FUNCIÓN PÚBLICA	**Órgano Interno de Control en el Instituto del Fondo Nacional para el Consumo de los Trabajadores**	N° de auditoría: 5/2021
Entidad Fiscalizada: Instituto FONACOT	**Sector:** Trabajo y Previsión Social	**Clave:** 14120
Unidad auditada: Subdirección General de Tecnologías de la Información y Comunicación		**Clave de programa:** 800 "Al Desempeño"

ÍNDICE

a) objetivo del acto de fiscalización

En cumplimiento al Programa Anual de Fiscalización 2021, se llevó a cabo la auditoría No. 5/2021, al amparo de la orden del acto de fiscalización número OIC/14/120/2021/0123, de fecha 14 de abril de 2021, la cual fue entregada personalmente al Mtro. Horacio Sánchez Tinoco, Subdirector General de Tecnologías de la Información y Comunicación, el 14 de abril de 2021, según consta en dicha orden del acto de fiscalización y el acta administrativa de inicio.

El servidor público comisionados para la revisión fue el CC. Ernesto Jesús Pedroza de la Llave, con cargo de Titular del Área de Auditoría Interna, de Desarrollo y Mejora de la Gestión Pública, quien fungió como Coordinador del Acto de Fiscalización, y los siguientes auditores públicos comisionados C.C. Víctor Noé Hernández Guadarrama, con cargo de Gerente de Auditoría Interna y los CC. Guadalupe Suárez Curiel y Germán Amezcua Vallarta, ambos con cargos de Coordinador Técnico Administrativo de Alta Responsabilidad y los CC. Ana Karen Mendiola Quiroz, Elia Maldonado Serrano y Mario Villalobos Rosas, los tres con cargo de Coordinadores Administrativos de Alta Responsabilidad adscritos a este Órgano Interno de Control en el Instituto FONACOT.

El objetivo de la auditoría consistió en evaluar el desempeño de la Subdirección General de Tecnologías de la Información y Comunicación, al verificar su eficiencia, eficacia, economía y efectividad en el cumplimiento de metas y objetivos.

b) Alcance de la auditoría

Presupuesto ejercido de la Subdirección General de Tecnologías de la Información y Comunicación para el ejercicio 2020:

Alcance	Presupuesto Ejercido 2020 (pesos)
Universo	$252´472,599
Muestra	$252´472,599
Representatividad	100%

El alcance de la Auditoría 5/2021 se dirigió a:

a) Verificar el cumplimiento de Programa Anual de Trabajo. (eficiencia).

b) Constatar que las tecnologías de la información se hayan orientado a eficientar el desarrollo de las actividades de los usuarios. (eficiencia).

c) Comprobar que el desarrollo de la infraestructura tecnológica se haya orientado a optimizar las operaciones sustantivas y adjetivas de la Institución. (Eficacia).

d) Validar que, en casos de contingencias, las políticas en materia de seguridad informática hayan permitido recuperar la información (eficiencia).

e) Verificar que la normativa en materia de Tecnologías de Información y Comunicaciones esté actualizada y asegure la debida atención de los usuarios. (Legalidad)

f) Verificar que los estudios de factibilidad en materia de tecnologías de la información e infraestructura tecnológica se hayan gestionado en tiempo y forma ante las instancias correspondientes. (Economía)

El periodo revisado comprendió del 2 de enero al 31 de diciembre de 2020:

Esta auditoría se desarrolló de conformidad con las Normas Generales de Auditoría Pública y con los procedimientos y técnicas de auditoría que se consideraron necesarios, las cuales consistieron, entre otras; en el estudio general, la inspección, la investigación, el análisis y cálculo, para comprobar la eficiencia, eficacia, economía y efectividad en el cumplimiento de metas y objetivos de la Subdirección General de Tecnologías de la Información y Comunicación.

c) Área fiscalizada

Con el fin de lograr el objetivo, se determinó, como parte de la metodología de la auditoría de desempeño, revisar la Subdirección General de Tecnología de la Información y Comunicación.

Objetivo: Desarrollar y dirigir los servicios de Tecnologías de Información y Comunicación para que el Instituto FONACOT cuente oportunamente con herramientas e infraestructura necesaria, que permita lograr la eficiencia operativa y se constituya como el soporte a la operación de acuerdo a la normatividad aplicable en materia de política digital vigente y en apego a los principios éticos de lealtad, honradez, legalidad, imparcialidad, eficiencia y los valores de integridad, cooperación, liderazgo, interés público, transparencia, respeto a los derechos humanos, igualdad, no discriminación, equidad de género y rendición de cuentas.

d) Antecedentes del área auditada

En los últimos ejercicios el Órgano Interno de Control no había practicado auditorías de desempeño o de ningún otro tipo a la Subdirección General de Tecnologías de la Información y Comunicación

e) Resultados

1. Manuales de Organización Específicos, Manuales de Políticas y Procedimientos de la Subdirección General de Tecnologías de la Información y Comunicación y Manual del Sistema de Gestión de Seguridad de la Información desactualizados

La última Estructura Orgánica de la Subdirección General de Tecnologías de la Información y Comunicación (SGTIC), autorizada por la Secretaría de la Función Pública, que tiene vigencia a partir del 1° de junio de 2019, dentro de sus áreas jerárquicas inferiores tiene adscritas dos Direcciones de área, la Dirección de Tecnologías de la Información, la cual tiene dos Subdirecciones de área y la Dirección de Infraestructura Tecnológica, que tiene una Subdirección de área.

