



15 ENE. 2025

RECIBIDO
UNIDAD PARA LA ADMINISTRACIÓN INTEGRAL DE RIESGOS

Dirección de Auditoría Interna
Oficio No. DAI/009/01/2025
Asunto: Informe de Auditoría de Administración Integral de Riesgos 04/2024



Ciudad de México 08 de enero de 2025

C.P. Laura Fernanda Campaña Cerezo
Directora General

15 ENE. 2025



C. P. Mariel Karina Zamora Nava
Coordinadora General de Crédito y Finanzas

RECIBIDO

Lic. Salvador Gazca Herrera
Coordinador General Comercial

COORDINACIÓN GENERAL COMERCIAL

15 ENE. 2025

RECIBIDO

Mtro. Agni Rodrigo Cerda Mendoza
Titular de la Unidad para la Administración Integral de Riesgos

12:31
OFICINA DEL ABOGADO GENERAL

Mtro. Erick Morgado Rodríguez
Abogado General

Ing. Ricardo Oria Esquivel
Subdirector General de Tecnologías de la Información y Comunicación



Lic. Jazmín García Juárez
Subdirectora General de Administración

15 ENE. 2025
12:32 12:31

RECIBIDO

Lic. Jaime Francisco Ricci Rojas
Subdirector General de Contraloría, Planeación y Evaluación

COORDINACIÓN GENERAL DE CRÉDITO Y FINANZAS

PRESENTE.

En relación con la orden de auditoría notificada mediante oficio DAI/332/10/2024 de fecha 04 de octubre del 2024, con fundamento en lo dispuesto en el artículo 69 de las Disposiciones de Carácter General Aplicables a los Organismos de Fomento y Entidades de Fomento; 73, fracciones I, III, IV, V, VI, VII, VIII y X del Estatuto Orgánico del Instituto FONACOT, y al Programa Anual de Trabajo 2024 autorizado por el Comité de Auditoría, Control y Vigilancia del Instituto FONACOT, se adjunta de forma electrónica el Informe de Auditoría de Administración Integral Riesgos 04/2024.

Como parte del contenido del informe se presenta el detalle de las observaciones determinadas, que previamente fueron comunicadas a los responsables de su atención, las cuales se refieren a:

| No. | DESCRIPCIÓN DE LA OBSERVACIÓN/RECOMENDACIÓN |
|-----|--|
| 1 | Vulnerabilidad en equipos de cómputo en sucursales. |
| 2 | Deficiencia en seguimiento a vulnerabilidades. |
| 3 | Seguridad y mantenimiento insuficiente al interior de las sucursales. |
| R1 | Reforzar la capacitación al analista del Front en sucursales. |
| R2 | Homogeneidad de las bases de datos históricas sobre las resoluciones judiciales y administrativas. |



Plaza de la Republica No.32 Col. Tabacalera CP. 06030, Alcaldía Cuauhtémoc, Ciudad de México Tel: 55 53 53 4400 inform@fonacot.gob.mx

15 ENE. 2025

13:59
RECIBIDO
SUBDIRECCIÓN GENERAL DE ADMINISTRACIÓN



Trabajo
Secretaría del Trabajo
y Previsión Social

fonacot



Por lo anterior, se solicita gire sus amables instrucciones a quien considere pertinente, con la finalidad de que implementen las medidas correctivas y preventivas acordadas, conforme a los términos y plazos establecidos en las cédulas de observaciones y/o recomendaciones correspondientes.

A partir de la fecha establecida para su atención, ésta Dirección realizará el seguimiento a las observaciones hasta su solventación.

Sin otro particular aprovecho la ocasión para enviar un cordial saludo

ATENTAMENTE

Lic. Mariana Isabel Flores Villanueva
Coordinadora Técnica Administrativa de Alta Responsabilidad,
Encargada y Responsable de los asuntos de la Dirección de Auditoría Interna
con fundamento en el artículo 82 del Estatuto Orgánico del Instituto FONACOT
y el oficio DG/017/2024 de fecha 29 de febrero de 2024



ORGANO INTERNO DE CONTROL EN EL
INSTITUTO FONACOT
(HORA: 13:34 RECIBE: EDILER S. ARGUERO
RSP)

C.c.e.p. Ing. Santiago Carlos Macías Herrera. - Presidente Suplente del Comité de Auditoría, Control y Vigilancia del Instituto FONACOT
Lic. Noé García Ortiz. - Titular del Órgano Interno de Control en el Instituto FONACOT

HJRR/JEGT



2025
Año de
La Mujer
Indígena



INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES

INFORME DE AUDITORÍA ADMINISTRACIÓN INTEGRAL DE RIESGOS 04/2024

Nivel de Riesgo: Bajo

Fecha de Término de Trabajo de Campo: 30 de diciembre 2024

Opinión de Auditoría: Estable

08 de enero de 2025





ÍNDICE

| | | |
|-----|--|----|
| 1. | RESUMEN EJECUTIVO | 3 |
| 1.1 | ANTECEDENTES..... | 3 |
| 1.2 | MARCO NORMATIVO..... | 3 |
| 1.3 | OBJETIVO | 3 |
| 1.4 | ALCANCE | 3 |
| 1.5 | CONCLUSIÓN | 4 |
| 2. | RESUMEN DE CALIFICACIONES..... | 5 |
| 3. | RESUMEN DE OBSERVACIONES | 6 |
| 4. | OBSERVACIONES ABIERTAS DE AUDITORÍAS DE RIESGOS DE REVISIONES ANTERIORES | 7 |
| 5. | EVENTO RELEVANTE | 8 |
| 6. | PERFIL DE LAS ÁREAS INVOLUCRADAS EN LA AUDITORÍA..... | 9 |
| 7. | DEFINICIONES DE LA CALIFICACIÓN DE AUDITORÍA..... | 10 |
| 8. | LISTA DE DISTRIBUCIÓN | 11 |
| 9. | CÉDULAS DE OBSERVACIONES..... | 12 |
| | OBSERVACIÓN DE AUDITORÍA #1 | 13 |
| | OBSERVACIÓN DE AUDITORÍA #2 | 17 |
| | OBSERVACIÓN DE AUDITORÍA #3 | 21 |
| | RECOMENDACIÓN DE AUDITORÍA #1 | 25 |
| | RECOMENDACIÓN DE AUDITORÍA #2..... | 28 |



1. RESUMEN EJECUTIVO

1.1 ANTECEDENTES

La Dirección de Auditoría Interna en cumplimiento al Plan Anual de Trabajo 2024, emitió la Orden de Auditoría en Materia de Administración Integral de Riesgos 04/2024, con oficio DAI/332/10/2024 de fecha 04 de octubre de 2024, la cual se ejecutó del 7 de octubre al 31 de diciembre de 2024 y se notificó a las siguientes áreas:

- Unidad para la Administración Integral de Riesgos
- Coordinación General de Crédito y Finanzas
- Coordinación General Comercial
- Abogado General
- Subdirección General de Contraloría, Planeación y Evaluación
- Subdirección General de Tecnologías de la Información y Comunicación

1.2 MARCO NORMATIVO

Con base en el artículo 69 de la Disposiciones de Carácter General Aplicables a los Organismos de Fomento y Entidades de Fomento (Disposiciones) señala: “Los Organismos de Fomento y Entidades de Fomento deberán contar con un área de Auditoría Interna independiente de las Unidades de Negocio y administrativas, cuyo responsable o responsables serán designados por el Consejo o, en su caso, por el Comité de Auditoría, que lleve a cabo, cuando menos, una vez al año o al cierre de cada ejercicio una auditoría de Administración Integral de Riesgos que contemple, entre otros,…”

1.3 OBJETIVO

Verificar que la Administración Integral de Riesgos se desarrolle en apego a lo establecido en las Disposiciones de Carácter General aplicables a los Organismos de Fomento y Entidades de Fomento, así como con objetivos, lineamientos y políticas en la materia aprobados por el Consejo Directivo del Instituto FONACOT y determinar la suficiencia, integridad, consistencia y grado de integración de los sistemas de procesamiento de información y para el análisis de riesgos. Así como la consistencia, precisión, integridad, oportunidad y validez de las fuentes de información y bases de datos utilizadas en los modelos de medición.

