial denominada Internet, vía telefónica y oficinas, entre otros, deberán en lo conducente:

Para el caso del numeral 3 y sus apartados del i. al vi., se concluye que no es aplicable al Fideicomiso, ya que no cuenta con canales de distribución para operaciones directas con los clientes, por lo tanto, no fue evaluado el nivel de riesgo tecnológico con base a esta disposición.

Los Organismos de Fomento y Entidades de Fomento deberán evaluar las circunstancias que en materia de riesgo tecnológico pudieran influir en su operación ordinaria, las cuales se sujetarán a vigilancia permanente a fin de verificar el desempeño del proceso de Administración Integral de Riesgos.

Para este punto, es importante que se desarrolle e implemente la Directriz de Administración de Riesgos como se menciona en el hallazgo ID. *10* para evaluar su impacto sobre los procesos y los servicios de la Institución de Tecnología Establecer los mecanismos de administración de riesgos que permitan identificar, analizar, evaluar, atender y monitorear los riesgos. Así mismo, es importante mencionar que la Gerencia de Informática cuenta con un plan de acción para la remediación de este punto.

Conclusiones

Derivado de lo descrito anteriormente, en conclusión, se determina que el desarrollo de controles, implementación de políticas y procedimientos y adopción de mejores prácticas por parte del FIFOMI, han mitigado los riesgos en el ambiente tecnológico y seguridad de la información, en apego a las Disposiciones y normatividad aplicable al mismo.

Por lo que, conforme al nivel de riesgo de los hallazgos detectados en la auditoría en materia informática y de acuerdo a los impactos que se pueden derivar en caso de omitir realizar acciones correctivas o preventivas para su atención, se determina que en promedio el Fideicomiso se encuentra en un nivel de riesgo Medio, como se describe en la siguiente tabla:

Nivel de Riesgo	***# de Hallazgos***
Alto	*6*
Medio	*22*
Bajo	*5*
Total	***33***

Es importante mencionar que la entidad se encuentra en proceso de desarrollo de metodologías de análisis de riesgos asociados a las Tecnologías de la Información y Comunicaciones, con el objetivo de asegurar la confidencialidad, integridad y disponibilidad de la información, que aseguren desde su identificación hasta su tratamiento.

Asimismo, la Gerencia de Informática ha confirmado que, con el desarrollo de diversos proyectos de TI, como es la "Actualización de la Plataforma SAP" que se llevará a cabo en el periodo 2020-2021, se continuará mitigando diversos riesgos existentes dentro de la entidad.

Opinión sobre Riesgo Tecnológico del FIFOMI

Se identificó que la Gerencia de Informática tiene una preocupación constante por mitigar el riesgo tecnológico del FIFOMI, lo cual toma como eje rector para el desarrollo de sus funciones y muestra de ello es el impulso de iniciativas que se han planteado, dentro de las que se encuentran:

- Pruebas de vulnerabilidades a las Tecnologías de la Información y Comunicaciones.
- Actualización del Sistema SAP del FIFOMI considerando su migración a la plataforma SAP S4/HANA.
- Programa de Seguridad de la Información.
- Digitalización y Sistematización con conectividad al Sistema SAP.
- Renovación del servicio integral de procesamiento, almacenamiento y respaldo proporcionado mediante un centro de datos en un esquema a demanda.

Se resalta el esfuerzo para implementar controles internos, a través del establecimiento de políticas y procedimientos que aseguren la disponibilidad del servicio en niveles óptimos para la operación y la seguridad de la información, así como la implementación de acciones, entre las cuales, se resalta la actualización del firewall con la finalidad de robustecer la seguridad perimetral.

Sin embargo, se considera que la estructura actual de personal dentro de la Gerencia de Informática puede resultar insuficiente para cubrir la demanda futura que se espera derivada del desarrollo de las iniciativas antes listadas, así como las necesidades actuales de las distintas áreas funcionales de la Institución.

Por esto es importante que se conserve el propósito de fortalecimiento de controles y el seguimiento de las iniciativas a fin de que se puedan mantener constantemente actualizados y vigentes, y con esto disminuir los niveles de riesgo tecnológico latentes en la institución al nivel más bajo posible.