1. Al comparar la estructura vigente contra la estructura que contiene el Manual de Organización Específico (MOE) de la Dirección de Infraestructura, adscrita a la Subdirección General de Tecnologías de la Información y Comunicación, se observó que el MOE de la Dirección de Infraestructura tiene dos Subdirecciones de área, cabe mencionar que el MOE de la Dirección de Infraestructura está vigente desde el 25 de octubre de 2018.

   Por lo anterior se determinó que, en el MOE de la Dirección de Infraestructura se reporta de más una Subdirección de Área, que es la Subdirección de Soporte. El detalle de la diferencia se presenta a continuación:

Estructura Orgánica del Manual de Organización Específico (25-10-2018)	**Estructura Orgánica autorizada por la SFP (01-06-2019)**
Dirección de Infraestructura (MO15.01)	**Dirección de Infraestructura Tecnológica**
- Subdirección de Infraestructura	- Subdirección de Infraestructura
- Subdirección de Soporte	No existe

2. Al comparar la estructura vigente contra la estructura que contiene el Manual de Organización Específico (MOE) de la Dirección de Tecnologías de la Información, clave MO14.01, que se encuentra vigente a partir del 25 de octubre de 2018, se determinaron diferencias en la existencia de dos departamentos de área, como se detalla a continuación:

Estructura Orgánica del Manual de Organización Específico (25-10-2018)	**Estructura Orgánica autorizada por la SFP (01-06-2019)**

Dirección de Tecnologías de la Información (MO14.01)	**Dirección de Tecnologías de la Información**
- Departamento de Desarrollo de Sistemas A	No existe
- Departamento de Desarrollo Funcional	No existe

3. Asimismo, se observó que el Manual de Políticas y Procedimientos (MPP) de la Subdirección General de Tecnologías de la Información y Comunicación (Clave: MPP14.01), que se encuentra vigente desde el 25 de octubre de 2018 y el Manual del Sistema de Gestión de Seguridad de la Información del Instituto FONACOT (Versión: MA24.00), que se encuentra vigente desde el 30 de julio de 2018, están desactualizados, ya que se encuentra alineados a la anterior Estructura Orgánica de la Subdirección General de Tecnologías de la Información y Comunicación. De igual forma, se observó que, el nombre de la Dirección de Infraestructura Tecnológica, dentro del MOE, se encuentra desactualizado, ya que aparece como la Dirección de Infraestructura. Por lo tanto, cuando se realice la actualización del MOE, se debe considerar, el nombre actual de la Dirección de Infraestructura Tecnológica con base en la Estructura Orgánica vigente.

Al respecto, la Dirección de Infraestructura Tecnológica, mediante Oficio No. DIT.004.05.2021, de fecha 05 de mayo de 2021, informó a este OIC, que la SGTIC ha llevado a cabo los trabajos para la revisión, actualización, difusión e implementación de la nueva versión de dichos manuales. Y para el Manual de Políticas y Procedimientos de la SGTIC, se optó por la estrategia de crear un manual por cada dirección como las demás Subdirecciones Generales del Instituto, es decir, se creará el Manual de Políticas y Procedimientos de la Dirección de Tecnologías de la Información y el Manual de Políticas y Procedimientos de la Dirección de Infraestructura Tecnológica, dichos manuales también se encuentran en proceso de autorización, para publicación y una vez sean publicados reemplazarán al Manual de Políticas y Procedimientos de la SGTIC. Sin embargo, a la fecha de mayo 2021, no se han llevado a cabo las actualizaciones en los Manuales antes referidos.

Acciones para contribuir a la solución de los hechos observados

Observación Correctiva:

La Subdirección General de Tecnologías de la Información y Comunicación, a través de la Dirección de Infraestructura Tecnológica y de la Dirección de Tecnologías de la Información deben realizar lo siguiente:

1. Establecer un programa con las actividades a realizar para que la Dirección de Infraestructura Tecnológica y la Dirección de Tecnologías de la Información, realicen la actualización de sus Manuales de Organización Específicos y, para que entre la Dirección de Tecnologías de la Información y la Dirección de Infraestructura Tecnológica, realicen la actualización de la nueva versión de los Manuales de Políticas y Procedimientos de cada Dirección y la actualización del Manual del Sistema de Gestión de Seguridad de la

Información, conforme a la Estructura Orgánica vigente del Instituto FONACOT. Se debe proporcionar a este OIC, el programa de trabajo calendarizado para la actualización de los manuales referidos, así como el soporte documental de las gestiones que se vayan realizando para tal fin.