1.4 ALCANCE

La auditoría fue dirigida a diversos aspectos de la Administración Integral de Riesgos con fundamento en el artículo 69 de las Disposiciones y demás normativa aplicable, para lo cual se revisaron los siguientes aspectos, correspondientes al periodo del 1 de octubre de 2023 al 30 de septiembre de 2024:

| No. | TEMAS | DISPOSICIONES ART. 69 |
|-----|--|-----------------------|
| 1 | Independencia de las Unidades de Negocio y Estructura Organizacional. | Fracc. II |
| 2 | Capacitación de personal | Fracc. II |
| 3 | Observancia de objetivos y lineamientos en la Administración Integral de Riesgos | Fracc. I |
| 4 | Objetivos, lineamientos, políticas y manuales de la UAIR | Fracc. I |





| No. | TEMAS | DISPOSICIONES ART. 69 |
|-----|--|-----------------------|
| 5 | La administración del riesgo tecnológico | Fracc. III |
| 6 | Fuentes de Información de la UAIR y sistemas para la medición de riesgos | Fracc. III y IV |
| 7 | Integridad de la base de datos de pérdidas por riesgos operacional | Fracc. IV |
| 8 | Modificaciones a los Modelos de Medición de Riesgos | Fracc. V |
| 9 | Modelos de Medición de Riesgos Utilizados por las Unidades de Negocio | Fracc. VI |
| 10 | Actualización y Observancia de la Política de Apetito de Riesgos | Fracc. VII |
| 11 | Visita a Sucursales (Riesgo Operativo en el otorgamiento de Crédito) | Fracc. IV |
| 12 | Revisión del Centro de Datos principal del Instituto FONACOT | Fracc. III |
| 13 | Desarrollo de las funciones del área de Contraloría Interna. Artículo 172 de las Disposiciones | Fracc. VIII |

1.5 CONCLUSIÓN

Derivado del análisis realizado durante la presente auditoría, se identificaron algunos aspectos en los que se requiere fortalecer y dar seguimiento, con la finalidad de reducir los riesgos a los que está expuesto el Instituto.

Lo anterior, implementando medidas y controles por parte de las áreas responsables, para así evitar vulnerabilidades en los equipos de cómputo en sucursales, dar seguimiento oportuno a las debilidades identificadas, salvaguardar la seguridad y mantenimiento a los espacios destinados al interior de las sucursales, así como reforzar la capacitación al analista del Front en sucursales.

En lo general, se cumple con el objetivo de la auditoría en materia de Administración Integral de Riesgos, así como lo establecido en el artículo 69 las Disposiciones, por lo tanto, con la finalidad de prevenir, minimizar y corregir las debilidades o inconsistencias referidas, se exhorta a llevar a cabo medidas preventivas y correctivas, para el debido cumplimiento de la normatividad interna y externa aplicable al Instituto.

En la siguiente tabla se observa el nivel de riesgo por área, de acuerdo a las observaciones detectadas.

| ÁREA | CALIFICACIÓN 04/2024 | NIVEL DE RIESGO |
|--|---|-----------------|
| Subdirección General de Tecnologías de la Información y Comunicación | Requiere mejorar – Estable ■ | Moderado |
| Subdirección General de Administración | Requiere Mejorar – Solución Oportuna ▲ | Bajo |
| Coordinación General Comercial | Requiere Mejorar – Solución Oportuna ▲ | Bajo |
| Oficina del Abogado General | Satisfactorio – Estable ■ | Bajo |

El nivel de riesgo se refiere a la importancia en materia de administración de riesgos que tiene esa área para el INFONACOT en el periodo revisado y ampliado si fue el caso. Ese dato debe verse en conjunto con la observación correspondiente y se vincula a dicha área.





2. RESUMEN DE CALIFICACIONES

Se indican únicamente las áreas donde se identifican observaciones de la que son titulares para su atención, o bien porque tienen mayor facilidad para atender de forma efectiva.

| ÁREA RESPONSABLE DE LA OBSERVACIÓN | CALIFICACIÓN AUDITORÍA 04/2024 | OBSERVACIONES/RECOMENDACIONES DE LA AUDITORÍA |
|--|---|--|
| Subdirección General de Tecnologías de la Información y Comunicación | Requiere mejorar – Estable ■ | 1. Vulnerabilidad en equipos de cómputo en sucursales. |
| Subdirección General de Tecnologías de la Información y Comunicación | Requiere Mejorar – Solución Oportuna ▲ | 2. Deficiencia en seguimiento a vulnerabilidades. |
| Subdirección General de Administración /Dirección de Recursos Materiales y Servicios Generales | Requiere Mejorar – Solución Oportuna ▲ | 3. Seguridad y mantenimiento insuficiente al interior de las sucursales. |
| Coordinación General Comercial | Requiere Mejorar – Solución Oportuna ▲ | R1. Reforzar la capacitación al analista del Front en sucursales. |
| Oficina del Abogado General Dirección de lo Contencioso/Dirección de Asuntos Laborales | Satisfactorio – Estable ■ | R2. Homogeneidad de las bases de datos históricas sobre las resoluciones judiciales y administrativas. |





3. RESUMEN DE OBSERVACIONES

Conforme a lo indicado en la sección de Conclusión; la clasificación de observación en esta revisión fue hecha en función a su criticidad en términos de cumplimiento regulatorio, impacto en materia de riesgos y en caso de que aplique las dependencias existentes tanto en su causa raíz como las acciones necesarias para su adecuada atención, solicitando, en cualquier caso, un plan de acción.

| No. | OBSERVACIÓN | ÁREA DONDE SE IDENTIFICA LA OBSERVACIÓN | FECHA COMPROMISO DEL ÁREA | ACCIONES ESPECÍFICAS PARA EL CIERRE DE LA OBSERVACIÓN* |
|-----|--|--|---------------------------|--|
| 1 | Vulnerabilidad en equipos de cómputo en sucursales. | Subdirección General de Tecnologías de la Información y Comunicación | 21 de marzo de 2025 | Evidencia de la ejecución del Plan de Trabajo. |
| 2 | Deficiencia en seguimiento a vulnerabilidades. | Subdirección General de Tecnologías de la Información y Comunicación | 04 de abril de 2025 | Evidencia de seguimiento a la vulnerabilidad observada e implementación del formato único. |
| 3 | Seguridad y mantenimiento insuficiente al interior de las sucursales. | Subdirección General de Administración /Dirección de Recursos Materiales y Servicios Generales | 31 de enero de 2025 | Evidencia de la habilitación de los detectores de humo (cambio de pilas). |
| R1 | Reforzar la capacitación al analista del Front en sucursales. | Coordinación General Comercial | 21 de marzo de 2025 | Evidencia de las capacitaciones ejecutadas. |
| R2 | Homogeneidad de las bases de datos históricas sobre las resoluciones judiciales y administrativas. | Oficina del Abogado General Dirección de lo Contencioso/Dirección de Asuntos Laborales | 31 de enero de 2025 | 2. Base de datos de con identificación de los eventos de pérdidas por año. 3. Evidencia de respuesta a la Dirección de Riesgos No Discrecionales sobre eventos de pérdidas. |

NOTA: Las observaciones detalladas y las respuestas obtenidas se anexan al informe, en la sección correspondiente.



4. OBSERVACIONES ABIERTAS DE AUDITORÍAS DE RIESGOS DE REVISIONES ANTERIORES

Actualmente, de las Auditorías de Administración Integral de Riesgos realizadas en revisiones anteriores, se puede observar que sólo se encuentra pendiente de solventar la siguiente:

| AUDITORÍA | NO. OBS. | DESCRIPCIÓN | % AVANCE | ÁREA |
|-----------------|----------|---|----------|-----------------|
| Riesgos 04-2021 | 5 | Diferencias entre CREDERE versus base de control de cobranza judicial y riesgo por prescripción en gestión judicial | 82% | Abogado General |





5. EVENTO RELEVANTE

Como parte del seguimiento a los Niveles de Tolerancia de Riesgo Tecnológico presentados ante el Comité de Administración Integral de Riesgos (CAIR), de manera específica la métrica "Plataformas tecnológicas obsoletas y/o desactualizadas (aplicativos KRI0008)", la cual consiste en el porcentaje de plataformas tecnológicas sobre versiones obsoletas y/o sin soporte por el fabricante, es de relevancia mencionar que, desde que se presentó en la 4ª Sesión Ordinaria (S.O.) del 2020, (celebrada el 28 de abril y propuestos en la 1ª S.O. del mismo año), continuamente se encontró fuera del nivel de tolerancia aprobado ($\leq 2\%$), siendo hasta en la 10ª Sesión Ordinaria del CAIR de 2024, con información al cierre de septiembre de 2024, se ubicó dentro de los niveles de tolerancia aprobados por el Consejo Directivo, lo cual permite observar que se mantuvo fuera de los límites permisibles por más de cuatro años.