2. Actualizar el nombre de la Dirección de Infraestructura Tecnológica, dentro del Manual de Organización Específico, ya que actualmente, aparece como la Dirección de Infraestructura. Esta modificación se debe incluir en el programa de trabajo antes mencionado.

Se deberá proporcionar a este OIC, el soporte documental que acredite las acciones realizadas.

Recomendación Preventiva:

La Subdirección General de Tecnologías de la Información y Comunicación a través de la Dirección de Infraestructura Tecnológica y de la Dirección de Tecnologías de la Información, deben establecer el mecanismo de control, para que sus áreas adscritas, actualicen sus Manuales de Organización Específicos, sus Manuales de Políticas y Procedimientos y el Manual del Sistema de Gestión de Seguridad de la Información, cuando el Instituto FONACOT modifique su estructura orgánica, que afecten la normativa interna en materia de tecnologías de la información, infraestructura y comunicaciones. Proporcionando a este OIC, evidencia documental correspondiente.

2. Incorrecciones de la normativa del INFONACOT en materia de seguridad de la información, con respecto del Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información

En la revisión se constató que la normativa institucional guardara la debida congruencia con el Manual Administrativo de Aplicación General en las Materias de Tecnologías de la Información y Comunicaciones y de Seguridad de la Información (MAAGMTICSI).

Al respecto, se observaron imprecisiones y omisiones de la normativa institucional.

En los puntos siguientes se presenta un cuadro comparativo de la normativa interna y el MAAGMTICSI.

1.- Clasificación de la Información

Normativa	Dice	Comentario del OIC Debe decir
Manual del Sistema de Gestión de Seguridad de la Información (MSGSI)	Págs. 2-188 Pie de página "Información Confidencial"	Págs. 2-188 Pie de página ~~"Información Confidencial"~~

El MSGSI no se encuentra en los supuestos normativos de los artículos 116 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) y 113 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP), por lo que no puede ser clasificado como **confidencial, a menos que presente el dictamen correspondiente**.

De acuerdo con el MAAGMTICSI, numeral II.C, Actividad del Proceso ASI 6, factor crítico 1, incisos j) y m) (pág. 53) la información se clasifica en **reservada** o **sensible**; sin embargo, el MSGSI no se encuentra en los supuestos normativos de los artículos 113 de la LGTAIP y 110 de la LFTAIP, por lo que no puede ser clasificado como **reservada, a menos que presente el dictamen correspondiente**.

Finalmente, la información **sensible** adquiere tal categoría cuando afecta la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste, de acuerdo con el artículo 3, fracción X de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), por lo que el MSGSI tampoco puede adquirir tal clasificación.

De lo anterior se concluye que el MGSI no contiene información confidencial, sensible o reservada, por lo que es necesario eliminar la leyenda al pie de página.

2.- Cifrado de Datos

Normativa	Dice	Comentario del OIC Debe decir
MSGSI	P. 41 4.5 [...] "Política para cifrado (POL-SEG-C- 003)". P. 47 2.5. [...] el Instituto FONACOT deberá apegarse a la Política para cifrado (POL-SEG-C-003).	*Nota: Valorar la inserción de la política de cifrado en el MSGSI.*

El MSGSI hace referencia a la "Política para cifrado (POL-SEG-C- 003)"; sin embargo, ésta no se encuentra establecida en dicho Manual. De acuerdo con el MAAGMTICSI, la política debe cumplir con los estándares 3DES de triple llave, AES-128, AES-192 y AES-256, así como redes con protocolos seguros para su envío.

Debido a que no se especifica la política para cifrado, se carece de evidencia del cumplimiento de los estándares y protocolos en la materia. Por lo anterior, se concluye que es necesario especificar la política para cifrado considerando los estándares 3DES de triple llave, AES-128, AES-192 y AES-256, así como redes con protocolos seguros para su envío.

3.- Pruebas de recuperación

Normativa	Dice	Comentario del OIC Debe decir (Texto sugerido)
MSGSI	Pág. 72 [...] El control de la realización de las copias de resguardo de	[...] El control de la realización de las copias de resguardo de información, así como la prueba **semestral** de su restauración.

	información, así como la prueba periódica de su restauración, [...].	
Manual de Políticas y Procedimientos de la Subdirección General de Tecnologías de la Información y Comunicación (MPPSGTIC)	Pág. 72 6.2. Objetivo [...] recuperar la operación normal del servicio lo antes posible [...].	6.2. Objetivo [...] **efectuar pruebas semestrales** para recuperar la operación normal del servicio lo antes posible [...].

El MAAGMTICSI, numeral II, Actividades del Proceso ADS 4, factor crítico 4 establece que se deben efectuar pruebas de recuperación, al menos **semestralmente**, al programa de continuidad para confirmar que los servicios de TIC puedan ser recuperados de forma efectiva.

4.- Responsabilidades administrativas

Normativa	Dice	Comentario del OIC Debe decir (texto sugerido)
MSGSI	Sin texto referente a las responsabilidades administrativas.	Pág. 10 El Instituto FONACOT [...] y PMO. Las disposiciones contenidas en este manual son de carácter general. El incumplimiento a las disposiciones se hará del conocimiento del Órgano Interno de Control, para que determine, en su caso, las responsabilidades que procedan de conformidad con la Ley General de Responsabilidades Administrativas.

El MAAGMTICSI, numeral II, Actividad del Proceso ASI 3, Factor Crítico "El Responsable de la seguridad de la información de la Institución", establece lo siguiente:

13. Hacer del conocimiento del órgano interno de control en la Institución y/o, cuando corresponda, de las autoridades que resulten competentes, el incumplimiento al SGSI a efecto de que se determinen, en su caso, las responsabilidades que procedan en términos de los ordenamientos legales aplicables.

La versión vigente del MSGSI no considera la LGRA, por lo que omite el apercibimiento de que un incumplimiento del SGSI deriva en responsabilidades administrativas.

Las omisiones e imprecisiones de la normativa interna en materia de seguridad de la información, genera a su vez, una inobservancia del *ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias* (Acuerdo), donde se establece, en el artículo 1, la observancia **obligatoria** del mismo en la Administración Pública Federal.

Acciones para contribuir a la solución de los hechos observados

Observación Correctiva

1 a 4.- La Subdirección General de Tecnologías de la Información y Comunicación debe analizar y aplicar los cambios que resulten procedentes, con base en su análisis del MAAGMTICSI y turnar evidencia documental al OIC de esta actividad.

Recomendación Preventiva

1 a 4.- La Subdirección General de Tecnologías de la Información y Comunicación debe analizar la factibilidad de establecer un procedimiento (listado), que asegure la debida observancia del MAAGMTICSI en la normativa interna en materia de seguridad de la información y enviar al OIC evidencia documental que compruebe las acciones realizadas.

3. Falta de Programa Anual de Trabajo de la Dirección de Infraestructura Tecnológica y de la Dirección de Tecnologías de la Información orientado a las funciones propias del Área y debidamente formalizado

1. Del análisis a la información proporcionada por la Dirección de Infraestructura Tecnológica (DIT), relativa a ocho diferentes Programas Anuales de Trabajo, uno por cada servicio contratado con terceros (Axtel, BSS, Hola Innovación, IQSEC, JR Intercontrol, Metronet, Tesecom y Tsystems), en donde se contó con un tablero de control de proyectos (contratos en operación); asimismo, se establecieron fechas de elaboración y de actualización y firmas de aceptación por parte de la persona que elaboró, revisó y autorizó el documento, de manera general, sin especificar a las personas responsables de cada actividad.

   Al respecto, se observó que estos ocho Programas Anuales de Trabajo del ejercicio 2020, no se encuentran debidamente formalizados por el personal encargado de realizar las actividades, en cuanto a la elaboración, supervisión, revisión y en su caso visto bueno; asimismo, no se especifica quienes son los responsables de ejecutar cada actividad del proyecto, así como el establecimiento de metas de desempeño.

   Lo anterior, debido a que corresponden a las actividades realizadas por los proveedores y no por la DIT. Adicionalmente, se observó que, la Dirección de Infraestructura Tecnológica, no contó con un Programa Anual de Trabajo del ejercicio 2020, orientado a las funciones propias del área y como responsable de la operación de Infraestructura Tecnológica del Instituto, que coadyuve en el cumplimiento de los objetivos de la Subdirección General de Tecnologías de la Información y Comunicación del Instituto FONACOT, situación que no permitió verificar su grado de alineación y vinculación con el cumplimiento de la visión, misión y objetivos estratégicos del INFONACOT.

Al no contar la DIT con un Programa Anual de Trabajo, orientado a las funciones propias del área, debidamente formalizado, que le permita contar con un mecanismo de control para medir el desempeño de sus actividades, se observan debilidades de control interno para verificar que sus funciones se encuentren alineadas con los objetivos y metas Institucionales, así como, el cumplimiento de cada una de sus funciones descritas en el Manual de Organización Específico de la Dirección de Infraestructura (MO15.01), vigente desde el 25 de octubre de 2018.

2. La Dirección de Tecnologías de la Información informó que con apoyo de los proveedores Merr Informática, S. de R.L. de C.V., It Era, S.A. de C.V. y Arduus TI, S.C., elaboró el Plan de Trabajo asociado al Servicio Integral para la Implementación, Puesta en Marcha y Operación de una Oficina de Administración de Proyectos Administrada (PMO), que corresponde a las actividades realizadas por los proveedores para administrar su servicio contratado con el Instituto FONACOT.