A continuación, se muestra un resumen del comportamiento de dicha métrica, presentada en el Comité de Administración Integral de Riesgos:

| AÑO | 2020 | | | 2021 | | | | 2022 | | | | 2023 | | | | 2024 | | | |
|------------------------|------|-----|-----|------|-----|-----|-----|------|-----|-----|-----|------|-----|-------|-------|-------|------|------|------|
| SESIÓN ORDINARIA | 4ª | 7ª | 10ª | 1ª | 4ª | 7ª | 10ª | 1ª | 4ª | 7ª | 10ª | 1ª | 4ª | 7ª | 10ª | 1ª | 4ª | 7ª | 10ª |
| KRI0008 ($\leq 2\%$) | 25% | 25% | 25% | 25% | 25% | 25% | 25% | 25% | 25% | 25% | 25% | 25% | 25% | 10.7% | 10.7% | 7.13% | 6.9% | 3.4% | 1.7% |

Actualmente la métrica se encuentra dentro del nivel de tolerancia aprobado, sin embargo, es importante mantenerla en los niveles permisibles con la finalidad de evitar la materialización de riesgos tecnológicos, que suelen derivarse de factores como fallas en los sistemas o infraestructura, pérdida de eficiencia y productividad, vulnerabilidad a ataques cibernéticos y brechas de seguridad, mismas que, puede generar impactos negativos en el Instituto, tales como pérdidas económicas, interrupción de operaciones, comprometer la seguridad e integridad de los datos sensibles, entre otros.

Jefa de Grupo

Lic. Mariana Isabel Flores Villanueva
Coordinadora Técnica Administrativa de Alta Responsabilidad,
Encargada y Responsable de los asuntos de la Dirección de Auditoría Interna
con fundamento en el artículo 82 del Estatuto Orgánico del Instituto FONACOT
y el oficio DG/017/2024 de fecha 29 de febrero de 2024





6. PERFIL DE LAS ÁREAS INVOLUCRADAS EN LA AUDITORÍA

Coordinación General de Crédito y Finanzas

Administrar el diseño e implementación de estrategias relativas al análisis y autorización de crédito, recuperación de cartera, mecanismos de protección de pagos, planeación financiera, inversión y financiamiento, así como, de información y registro contable, a efecto de asegurar la sustentabilidad del Instituto y proveer información institucional para una adecuada toma de decisiones, con base en los principios éticos de legalidad, imparcialidad, eficiencia, honradez, lealtad y valores de igualdad, no discriminación, liderazgo, cooperación, interés público, respeto a los derechos humanos, transparencia, rendición de cuentas y equidad de género.

Coordinación General Comercial

Determinar las estrategias vinculadas a los procesos de operación y supervisión comercial a nivel nacional, mercadotecnia, investigación de mercados, calidad en los procesos comerciales, promoción y desarrollo, así como, el diseño de los nuevos productos digitales para el otorgamiento de crédito que ofrece el Instituto FONACOT, fijando las directrices para la integración de metas y objetivos a cumplir, en apego a los planes y programas estratégicos institucionales.

Unidad para la Administración Integral de Riesgos

Determinar, medir, vigilar, e informar los riesgos cuantificables que enfrenta el Instituto FONACOT para cumplir con la normatividad aplicable.

Subdirección General de Contraloría, Planeación y Evaluación

Coordinar las acciones de diseño, generación, monitoreo y evaluación de los planes, programas, y proyectos estratégicos, para contribuir con la gestión del control interno, la implantación de acciones de mejora continua y la generación y análisis de información confiable que permita la toma oportuna de decisiones, en apego a los principios éticos de lealtad, honradez, legalidad, imparcialidad, eficiencia y los valores de cooperación, liderazgo, transparencia, respeto a los derechos humanos, igualdad, no discriminación, equidad de género y rendición de cuentas.

Subdirección General de Tecnologías de la Información y Comunicación

Dirigir los servicios de tecnologías de la información del Instituto FONACOT impulsando el crecimiento en materia de ingeniería de software para entregar de forma consistente servicios informáticos, evaluando soluciones innovadoras y con un enfoque de servicio que permitan al Instituto FONACOT acceder a una posición competitiva, segura y acorde a la normatividad aplicable, con base en los principios éticos de lealtad, honradez, legalidad, imparcialidad y los valores de integridad, cooperación, liderazgo, interés público, transparencia, respeto a los derechos humanos, no discriminación, equidad de género y rendición de cuentas.

Abogado General

Dirigir estrategias, así como los criterios para la atención de los diferentes asuntos jurídicos en los que el Instituto FONACOT sea parte, proporcionando la asesoría técnico jurídico a las áreas del Instituto FONACOT, en total apego a la normatividad aplicable, a fin de, salvaguardar los intereses institucionales, con base en los principios éticos de legalidad, imparcialidad, eficiencia, honradez, lealtad y valores de igualdad, no discriminación, liderazgo, cooperación, respeto a los derechos humanos, transparencia, rendición de cuentas y equidad de género.

Fuente: Manual De Organización General del Instituto FONACOT. - MOG01.02 (vigencia: oct. 2024)





7. DEFINICIONES DE LA CALIFICACIÓN DE AUDITORÍA

Se utiliza una estructura de calificación de dos partes, para comunicar la opinión de Auditoría sobre los controles internos. El primer componente (Satisfactorio, Requiere Mejorar, Insatisfactorio, para efectos de cumplimiento regulatorio es: cumple, cumple parcialmente o incumple) representa la evaluación de la condición de los controles al momento de la auditoría y el 'Símbolo' refleja la evaluación de la dirección en opinión de Auditoría Interna. Las calificaciones son evaluadas al nivel de proceso/unidad que está siendo auditada.

| CONDICIÓN DE CONTROLES INTERNOS | SÍMBOLO | CALIFICACIÓN Y DIRECCIÓN | DESCRIPCIÓN |
|--|---|--------------------------------------|--|
| Satisfactorio El diseño y la operación de los controles son satisfactorios para administrar el riesgo. Sin embargo, se pueden haber identificado deficiencias. |  | Satisfactorio - Estable | La unidad auditada tiene la intención y la capacidad de solucionar las observaciones de auditoría en un <i>tiempo razonable</i> . |
| |  | Satisfactorio - Deteriorando | La unidad auditada no ha identificado ni solucionado activamente las deficiencias y/o las observaciones de auditoría o no se espera que sean corregidas en un <i>tiempo razonable</i> . Como consecuencia, se espera que los controles se deterioren y/o el riesgo o incumplimiento se incremente. |
| Requiere Mejorar El diseño y/u operación de los controles requiere mejorar para administrar el riesgo o incumplimiento. |  | Requiere Mejorar - Solución Oportuna | Las observaciones de la auditoría han sido, ya sea, identificadas por la propia unidad auditada o han sido aceptadas por ésta. Se espera que las observaciones sean solucionadas en un <i>tiempo razonable</i> (2 meses) o que sean implementados controles compensatorios. Generalmente no se puede dar esta calificación a Auditorías con observaciones abiertas o identificadas nuevamente. |
| |  | Requiere Mejorar - Estable | Se espera que la unidad auditada implemente acciones correctivas o las recomendaciones, aun cuando existe alguna incertidumbre si los cambios puedan ser realizados en un <i>tiempo razonable</i> . |
| |  | Requiere Mejorar - Deteriorando | La unidad auditada no ha identificado ni solucionado activamente las deficiencias de control, incumplimientos y/o las observaciones de auditoría no han sido atendidas o no se espera que sean corregidas en un <i>tiempo razonable</i> . Como consecuencia, se espera que los controles se deterioren y/o el riesgo o incumplimiento se incremente. |
| Insatisfactorio El diseño y/u operación de los controles son insatisfactorios para administrar el riesgo o incumplimiento, debido a la identificación de debilidades de control significativas que podrían tener un impacto material en el proceso. |  | Insatisfactorio - Solución Oportuna | Las observaciones de la auditoría han sido, ya sea, identificadas por la propia unidad auditada o han sido aceptadas por ésta. Se espera que las observaciones sean solucionadas en un <i>tiempo razonable</i> (2 meses) o que sean implementados controles compensatorios. Generalmente no se puede dar esta calificación a Auditorías con observaciones abiertas o identificadas nuevamente. |
| |  | Insatisfactorio - Estable | Se espera que la unidad auditada implemente acciones correctivas, aun cuando existe alguna incertidumbre si los cambios puedan ser realizados en un <i>tiempo razonable</i> . |
| |  | Insatisfactorio - Deteriorando | La unidad auditada no ha identificado ni solucionado activamente las deficiencias de control, incumplimientos o riesgos y/o las observaciones de auditoría no han sido atendidas o no se espera que sean corregidas en un <i>tiempo razonable</i> . Como consecuencia, se espera que los controles internos se deterioren, y/o el riesgo o incumplimiento se incremente. |



8. LISTA DE DISTRIBUCIÓN

C.P. Laura Fernanda Campaña Cerezo

Directora General

C. P. Mariel Karina Zamora Nava

Coordinadora General de Crédito y Finanzas

Lic. Salvador Gazca Herrera

Coordinador General Comercial

Mtro. Agni Rodrigo Cerda Mendoza

Titular de la Unidad para la Administración Integral de Riesgos

Mtro. Erick Morgado Rodríguez

Abogado General

Ing. Ricardo Oria Esquivel

Subdirector General de Tecnologías de la Información y Comunicación

Lic. Jazmín García Juárez

Subdirectora General de Administración

Lic. Jaime Francisco Ricci Rojas

Subdirector General de Contraloría, Planeación y Evaluación

Ing. Santiago Carlos Macías Herrera

Presidente Suplente del Comité de Auditoría, Control y Vigilancia del Instituto FONACOT

Lic. Noé García Ortiz

Titular del Órgano Interno de Control Específico en el Instituto FONACOT





9. CÉDULAS DE OBSERVACIONES

| No. | DESCRIPCIÓN DE LA OBSERVACIÓN/RECOMENDACIÓN |
|-----|--|
| 1 | Vulnerabilidad en equipos de cómputo en sucursales. |
| 2 | Deficiencia en seguimiento a vulnerabilidades. |
| 3 | Seguridad y mantenimiento insuficiente al interior de las sucursales. |
| R1 | Reforzar la capacitación al analista del Front en sucursales. |
| R2 | Homogeneidad de las bases de datos históricas sobre las resoluciones judiciales y administrativas. |





OBSERVACIÓN DE AUDITORÍA #1

| | |
|--|--|
| Nombre de la Auditoría | Administración Integral de Riesgos 04/2024 |
| Título de la Observación | Vulnerabilidad en equipos de cómputo en sucursales |
| Responsable del cierre de la observación | Subdirección General de Tecnologías de la Información y Comunicación |
| Nivel de Riesgo | Medio |

I.- Observación

Derivado de la revisión a 32 equipos de cómputo de analistas de front, donde se ejecuta el proceso de originación de crédito, en las Sucursales: Vallejo, Iztacalco, Tlalnepantla, Mixcoac, San Antonio Abad y Representaciones: Chalco y Plaza de la República, se detectó en cuanto a seguridad de la información lo siguiente:

| NO. | ATRIBUTOS | TOTAL CASOS | CUMPLE | NO CUMPLE | CUMPLE % | NO CUMPLE % |
|-----|--|-------------|--------|-----------|----------|-------------|
| 1 | Verificar que no pueda tener más de una sesión simultánea en el sistema de crédito. | 32 | 3 | 29 | 9.38 | 90.63 |
| 2 | Verificar que no cuente con privilegios de administrador. | 32 | 12 | 20 | 37.50 | 62.50 |
| 3 | Verificar que los equipos de cómputo no permitan la extracción de información a través de puertos USB. | 32 | 31 | 1 | 96.88 | 3.13 |
| 4 | Verificar que no tenga acceso a correo electrónico personal. | 32 | 32 | 0 | 100.00 | 0.00 |

- a) En 29 equipos de cómputo, se constató que se pueden tener sesiones simultáneas en el sistema de crédito. Lo anterior contraviene lo establecido en la Política de Control de Accesos, punto 2.2, del Marco de Gestión de Seguridad de la Información del Instituto FONACOT que establece:

2. POLÍTICA DE CONTROL DE ACCESOS

...

2. CONTROL DE ACCESOS.

...

2.2 Acceso a la información del Instituto FONACOT.

El área de sistemas debe controlar el acceso único de cada persona, evitando sesiones simultáneas.

- b) Se detectó que 20 analistas de front tienen en sus equipos de cómputo privilegios de administrador, no presentaron justificación, lo que incumple el Marco de Gestión de Seguridad de la Información del Instituto FONACOT:

2. POLÍTICA DE CONTROL DE ACCESOS

...

3. PRIVILEGIOS DE ACCESO.





3.2. Administración de Privilegios de Acceso.

- Apegarse al Procedimiento de Gestión de Cuentas.
 - Las cuentas o accesos con altos privilegios en los sistemas operativos, aplicativos, herramientas, redes, bases de datos, están restringidos, dichos accesos deben ser gestionados por el administrador del contrato y concederse a través de una solicitud formal que incluya la justificación detallada y fundamentada, la aprobación debe ser provista por el RSI. Los accesos privilegiados deben ser limitados, específicos, justificados plenamente y antes de ser evaluada la autorización, se deben agotar las posibilidades de poder realizar el acceso con identificadores y privilegios estándares.
- c) En 1 caso, se pudo extraer información del equipo de cómputo a través de memoria USB, sin justificación. Lo anterior, se contrapone al Marco de Gestión de Seguridad de la Información del Instituto FONACOT.

16. POLÍTICA DE USO DE MEDIOS DE ALMACENAMIENTO EXTERNOS EN EQUIPOS DE CÓMPUTO

...

2. ALMACENAMIENTO EN DISPOSITIVOS EXTRAÍBLES.

2.1 Políticas Generales.

...

Está prohibida la conexión de dispositivos de almacenamiento extraíbles en los equipos de cómputo del Instituto FONACOT, con la finalidad de anular la posibilidad de utilizar los puertos USB; se utilizará el bloqueo de estos. Se considera que puedan existir excepciones justificadas, por lo que estas deben solicitarse y aprobarse conforme al Procedimiento de Bloqueo y Desbloqueo de Puertos USB.

II.- Implicación/Riesgo

1.- Potencial sustracción de información de los equipos de cómputo.

2.- Sanciones por incumplimiento al Marco de Gestión de Seguridad de la Información del Instituto FONACOT y a las Disposiciones de Carácter General aplicables a los Organismos de Fomento y Entidades de Fomento:

Artículo 10.- Los Organismos de Fomento y Entidades de Fomento deberán contar con sistemas de información de crédito, para la gestión de los créditos en las diferentes etapas del Proceso Crediticio, los cuales como mínimo deberán:

...

III. Mantener controles adecuados que garanticen la confidencialidad de la información, procuren su seguridad tanto física como lógica, así como medidas para la recuperación de la información en casos de contingencia.

III.- Causa Raíz

Fallas en la ejecución del control.





IV.- Recomendación

- 1.- Controlar el acceso único del personal de sucursales en el sistema de crédito, a fin de evitar sesiones simultáneas.
- 2.- Verificar que solo personal autorizado, previa justificación, en las Direcciones Estatales, de Plaza y Representaciones tenga privilegios de administrador.
- 3.- Bloquear los puertos USB de los equipos de cómputo de los analistas del front, en las Direcciones Estatales, de Plaza y Representaciones. Exceptuando aquellos casos donde exista autorización, previa justificación.

V.- Plan de Acción y Fechas compromiso para solventar:

Mediante oficio SGTIC.604.12.2024 recibido a través de correo electrónico el día 30 de diciembre de 2024, la Subdirección General de Tecnologías de la Información y Comunicación, comunicó lo siguiente:

“... ”

Se informa que se revisó al interior de esta Subdirección General y se conjunto la evidencia correspondiente, así como el plan de acción y fechas compromiso de atención a las mismas...”

Como parte de la información proporcionada se muestra un extracto del Plan de Trabajo compartido por la SGTIC para la revisión de equipos de cómputo en sucursales:

| Id | Modo de tarea | Nombre de tarea | Duración | Comienzo | Fin | Cantidad de equipos de cómputo | Trimestres | | | | | | | | | | | | | | | |
|----|---------------|------------------------------|----------|--------------|--------------|--------------------------------|---|---------------------------------|----------------------------------|---------------|--|--|--|--|--|--|--|--|--|--|--|--|
| | | | | | | | 1er trimestre ene feb mar | 2º trimestre abr may jun | 3er trimestre jul ago sep | 4º tri oct | | | | | | | | | | | | |
| 1 | ★ | Centro | 44 días | lun 13/01/25 | jue 13/03/25 | | [Bar chart showing task progress across quarters] | | | | | | | | | | | | | | | |
| 2 | ★ | Coapa | 1 día | lun 13/01/25 | lun 13/01/25 | 15 | [Bar chart] | | | | | | | | | | | | | | | |
| 3 | ★ | Chalco | 1 día | mar 14/01/25 | mar 14/01/25 | 1 | [Bar chart] | | | | | | | | | | | | | | | |
| 4 | ★ | Iztacalco | 3 días | mié 15/01/25 | vie 17/01/25 | 24 | [Bar chart] | | | | | | | | | | | | | | | |
| 5 | ★ | Texcoco | 1 día | lun 20/01/25 | lun 20/01/25 | 5 | [Bar chart] | | | | | | | | | | | | | | | |
| 6 | ★ | Congreso del trabajo | 1 día | mar 21/01/25 | mar 21/01/25 | 8 | [Bar chart] | | | | | | | | | | | | | | | |
| 7 | ★ | Insurgentes | 3 días | mié 22/01/25 | vie 24/01/25 | 10 | [Bar chart] | | | | | | | | | | | | | | | |
| 8 | ★ | Modulo plaza de la republica | 1 día | lun 27/01/25 | lun 27/01/25 | 1 | [Bar chart] | | | | | | | | | | | | | | | |
| 9 | ★ | San Antonio abad | 3 días | mar 28/01/25 | jue 30/01/25 | 27 | [Bar chart] | | | | | | | | | | | | | | | |
| 10 | ★ | Cuautitlán | 3 días | vie 31/01/25 | mar 04/02/25 | 7 | [Bar chart] | | | | | | | | | | | | | | | |
| 11 | ★ | Lerma | 1 día | mié 05/02/25 | mié 05/02/25 | 8 | [Bar chart] | | | | | | | | | | | | | | | |
| 12 | ★ | Tlalnepantla | 3 días | jue 06/02/25 | lun 10/02/25 | 32 | [Bar chart] | | | | | | | | | | | | | | | |
| 13 | ★ | Toluca | 3 días | mar 11/02/25 | jue 13/02/25 | 23 | [Bar chart] | | | | | | | | | | | | | | | |
| 14 | ★ | Ecatepec | 1 día | vie 14/02/25 | vie 14/02/25 | 11 | [Bar chart] | | | | | | | | | | | | | | | |
| 15 | ★ | Pachuca | 3 días | lun 17/02/25 | mié 19/02/25 | 12 | [Bar chart] | | | | | | | | | | | | | | | |
| 16 | ★ | Tizayuca | 1 día | jue 20/02/25 | jue 20/02/25 | 3 | [Bar chart] | | | | | | | | | | | | | | | |
| 17 | ★ | Tula | 1 día | vie 21/02/25 | vie 21/02/25 | 1 | [Bar chart] | | | | | | | | | | | | | | | |
| 18 | ★ | Acapulco | 3 días | lun 24/02/25 | mié 26/02/25 | 11 | [Bar chart] | | | | | | | | | | | | | | | |
| 19 | ★ | Chilpancingo | 1 día | jue 27/02/25 | jue 27/02/25 | 1 | [Bar chart] | | | | | | | | | | | | | | | |
| 20 | ★ | Cuautla | 1 día | vie 28/02/25 | vie 28/02/25 | 4 | [Bar chart] | | | | | | | | | | | | | | | |
| 21 | ★ | Cuernavaca | 3 días | lun 03/03/25 | mié 05/03/25 | 17 | [Bar chart] | | | | | | | | | | | | | | | |
| 22 | ★ | Mixcoac | 3 días | jue 06/03/25 | lun 10/03/25 | 27 | [Bar chart] | | | | | | | | | | | | | | | |

| | | | | | |
|--|----------------------|--------------|---------------------------|-------|-----------------|
| Proyecto: plan de trabajo audit Fecha: vie 27/12/24 | Tarea | [Bar] | Resumen inactivo | [Bar] | Tareas externas |
| | División | [Dotted bar] | Tarea manual | [Bar] | Hito externo |
| | Hito | [Diamond] | solo duración | [Bar] | Fecha limite |
| | Resumen | [Bar] | Informe de resumen manual | [Bar] | Progreso |
| | Resumen del proyecto | [Bar] | Resumen manual | [Bar] | Progreso manual |
| | Tarea inactiva | [Bar] | solo el comienzo | [Bar] | |
| Hito inactivo | [Diamond] | solo fin | [Bar] | | |

Página 1



V.1.- Comentario de la Dirección de Auditoría Interna

De acuerdo al Plan de trabajo proporcionado, se contemplan diferentes fechas de comienzo y termino por cada región para la ejecución de dicho Plan, por lo que se estará dando seguimiento conforme vayan cubriendo las regiones.

A continuación, a manera de resumen pretenden llevar cabo el Plan de trabajo de la siguiente manera:

| REGIÓN | DURACIÓN | FECHA COMIENZO/ FECHA FIN | EQUIPOS DE CÓMPUTO TOTALES |
|-----------|----------|------------------------------|-------------------------------|
| Centro | 44 días | 13/01/2025 – 13/03/2025 | 275 |
| Sur | 35 días | 14/03/2025 – 01/05/2025 | 187 |
| Occidente | 35 días | 02/05/2025 – 19/06/2025 | 244 |
| Norte 1 | 22 días | 20/06/2025 – 21/07/2025 | 154 |
| Norte 2 | 32 días | 22/07/2025 – 03/09/2025 | 237 |

V.2.- Fecha compromiso para solventar

El 1er. seguimiento se llevará a cabo el 21 de marzo de 2025, para verificar el avance realizado.



OBSERVACIÓN DE AUDITORÍA #2

| | |
|--|--|
| Nombre de la Auditoría | Administración Integral de Riesgos 04/2024 |
| Título de la Observación/Recomendación | Deficiencia en seguimiento a vulnerabilidades |
| Responsable del cierre de la observación | Subdirección General de Tecnologías de la Información y Comunicación |
| Nivel de Riesgo | Bajo |

I.- Observación

El Marco de Gestión de Seguridad de la Información del Instituto FONACOT, en su numeral XII.II Proceso de Identificación y Remediación de Vulnerabilidades, enlista las siguientes actividades:

El Instituto FONACOT realiza las siguientes actividades:

- Seguridad - Realiza actividades de análisis de seguridad a la infraestructura tecnológica con la finalidad de identificar vulnerabilidades.
- Seguridad – Por cada una de la vulnerabilidad detectada se entrega al área involucrada del Instituto FONACOT en cuestión, el detalle, la criticidad y urgencia de corrección, incluyendo recomendaciones de corrección. **Cada vulnerabilidad debe contar con un ID a través del cual se lleve a cabo el seguimiento a la atención y remediación del mismo**, se debe documentar todo el seguimiento en la bitácora de seguimiento a vulnerabilidades.
- El área involucrada del Instituto FONACOT - Analiza la sugerencia de corrección y demás información recibida por el equipo de seguridad de la información.
- El área involucrada del Instituto FONACOT - Informa la decisión acerca de implementar la solución propuesta por el equipo de seguridad o bien considerar una solución alternativa para la vulnerabilidad, justificando los motivos.
- El área involucrada del Instituto FONACOT - Implementa la solución y notifica al equipo de seguridad de la información los resultados.
- **Seguridad - Confirma que la solución a la vulnerabilidad ha sido atendida.**
(El resaltado es de la DAI)

El encargado de las funciones de oficial de seguridad de la información, a través del enlace de la Subdirección General de Tecnologías de la Información y Comunicación (en adelante SGTIC), entregó 36 documentos con pruebas de análisis de identificación de vulnerabilidades sobre la infraestructura tecnológica, bases de datos y aplicativos webs que se presentaron en el periodo en revisión; posteriormente en la entrega de documentación que avala el seguimiento correspondiente se detectó lo siguiente:

| INFORMES DE VULNERABILIDADES | ESTATUS |
|------------------------------|----------------------|
| 27 | EN ATENCIÓN |
| 8 | MITIGADO |
| 1 | SIN SEGUIMIENTO |
| 36 | TOTAL GENERAL |



Al verificar el proceso de seguimiento y remediación de vulnerabilidades, se constató que, no cuentan con un identificador, es decir, el prestador de servicio entrega el informe, y el responsable de seguridad de la información se encarga de entregarlo al personal asignado para mitigar las vulnerabilidades detectadas, sin embargo, en el correo y/o oficio no maneja identificador (ID de vulnerabilidad) que pueda rastrear el historial de seguimiento, de igual manera, omite informar fechas compromiso de seguimiento o resultado de la mejora implementada.

En resumen, se identificó en la revisión de los reportes de vulnerabilidades que:

- 1) Carece de ID a través del cual se lleve a cabo el seguimiento a la atención y remediación del mismo.
- 2) No se encuentra documentado el seguimiento del reporte de vulnerabilidades correspondiente a febrero de 2024 "Sistema de Crédito", ya que solo entregaron correo del informe de vulnerabilidad por parte de Seguridad de la Información a la Subdirección General de Productos Digitales.
- 3) De las vulnerabilidades que a la fecha de revisión se reportaron en estatus de "en atención" no se tiene certeza que las acciones realizadas para mitigar dichas vulnerabilidades se están llevando a cabo, ya que no cuenta con información de retroalimentación y/o seguimiento de manera periódica.

II.- Implicación/Riesgo

Al no contar con información precisa que avale el debido proceso de identificación y remediación de vulnerabilidades no se tiene la certeza de cuales han sido mitigadas y cuales en seguimiento.

III.- Causa Raíz

Falta de atención al Marco de Gestión de Seguridad de la Información del Instituto FONACOT en su XII.II Proceso de Identificación y Remediación de Vulnerabilidades.

IV.- Recomendación

Contar con una base de datos de vulnerabilidades con su ID correspondiente, así como documentar y dar seguimiento.