   Por lo que se determinó que, la Dirección de Tecnologías de la Información, no contó con un Programa Anual de Trabajo del ejercicio 2020, que le permita contar con un mecanismo de control para medir el desempeño de sus actividades y funciones propias y que coadyuve en el cumplimiento de los objetivos de la Subdirección General de Tecnologías de la Información y Comunicación del Instituto FONACOT, situación que no permitió verificar su contribución para lograr el cumplimiento de la visión, misión y objetivos estratégicos del INFONACOT.

La falta de los Programas de Trabajo de las dos Direcciones mencionadas, se sustenta de conformidad con lo estipulado en el Acuerdo por el que se emiten las Disposiciones y el Manual Administrativo de Aplicación General en Materia de Control Interno en el artículo 9. Normas Generales, Principios y Elementos de Control Interno, Segunda Norma. Administración de Riesgos, Numeral 6. Definir Metas y Objetivos Institucionales, que establece la necesidad de formular un Programa Anual de Trabajo, donde se señalen objetivos, metas y actividades, que permitan evaluar el desempeño de dicha unidad administrativa.

Acciones para contribuir a la solución de los hechos observados

Recomendaciones Al Desempeño:

La Subdirección General de Tecnologías de la Información y Comunicación, a través de la Dirección de Infraestructura Tecnológica y la Dirección de Tecnologías de la Información, debe establecer su respectivo Programa Anual de Trabajo, debidamente alineado a los aspectos estratégicos de la Subdirección General de Tecnologías de la Información y Comunicación, contemplando la definición de objetivos y metas, alineados al cumplimiento de la visión, misión y objetivos del INFONACOT, así como las diferentes actividades, los responsables de su ejecución, su debida calendarización y formalización, a fin de mejorar la eficiencia y el control interno y tener constancia de las acciones realizadas para futuras revisiones.

Dicho Programa deberá ser proporcionado al OIC, así como el soporte documental de las gestiones que se vayan realizando para tal fin.

Recomendación Preventiva:

Se recomienda que la Subdirección General de Tecnologías de la Información y Comunicación, a través de la Dirección de Tecnologías de la Información y de la Dirección de Infraestructura Tecnológica, implementen un Tablero de Indicadores alineado con el Programa Anual de Trabajo y con los procesos bajo su responsabilidad, señalando los mecanismos de seguimiento y control que aseguren su cumplimiento. Deberá ser proporcionado al OIC, el soporte documental de las gestiones que se vayan realizando para tal fin.

4. Falta de Soporte documental que demuestre la Metodología empleada para su diseño y para los resultados obtenidos derivado de la aplicación de Indicadores de rendimiento en la Subdirección de Infraestructura

A efecto de verificar que la Subdirección de Infraestructura, haya dado cumplimiento a la función número 5, del Manual de Organización Especifico de la Dirección de Infraestructura, mediante oficio No. OIC/14/120/2021/143, de fecha 23 de abril de 2021, se solicitó al área auditada, se proporcionara el diseño y evaluación a los indicadores de rendimiento para los servicios de software, hardware y telecomunicaciones, que fueron aplicados en el ejercicio 2020, en materia de responsabilidad de la Subdirección de Infraestructura.

En respuesta mediante oficio No. DIT.004.05.2021, de fecha 05 de mayo de 2021, el área auditada proporcionó los indicadores de rendimiento correspondientes al periodo de diciembre de 2020, de acuerdo a lo siguiente:

- Reporte de disponibilidad de enlaces.
- Reporte de disponibilidad de infraestructura.

Del análisis a la evidencia documental proporcionada de los indicadores de rendimiento en los reportes antes mencionados, se observó que, estos no describen la metodología empleada para su diseño, el algoritmo utilizado, la parametrización, la unidad de medida y la frecuencia de emisión, así como los parámetros para determinar la semaforización.

Por otro lado, del análisis a las respuestas a la pregunta número 19 del Cuestionario de Control Interno de la Dirección de Infraestructura Tecnológica y a la pregunta número 13 del Cuestionario de Control Interno de la Subdirección de Infraestructura, se contestó en ambos Cuestionarios que, como evidencia de la relación de indicadores de rendimiento, son los que se especifican en el MAAGTICSI, referentes a indicadores de eficiencia. Sin embargo, revisando lo especificado en el MAAGTICSI, no corresponden a los mismos indicadores a los que hace referencia la función 5 de la Subdirección de Infraestructura, del Manual de Organización Especifico de la Dirección de Infraestructura, ya que los indicadores a los que hace referencia el MAAGTICSI, corresponden a indicadores de eficiencia para alcanzar los objetivos de seguridad de la información.

Por lo anterior, no se proporcionó evidencia documental de la metodología empleada para su diseño, algoritmos, unidad de medida y frecuencia, así como los parámetros para determinar la semaforización, que demuestre los resultados obtenidos de la aplicación de los indicadores de rendimiento para los servicios de software, hardware y telecomunicaciones para el seguimiento oportuno y óptima atención al usuario, lo anterior, con fundamento en el Numeral X Objetivo y Funciones, punto 1.1.2 Subdirección de Infraestructura, Función número 5, del Manual de Organización Especifico de la Dirección de Infraestructura, que a la letra menciona lo siguiente:

"5. Diseñar y evaluar los indicadores de rendimiento para los servicios de software, hardware y telecomunicaciones para el seguimiento oportuno y óptima atención al usuario (definición de niveles de servicio y criterios de prioridades)."

Acciones para contribuir a la solución de los hechos observados

Observación Correctiva:

La Subdirección General de Tecnologías de la Información y Comunicación, a través de la Dirección de Infraestructura Tecnológica, debe proporcionar lo siguiente:

1. El soporte documental (la metodología empleada para su diseño, algoritmos, unidad de medida y frecuencia, así como los parámetros para determinar la semaforización), de los indicadores de rendimiento para los servicios de software, hardware y telecomunicaciones, en donde se puedan identificar los resultados obtenidos (evaluación de indicadores de rendimiento).

Recomendaciones

Al Desempeño:

El Subdirector General de Tecnologías de la Información y Comunicación, debe establecer mecanismos de control, en coordinación con el Director de Infraestructura Tecnológica y el Subdirector de Infraestructura, donde se identifiquen y den seguimiento puntual a sus funciones que tienen asignadas en su Manual de Organización Específico de la Dirección de Infraestructura, de lo cual deberá dejar constancia de las acciones realizadas para futuras revisiones, asimismo, remitir a esta instancia fiscalizadora el soporte documental de las acciones realizadas para tal fin.

Preventiva:

La Subdirección General de Tecnologías de la Información y Comunicación, a través de la Dirección de Infraestructura Tecnológica, deben realizar la acción siguiente:

1.- Realizar un tablero de control, con corte al último día hábil de cada mes, del estatus del seguimiento de los indicadores de rendimiento para los servicios de software, hardware y telecomunicaciones, donde se definan los niveles de servicio y los criterios de prioridades.

Remitir, a esta instancia fiscalizadora, el soporte documental de las acciones realizadas para tal fin.

5. Falta de Actualización del Inventario de Procesos que Integran el Plan de Continuidad de Negocios, al Inventario Global de Procesos del Instituto y Métricas fuera de los Niveles de Tolerancia establecidos para los Riesgos Tecnológicos

1. Falta de actualización del inventario de procesos que integran el Plan de Continuidad de Negocios del Instituto, al inventario global de procesos del Instituto

Derivado de la Auditoría en materia de Riesgos No. 04/2020, realizada por la Dirección de Auditoría Interna del Instituto FONACOT, en el ejercicio 2020, en la que determinó la siguiente observación: *"Falta de Actualización a la métrica Riesgos No Discrecionales"*, en el Informe de dicha Auditoría se menciona que, como Plan de acción, la SGTIC, presentó el oficio No. SGTIC.402.12.1220, de fecha 22 de diciembre de 2020, en el cual informa lo siguiente, sin definir una fecha para su atención.

- Se han llevado a cabo las acciones correspondientes para estabilizar los niveles reportados ante el CAIR, a través de la matriz de indicadores de riesgos, mismos que fueron establecidos por el CAIR, basándose en estándares para instituciones bancarias. Asimismo, se comenta que existen cinco de un total de veinte indicadores que rebasan la tolerancia establecida (de los riesgos tecnológicos).

Es preciso señalar, que dicha observación fue realizada a la SGTIC y, por ende, es la responsable de dar atención a la misma.

En ese sentido, en la 5° Sesión Ordinaria del Comité de Administración Integral de Riesgos (CAIR), celebrada con fecha 26 de mayo de 2021, respecto al monitoreo, seguimiento y cumplimiento del nivel de tolerancia para los riesgos no discrecionales y para los riesgos tecnológicos, presentados de manera mensual en las Sesiones Ordinarias del CAIR, se identificó lo siguiente:

La métrica de exposición total a Riesgos No Discrecionales (Operacionales), se encuentra desactualizada desde enero 2020 a la fecha de elaboración de esta observación. Lo anterior, debido a que, al cierre del mes de mayo 2021, hace falta que la Subdirección General de Tecnologías de la Información y Comunicación (SGTIC), integre la actualización del inventario de procesos que componen el Plan de Continuidad de Negocios del Instituto, al inventario global de procesos del Instituto. Cabe aclarar que, este inventario, identifica la descripción de cada proceso y procedimiento descrito en la normativa vigente, así como la inclusión de diagramas de flujo de dichos procesos.