V.- Plan de Acción y Fechas compromiso para solventar:

Mediante oficio SGTIC.604.12.2024 recibido a través de correo electrónico el día 30 de diciembre de 2024, la Subdirección General de Tecnologías de la Información y Comunicación, comunicó lo siguiente:

"...

Se informa que se revisó al interior de esta Subdirección General y se conjunto la evidencia correspondiente, así como el plan de acción y fechas compromiso de atención a las mismas..."

Como parte de la respuesta a esta observación, anexaron una nota realizada por el Encargado de las Funciones de Oficial de Seguridad de la Información que indica lo siguiente:

"..., Se proporciona el documento denominado "Anexo 1 - SI - Seguimiento a Vulnerabilidades.xlsx", el cual permite gestionar de manera adecuada el seguimiento de las vulnerabilidades identificadas





en los activos del Instituto. Cabe destacar que cada vulnerabilidad es registrada y monitoreada mediante un identificador único (ID), mismo que se puede observar en la columna "ID Vuln" del documento en cuestión.

Con este enfoque y con el objetivo de garantizar una adecuada documentación y seguimiento de las vulnerabilidades identificadas y notificadas a las áreas responsables de los activos de información, se implementará un formato único de seguimiento a vulnerabilidades durante el primer trimestre de 2025. Este formato incluirá los campos "Responsable de la Mitigación" y "Fecha de Remediación", facilitando un control más eficiente y transparente del proceso. Para mayor referencia remitirse al documento denominado "Anexo 2 - EJEMPLO - Formato de Seguimiento a Vulnerabilidades.xlsx".

Extracto del Anexo 1 Seguimiento a Vulnerabilidades:

| No Oficio | Fecha de envío | ID Vuln | Mes de detección de vulnerabilidad | Activo | IP | Vulnerabilidad | Criticidad | Fecha 1er retest |
|----------------|----------------|---------------------|------------------------------------|------------|----------------|--|-------------|------------------|
| SI/015/05/2024 | 24/05/2024 | Vuln-FNC-052024-001 | Mayo | FNCASPROEC | 128.160.215.21 | Uso de software con vulnerabilidades conocidas: Apache MQ (CVE-2023-46804) | Crítica | 12/06/2024 |
| | | Vuln-FNC-052024-002 | | | | Directory Path Traversal | Alta | 12/06/2024 |
| | | Vuln-FNC-052024-003 | | | | Implementación inadecuada de CAPTCHA | Alta | 12/06/2024 |
| | | Vuln-FNC-052024-004 | | | | Aplicación web sin soporte HTTPS | Alta | 12/06/2024 |
| | | Vuln-FNC-052024-005 | | | | Cross Site Scripting | Media | 12/06/2024 |
| | | Vuln-FNC-052024-006 | | | | Contraseñas/hasheos detectados | Baja | 12/06/2024 |
| | | Vuln-FNC-052024-007 | | | | Exfiltración de información | Baja | 12/06/2024 |
| | | Vuln-FNC-052024-008 | | | | SELinux deshabilitado | Baja | 12/06/2024 |
| | | Vuln-FNC-052024-009 | | | | Seguridad en certificados | Informativa | 12/06/2024 |
| | | Vuln-FNC-052024-010 | | | | Puertos detectados | Informativa | 12/06/2024 |

Extracto del Anexo 2 Ejemplo Formato de Seguimiento a vulnerabilidades (a implementar):

| # | Activo | ID vulnerabilidad | Vulnerabilidad | Criticidad | Responsables de la mitigación | Fecha de remediación |
|---|---------------------|---------------------|---|------------|--|----------------------|
| 1 | Nombre del Activo 1 | Vuln-ACT-122024-001 | Falta la política de seguridad HTTP | Media | Dirección de Tecnologías de la Información | 01/02/2025 |
| | | Vuln-ACT-122024-002 | Página de Índice por defecto de Microsoft IIS | Media | Dirección de Tecnologías de la Información | 01/03/2025 |
| | | Vuln-ACT-122024-003 | Información publicada en internet | Media | Dirección de Tecnologías de la Información | 01/04/2025 |
| | | Vuln-ACT-122024-004 | Falta de cabecera 'X-Frame-Options' | Baja | Dirección de Tecnologías de la Información | 01/05/2025 |
| | | Vuln-ACT-122024-005 | Falta de cabecera 'XContent-Type-Options' | Baja | Dirección de Tecnologías de la Información | 01/06/2025 |
| 2 | Nombre del Activo 2 | Vuln-PRU-122024-001 | Falta la política de seguridad HTTP | Media | Dirección de Desarrollo | 01/02/2025 |
| | | Vuln-PRU-122024-002 | Página de Índice por defecto de Microsoft IIS | Media | Dirección de Desarrollo | 01/03/2025 |
| | | Vuln-PRU-122024-003 | Información publicada en internet | Media | Dirección de Desarrollo | 01/04/2025 |
| | | Vuln-PRU-122024-004 | Falta de cabecera 'X-Frame-Options' | Baja | Dirección de Desarrollo | 01/05/2025 |
| | | Vuln-PRU-122024-005 | Falta de cabecera 'XContent-Type-Options' | Baja | Dirección de Desarrollo | 01/06/2025 |





V.1.- Comentario de la Dirección de Auditoría Interna

Respecto a la vulnerabilidad “La evaluación de código Estático se realizó de manera general para identificar los riesgos y/o amenazas dentro del aplicativo con alcance Sistema de Crédito” misma que se detectó que se encuentra sin seguimiento, no se obtuvo información relativa.

De la revisión a la información que se indica en la Nota en el “Anexo 1 - SI - Seguimiento a Vulnerabilidades.xlsx” se verificó que dicho archivo cuenta con el campo *ID Vuln* para la identificación de cada vulnerabilidad. Adicionalmente, el área implementará un formato único de seguimiento durante el 1er trimestre de 2025 para facilitar un control más eficiente.

Por lo tanto, se espera la evidencia del seguimiento a la vulnerabilidad antes mencionada.

V.2.- Fecha compromiso para solventar

04 de abril de 2025.



OBSERVACIÓN DE AUDITORÍA #3

| | |
|--|--|
| Nombre de la Auditoría | Administración Integral de Riesgos 04/2024 |
| Título de la Observación | Seguridad y mantenimiento insuficiente al interior de las sucursales |
| Responsable del cierre de la observación | Subdirección General de Administración Dirección de Recursos Materiales y Servicios Generales |
| Nivel de Riesgo | Bajo |

I.- Observación

Como resultado de la inspección ocular efectuada a las Sucursales: Vallejo, Iztacalco, Tlalnepantla, Mixcoac, San Antonio Abad y Representaciones: Chalco y Plaza de la República, se obtuvo lo siguiente:

1.- De la revisión al SITE, se detectó al interior:

| SUCURSAL | SITUACIÓN DETECTADA |
|-----------|-------------------------------------|
| Iztacalco | Cajas vacías |
| Vallejo | Suciedad y humedad |
| Mixcoac | El SITE no estaba cerrado con llave |

2.- La Representación Chalco, no cuenta con detectores de humo. El contar con ellos puede prevenir pérdidas materiales, además de, evitar poner en riesgo la vida del personal que se encuentre en el recinto donde se pueda presentar algún incendio.

II.- Implicación/Riesgo

Al no contar con la seguridad y el mantenimiento adecuado al interior de la sucursal, pueden presentarse riesgos potenciales, lo cual compromete lo establecido en el Marco de Gestión de Seguridad de la Información del Instituto FONACOT, en la política "15. POLITICA DE SEGURIDAD FÍSICA DE LA INFORMACIÓN", que establece lo siguiente:

4. ÁREAS DE SEGURIDAD.

Un área resguardada puede ser una oficina, cuarto o piso completo de cuartos dentro de un perímetro de seguridad física. Los equipos de cómputo y cualquier otro equipo de procesamiento de datos que manipulan, almacenan o transmiten información confidencial deben estar en un área segura.

El área asegurada dentro de una instalación debe proporcionar lo siguiente:

- Acceso restringido.
- Las instalaciones y equipo de tecnología de información que alojan información del Instituto FONACOT deben estar físicamente protegidas contra el acceso no autorizado, daño e interferencia. Estas instalaciones tienen que estar protegidas por un perímetro físico definido, con controles de entrada y barreras de seguridad apropiadas.





- Se debe contar con equipo contra incendios (extintores, detectores de humo), aire acondicionado, energía regulada en las instalaciones. Estos equipos deben recibir mantenimiento anual para su buen funcionamiento.