Lo anterior, de conformidad con las fracciones XI.2.2. y XI.2.3., del Manual de Administración Integral de Riesgos del Instituto FONACOT, Clave: MA23.03, que a la letra dice:

> *"Una vez que se tienen identificados y documentados los procesos del Instituto FONACOT,* ***se procederá en conjunto con las unidades administrativas*** *a la identificación de riesgos operacionales implícitos a cada proceso, así como al establecimiento de puntos de control para cada riesgo. Derivado de los puntos anteriores, se deberán establecer los Niveles de Tolerancia al Riesgo para cada tipo de riesgo identificado, definiendo sus causas, orígenes o Factores de Riesgo".*

2. Métricas fuera de los niveles de tolerancia establecidos para los riesgos tecnológicos

Considerando lo antes expuesto y, respecto de los niveles de tolerancia de riesgos tecnológicos, a la fecha de mayo 2021, se tiene la siguiente actualización:

- Cuatro indicadores que evalúan al riesgo tecnológico en el Instituto, se encuentran fuera del nivel de tolerancia (métricas KRI0008, KRI0026, KRI0027 y KRI0030), como a continuación se muestra:

Nivel de Tolerancia – Riesgo Tecnológico			
Inobservancia	**Métrica**	**Niveles de Tolerancia Dic-2020**	**Nivel de Tolerancia permitido**
1	Plataformas tecnológicas obsoletas y/o desactualizadas (aplicativos KRI0008)	**25.0%**	<=2.0%
2	Data base managers (DBM) con versiones de tecnología obsoletas o no soportadas (KRI0026)	**14.0%**	<= 5.0%
3	Aplicaciones obsoletas o no soportadas (KRI0027)	**25.0%**	<= 2.0%
4	Data base managers (DBM) sin cobertura de parches de seguridad (KRI0030)	**14.0%**	<= 2.0%

Lo anterior, de conformidad con la fracción XII.3. Administración de Niveles de Tolerancia, del Manual de Administración Integral de Riesgos del Instituto FONACOT, Clave: MA23.03, que a la letra dice: "Mensualmente se actualiza la información relativa a los niveles de tolerancia del riesgo tecnológico que se encuentran en el "Anexo D – Niveles de Tolerancia de Riesgo Tecnológico" de este documento".

Derivado de lo antes mencionado, la SGTIC, en la Carpeta de la 5° Sesión Ordinaria de 2021 del CAIR, celebrada con fecha 26 de mayo de 2021, informó lo siguiente:

a) Para los indicadores KRI0008 y KRI0027, actualmente CREDERE se encuentra con una versión desactualizada, pero soportada por el aplicativo "Topaz". La remediación para estos indicadores se requiere la actualización del aplicativo a la versión 19.C, lo cual se está analizando las diferentes opciones con proveedores que prestan dichos servicios especializados para poder realizar la actualización, sin embargo, es importante considerar que llevar a cabo dicha actualización requeriría la interrupción del sistema que implicaría que el sistema no estuviera operando, deteniendo la colocación de créditos.

b) Para los indicadores KRI0026 y KRI0030, actualmente Crédito Seguro (sucursales) opera bajo la plataforma Windows Server 2012 R2 y SQL Server Enterprise 2012. Como parte del proceso de remediación de tecnologías obsoletas, se tiene planeada llevar a cabo la migración y actualización del sistema operativo a Windows Server 2019 y motor de base de datos a SQL Server 2019 de la plataforma Crédito Seguro; la cual está planeada que concluya el primer semestre del año en curso (2021). Cabe mencionar que Microsoft ha dado a conocer la nueva fecha de fin de soporte extendido para Windows Server 2012 que es el 10 de octubre de 2023.

- Data base managers (DBM) con versiones de tecnología obsoletas o no soportadas. (KRI0026)
- Data base managers (DBM) sin cobertura de parches de seguridad. (KRI0030)

Para estos indicadores tecnológicos se planea llevar a cabo la migración y actualización del sistema operativo a Windows Server 2019 y motor de base de datos a SQL Server 2019 de la plataforma Crédito Seguro.

En ese orden de ideas, se observa que las cuatro métricas se encuentran fuera de los niveles de tolerancia establecidos para los riesgos tecnológicos, en consecuencia, se encuentra comprometida la seguridad del Instituto FONACOT, ya que influye en su operación ordinaria y a la fecha de mayo 2021, no se ha tenido una respuesta por parte de la SGTIC, que atienda con precisión y por completo, el requerimiento.

Asimismo, el acuerdo del CAIR, No. CAIR/026/2020, a la letra establece lo siguiente:

> *"El Comité de Administración Integral de Riesgos del Instituto del Fondo Nacional para el Consumo de los Trabajadores, con base en lo dispuesto en el Artículo 79, último párrafo de las Disposiciones de Carácter General Aplicables a los Organismos de Fomento y Entidades de Fomento, y derivado de que la Subdirección de Riesgo Tecnológico fue eliminada de la estructura orgánica de la UAIR, como consecuencia de las medidas de austeridad implementadas en 2019, solicita el apoyo auxiliar de la Subdirección General de Tecnologías de la Información y Comunicación y la Oficina del Abogado General, para llevar acabo las funciones relativas a la administración del riesgo tecnológico y riesgo legal, respectivamente, siempre y cuando en las actividades que dichas áreas auxilien, no se susciten conflictos de interés."*

Por lo anterior y con la finalidad de que la exposición a los riesgos tecnológicos regresen a los niveles permisibles, es importante que se considere lo antes posible, llevar a cabo la actualización del aplicativo a la versión 19.C, y llevar a cabo la migración y actualización del sistema operativo a Windows Server 2019 y motor de base de datos a SQL Server 2019 de la plataforma Crédito Seguro; para que se minimice de manera considerable la exposición a los riesgos tecnológicos a los que está expuesto actualmente el Instituto FONACOT.

Acciones para contribuir a la solución de los hechos observados

Observación Correctiva:

La Subdirección General de Tecnologías de la Información y Comunicación, debe realizar lo siguiente:

1. Las actualizaciones y migraciones necesarias, para dar cumplimiento con los niveles de tolerancia permisibles para los riesgos tecnológicos. Por lo anterior, la SGTIC, debe elaborar un programa de trabajo calendarizado, para llevar a cabo la actualización del aplicativo a la versión 19.C y del sistema operativo a Windows Server 2019 y motor de base de datos a SQL Server 2019 de la plataforma Crédito Seguro, así como la migración y así poder fijar un plazo para que, la SGTIC de solución y cumplimiento a los 4 indicadores de riesgo tecnológico (KRI0008, KRI0026, KRI0027 y KRI0030), y éstos regresen a los valores permisibles tolerables, para mitigar los riesgos a los que está expuesto actualmente el Instituto FONACOT y que esta situación no comprometa, en ningún momento, la seguridad del Instituto. Para lo cual, deberá proporcionar a este OIC, el Programa de Trabajo calendarizado, debidamente formalizado con las actividades a realizar y con el personal responsable, así como el soporte documental que acredite las acciones realizadas.

Recomendaciones

Al Desempeño:

La Subdirección General de Tecnologías de la Información y Comunicación, debe implementar un mecanismo de seguimiento y control, para que se puedan atender puntualmente los requerimientos necesarios, para cumplir con la métrica del nivel de tolerancia de los riesgos tecnológicos, identificando y dando seguimiento a los incidentes tecnológicos detectados y los análisis de vulnerabilidades que puedan obstaculizar el tener en niveles permisibles la métrica del nivel de tolerancia para los riesgos tecnológicos. De lo anterior, deberá proporcionar a este OIC, evidencia documental del mecanismo de seguimiento y control implementado, así como el soporte documental de las acciones realizadas para tal fin.

Preventiva:

La Subdirección General de Tecnologías de la Información y Comunicación, debe realizar lo siguiente:

1. Realizar las acciones necesarias, de acercamiento con la Subdirección General de Administración de Riesgos, para que ambas áreas, en común acuerdo, lleguen a una solución, y se pueda justificar quien es el área responsable, para solventar lo observado, que es el realizar el análisis, identificar, documentar y mapear al 100% (actualización al inventario global) de procesos de cada Unidad Administrativa del Instituto FONACOT. Se debe proporcionar a este OIC, evidencia documental que acredite las acciones realizadas para tal fin.

f) Monto, por justificar, aclarar o recuperar

No se determinaron montos, por justificar, aclarar o recuperar

g) Resumen (número de recomendaciones y acciones)

Se determinaron 5 cédulas de resultados finales, de las cuales, en 4 corresponden a observaciones correctivas y recomendaciones y la restante a recomendaciones al desempeño y preventivas.

h) Opinión o dictamen

El presente se emitió el 30 de junio de 2021, fecha de conclusión de los trabajos de auditoría. Éste se realizó con la información proporcionada por el área auditada, de cuya veracidad es responsable; sin embargo, esta área fiscalizadora, evaluará la información proporcionada en el seguimiento de las acciones determinadas.

La revisión se realizó al desempeño de la Subdirección General de Tecnologías de la Información y Comunicación, al verificar su eficiencia, eficacia, economía y efectividad en el cumplimiento de metas y objetivos, verificando que su desempeño se haya realizado con apego a lo establecido en la normativa aplicable del Instituto FONACOT.

Los resultados obtenidos en la auditoría, evidencian debilidades de control en la supervisión de las actividades y procesos inherentes al desempeño de la Subdirección General de Tecnologías de la Información y Comunicación.

En opinión de este Órgano Interno de Control, se recomienda llevar a cabo acciones para mejorar el control interno existente y reforzar la supervisión e implementación de controles internos por parte del área auditada a efecto de que se apliquen de manera efectiva los procedimientos a cargo de la Subdirección General de Tecnologías de la Información y Comunicación, constatando el apego al marco normativo aplicable.

Por lo tanto, es necesario corregir y prevenir las inconsistencias detectadas, atendiendo con oportunidad las recomendaciones establecidas por éste Órgano Interno de Control, lo cual permitirá desempeñar, de manera eficiente, un mejor control y una adecuada administración de sus operaciones.