6. SEGURIDAD DEL EQUIPO.

6.1 Manejo y Protección de Equipo Asignado al Personal Laboral del Instituto FONACOT.

- El equipo debe estar protegido de amenazas de seguridad y riesgos ambientales.
- El equipo de TI (incluyendo equipo usado fuera de la oficina), equipo de comunicación, computadoras de escritorio y equipo de TI periférico (incluyendo fax, copiadoras y equipo de comunicación) debe estar protegido físicamente para reducir el riesgo de accesos no autorizados a información asegurada y protegerlo contra pérdida o daño.
- Se deben aplicar controles para minimizar el riesgo que surge de amenazas potenciales, tales como:
 - Incendio.
 - Explosión.
 - Humo.
 - Polvo y otros contaminantes.
 - Interferencia de suministros eléctricos.

III.- Causa Raíz

Falta de mantenimiento a sucursales y representaciones.

IV.- Recomendación

- 1.- Mantener los espacios destinados para el SITE libres de materiales no pertenecientes al lugar (cajas, basura, entre otros), así como limpios.
- 2.- Verificar que los SITE cuente con acceso restringido.
- 3.- Llevar a cabo un análisis sobre la posibilidad de poder colocar detectores de humo.

V.- Plan de Acción y Fechas compromiso para solventar:

Mediante oficio SGA/DRMYSG/1818/12/2024 recibido a través de correo electrónico el día 30 de diciembre de 2024, la Dirección de Recursos Materiales y Servicios General, proporcionó lo siguiente:

1. El día 21 de diciembre, el personal de esta Dirección, realizó recorrido a las Sucursales Vallejo, Iztacalco, Tlalnepantla, Mixcoac, San Antonio Abad, y a las representaciones Chalco y Plaza de la República.

Derivado de dicho recorrido se observó:





| SUCURSAL/ REPRESENTACIÓN | OBSERVACIÓN | FECHA COMPROMISO |
|-----------------------------|---|--|
| Mixcoac | Cuenta con chapa y llave del SITE en buen estado, 3 detectores de humo y 3 extintores, SITE limpio. Se observa humedad en 20 plafones. | 27 de diciembre cambio de plafones |
| San Antonio Abad | Cuenta con chapa y llave del SITE, 7 extintores y 4 detectores de humo, SITE limpio. 2 extintores se encuentran en el piso. | 03 de enero para colocación de extintores |
| Vallejo | Chapa y llaves del SITE en buenas condiciones, 9 extintores y 5 detectores de humo. SITE sucio | 03 de enero de 2025, limpieza del SITE y se colocaran los extintores que estén en el piso. |
| Tlalnepantla | Chapa y llaves del SITE en buenas condiciones, 5 extintores y 4 detectores de humo, 1 hidrante, SITE limpio | Sin observaciones |
| Chalco | Chapa y llaves del SITE en buenas condiciones, 2 extintores, sin detectores de humo. SITE con cajas de cartón. | Se instalarán 03 detectores de humo, a más tardar el 07 de enero de 2025. Retiro de cajas de cartón y limpieza, el 03 de enero de 2025. |
| Iztacalco | Chapa y llaves del SITE en buenas condiciones, 7 extintores y 4 detectores de humo. SITE con cajas de cartón. | 03 de enero de 2025, limpieza del SITE |
| Plaza de la República | Chapas y llaves de los SITE (se encuentran cerrados) en buenas condiciones, 25 extintores y 65 detectores de humo. SITE limpios. | Sin observaciones |

En todos los inmuebles objeto de la revisión, se cambiarán las pilas de los detectores de humo y se colocarán a más tardar el 24 de enero del presente año.

Aunado a lo anterior, se informa que, durante 2024, se dio mantenimiento de manera trimestral a los equipos de aire acondicionado de las sucursales que nos ocupan, asimismo, en el mes de diciembre se realizó la recarga de los extintores (se adjuntan ordenes de servicio de algunos de los mantenimientos y recargas).

Se giró oficio a la Subdirección General Comercial, así como a los proveedores del servicio de limpieza con la finalidad de que mantengan limpios los SITE y eviten guardar cajas, artículos de limpieza u otros artículos distintos a bienes informáticos, y se restrinja el ingreso a los mismos (se adjunta copia).

De igual forma, se giró oficio a la Subdirección de General de Tecnologías de la Información y Comunicación, con la finalidad de que gire sus instrucciones para atender las observaciones de su competencia, relacionadas con el acceso y seguridad de los equipos de cómputo y cualquier otro equipo de procesamiento de datos (se adjunta copia).





V.1.- Comentario de la Dirección de Auditoría Interna

De acuerdo a la información proporcionada, junto con la evidencia fotográfica y oficios girados a las diferentes áreas, se pudo verificar que llevaron a cabo la revisión de los inmuebles (sucursales), para atender las recomendaciones, queda pendiente la habilitación de los detectores de humo (cambio de pilas), la cual indican que se llevará a cabo a más tardar el 24 de enero de 2025.

Por lo cual se solicita evidencia de las acciones señaladas en su Plan de Acción.

V.2.- Fecha compromiso para solventar

31 de enero de 2025.





RECOMENDACIÓN DE AUDITORÍA #1

| | |
|--|--|
| Nombre de la Auditoría | Administración Integral de Riesgos 04/2024 |
| Título de la Recomendación | Reforzar la capacitación al analista del Front en sucursales |
| Responsable del cierre de la recomendación | Coordinación General Comercial |
| Nivel de Riesgo | Bajo |

I.- Recomendación

Derivado de la revisión al proceso de originación de crédito, en las Sucursales: Vallejo, Iztacalco, Tlalnepantla, Mixcoac, San Antonio Abad y Representaciones: Chalco y Plaza de la República, se detectó lo siguiente:

1.- De una muestra de 32 solicitudes para otorgamiento de crédito, se detectó que el cálculo correspondiente al ID 6521781 fue realizado de forma incorrecta, ya que se consideró una percepción que no correspondía.

| No. | SUCURSAL | TOTAL CASOS | CUMPLE | NO CUMPLE | NO CUMPLE % | CUMPLE % |
|--------------|-----------------------|-------------|-----------|-----------|-------------|--------------|
| 1 | Chalco | 4 | 4 | 0 | 0.00 | 100.00 |
| 2 | Vallejo | 5 | 4 | 1 | 20.00 | 80.00 |
| 3 | Iztacalco | 5 | 5 | 0 | 0.00 | 100.00 |
| 4 | Tlalnepantla | 4 | 4 | 0 | 0.00 | 100.00 |
| 5 | Mixcoac | 6 | 6 | 0 | 0.00 | 100.00 |
| 6 | San Antonio Abad | 5 | 5 | 0 | 0.00 | 100.00 |
| 7 | Plaza de la República | 3 | 3 | 0 | 0.00 | 100.00 |
| Total | | 32 | 31 | 1 | 3.13 | 96.88 |

Por lo antes expuesto, se sugiere fortalecer la preparación del analista del Front, respecto a los conceptos que deben considerarse para el cálculo de percepciones fijas, permanentes y en efectivo, desarrollados dentro del Procedimiento Específico de Registro de Persona Trabajadora.

2.- Se tuvo una plática con 32 analistas del Front, obteniendo la siguiente información:

| No. | TEMA | TOTAL CASOS | CUMPLE | NO CUMPLE | CUMPLE % | NO CUMPLE % |
|-----|--|-------------|--------|-----------|----------|-------------|
| 1 | Conocer los datos registrados por el trabajador en el Portal del Instituto | 32 | 31 | 1 | 96.88 | 3.13 |
| 2 | Conoce los requisitos para las personas trabajadoras eventuales | 32 | 31 | 1 | 96.88 | 3.13 |
| 3 | Conocer los documentos que se tienen que escanear en el sistema de crédito | 32 | 32 | 0 | 100.00 | 0.00 |
| 4 | Saber que realizar si el comprobante de domicilio no coincide con lo que genera el sistema | 32 | 32 | 0 | 100.00 | 0.00 |
| 5 | Sabe qué hacer, si se presenta un extranjero con prórroga | 32 | 24 | 8 | 75.00 | 25.00 |
| 6 | Saber en qué situaciones se utiliza el sello de cotejo y que leyenda debe contener | 32 | 31 | 1 | 96.88 | 3.13 |



- Un analista no conocía algunos datos registrados por el trabajador en el portal del Instituto.
- Un analista no sabía algunos requisitos para las personas trabajadoras eventuales.
- Ocho analistas ignoraban que hacer, si se presenta un extranjero con prórroga.
- Un analista no sabía en qué situaciones se utiliza el sello de cotejo y que leyenda debe contener.

Por lo anterior, se sugiere fortalecer la preparación del analista del Front, respecto a los requisitos que deben considerarse de acuerdo al Procedimiento Específico de Pre-Registro de Persona Trabajadora y al Procedimiento Específico de Registro de Persona Trabajadora, con base en las deficiencias antes señaladas.

II.- Implicación/Riesgo

1. Indebido otorgamiento de créditos.
2. Incumplimiento al Procedimiento Específico de Pre-Registro de Persona Trabajadora y al Procedimiento Específico de Registro de Persona Trabajadora.

III.- Causa Raíz

Falta de reforzamiento de capacitación en el Procedimiento Específico de Pre-Registro de Persona Trabajadora y Procedimiento Específico de Registro de Persona Trabajadora a los analistas del Front.

IV.- Recomendación

Reforzar la capacitación a los analistas del Front en sucursales.

V.- Plan de Acción y Fechas compromiso para solventar:

Mediante el oficio DCSO/113/12/2024 con fecha 20 de diciembre de 2024, la Subdirección General Comercial, a través de la Dirección de Continuidad y Supervisión de Operaciones proporcionó lo siguiente:

1. Con el objeto de reforzar la normatividad aplicable respecto la originación de créditos, la Dirección de Continuidad y Supervisión de Operaciones en conjunto con el SINEIF pusieron en marcha a partir del 7 de agosto, una serie de videos de capacitación dirigidos a los Analistas Front y Comercial (**Anexo 1**).

Dichos videos de capacitación se encuentran activos en todo momento en la plataforma e-Learning a efecto de que los Analistas estén en posibilidad de consultarlos en caso de presentar dudas respecto a la originación de crédito.

2. Con el objeto de disminuir el índice de créditos rechazados por inconsistencias en su originación, la Dirección de Continuidad y Supervisión de Operaciones lleva a cabo un análisis de la base de datos de los créditos que se encuentran en estas condiciones, posteriormente analiza e identifica la recurrencia mensual por analista, en caso de detectar que un Analista incurrió nuevamente en error al realizar un crédito, se solicita a la Dirección de Análisis y Administración de Crédito capacite al Servidor Público recurrente (**Anexo 2**).





3. Adicional a lo anterior, la Dirección de Análisis y administración del Crédito lleva a cabo un programa anual de capacitación, el cual, se imparte a los Analistas con el mayor índice de créditos rechazados de acuerdo con el motivo del rechazo (**Anexo 3**).
4. Por parte de las Direcciones Comerciales Regionales, como parte de su control interno dan seguimiento a la productividad de los Analistas y su índice de rechazos, enviando correos electrónicos de apoyo con los cuales les transmiten la confianza de solicitar una capacitación en caso de así requerirlo (**Anexo 4**).

Así mismo, son ellos quienes exhortan a los Analistas adscritos a su Región a tomar los cursos que les sean designados.

V.1.- Comentario de la Dirección de Auditoría Interna

De acuerdo a la información y anexos proporcionados, señalan que a partir del 7 de agosto de 2024 pusieron en marcha una serie de videos de capacitación dirigidos a los Analistas de Front y Comercial, se detecta la recurrencia mensual por Analista para capacitarlo, se lleva a cabo un programa anual de capacitación (impartido a los Analistas con mayor número de rechazos), y como parte del control interno dan seguimiento a la productividad de los Analistas y su índice de rechazos, si bien se menciona que, desde el mes de agosto se han estado llevando a cabo acciones para reforzar la normatividad, es de relevancia mencionar que al mes de noviembre de 2024 (mes de revisión y visita a sucursales) se identificó en la revisión que aún se presentan errores en el cálculo de percepciones, por lo cual se recomienda y exhorta reforzar las capacitaciones y darles continuidad para que las inconsistencias o errores identificados disminuyan en la medida de lo posible. De lo anterior se solicita presentar evidencia de las capacitaciones llevadas a cabo para poder solventar dicha recomendación.

V.2.- Fecha compromiso para solventar

21 de marzo de 2025.





RECOMENDACIÓN DE AUDITORÍA #2

| | |
|--|---|
| Nombre de la Auditoría | Administración Integral de Riesgos 04/2024 |
| Título de la Recomendación | Homogeneidad de las bases de datos históricas sobre las resoluciones judiciales y administrativas |
| Responsable del cierre de la recomendación | Oficina del Abogado General Dirección de lo Contencioso/Dirección de Asuntos Laborales |
| Nivel de Riesgo | Bajo |

I.- Recomendación

Derivado de la recomendación efectuada por la Comisión Nacional Bancaria y de Valores en oficio 122-1/12839/2024 (anexo 2) y con fundamento en el artículo 79 fracción II, de las Disposiciones de Carácter General Aplicable a los Organismos de Fomento y Entidades de Fomento (Disposiciones), que indica:

Apartado B

De los riesgos cuantificables no discrecionales.

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

...

II. En adición a lo anterior, deberán como mínimo desarrollar las funciones siguientes respecto de:

...

a) La administración del riesgo operacional:

...

c) La administración del riesgo legal

5. Para el registro de eventos de pérdida por riesgo operacional, incluyendo el tecnológico y legal, deberán:

...

iii. Mantener una base de datos histórica que contenga el registro sistemático de los diferentes tipos de pérdida y su costo, en correspondencia con su registro contable, debidamente identificados con la línea o Unidad de Negocio de origen, según las clasificaciones al efecto definidas por los subincisos i y ii anteriores. Para la generación y actualización de dicha base de datos, se deberá cumplir con lo establecido en el Anexo 25 de las presentes disposiciones.

6. Mantener una base de datos histórica sobre las resoluciones judiciales y administrativas, sus causas y costos, asegurándose que aquellas resoluciones judiciales y administrativas que resulten en eventos de pérdida sean incluidas en la fracción II, inciso a) numeral 5, subinciso iii de este artículo.

Se revisaron las bases de datos históricas sobre las resoluciones judiciales y administrativas, que genera la Oficina del Abogado General, obteniendo lo siguiente:

1.- Se gestionan en formato Excel y se identifican con los siguientes títulos:

- RELACIÓN DE BASE HISTÓRICA DE SENTENCIAS JUDICIALES EN MATERIA LABORAL
- RELACIÓN DE JUICIOS ADMINISTRATIVOS CONCLUIDOS
- RELACIÓN HISTÓRICA DE RESOLUCIONES 2015-2024



El artículo 79 fracción II inciso c), numeral 6, antes citado dice: “base de datos histórica sobre las resoluciones judiciales y administrativas...” por lo cual, para una mejor identificación, se sugiere se estandarice dicho título, iniciando como lo indica el precepto legal antes citado, esto es, “Base de datos histórica sobre resoluciones ...”. Lo anterior permitirá que, a través del tiempo, se identifique la razón de ser de las bases, es decir, en cumplimiento al artículo antes señalado.

2.- La “relación histórica de resoluciones 2015-2024”, no contiene identificación de los eventos de pérdidas por año, como es el caso de juicios laborales y administrativos, por lo cual, se sugiere se iguale, ya que permitirá tener información más precisa.

3.- Para cumplir con lo establecido en el artículo 79 fracción II, inciso a), subinciso iii de las Disposiciones, la Dirección de Riesgos No Discrecionales solicita, a través de correo electrónicos a las diversas áreas del Instituto, los reportes de eventos de pérdidas, verificando que la Dirección de lo Contencioso, en el periodo del 1° de octubre de 2023 a 30 de septiembre de 2024, no proporcionó respuesta.

II.- Implicación/Riesgo

Estandarizar las bases de datos históricas de las resoluciones judiciales y administrativas, permite identificar que a través de ellas se cumple con las Disposiciones.

Responder a las solicitudes que realiza la Dirección de Riesgos No Discrecionales, permite tener certeza si ocurrió o no, un evento de pérdida legal, impactando en la confiabilidad de la información que se gestiona en la base de eventos de pérdidas Institucional.

III.- Causa Raíz

Falta de comunicación, entre las áreas involucradas.

IV.- Recomendación

1.- Estandarizar el nombre de las bases, iniciando como lo señala el 79 fracción II, inciso c), numeral 6, es decir, “Base de datos histórica sobre resoluciones ...”.

2.- Que la “relación histórica de resoluciones 2015-2024”, se identifique por año.

3.- La Dirección de lo Contencioso debe dar contestación a la Dirección de Riesgos No Discrecionales, respecto a los eventos de pérdidas.

V.- Plan de Acción y Fechas compromiso para solventar:

Mediante oficio AG/DCN/JDCC/001/12/2024 fechado el 30 de diciembre de 2024, la Dirección de lo Consultivo y Normativo, indicó lo siguiente:

“..., me permito atender dicho requerimiento en mi carácter de Enlace para la citada auditoría, con la información proporcionada por cada una de las áreas correspondientes conforme a lo siguiente:



- *“Homogeneidad de las bases de datos históricas sobre las resoluciones judiciales y administrativas.”*

Con motivo de lo anterior y en relación a la recomendación 1 se agrega al presente como **Anexo 1**, correo electrónico a través del cual la Dirección de Asuntos Laborales atendió la misma, y como **Anexo 2** la base de datos relativa a la Dirección de lo Contencioso.

Ahora bien, por lo que respecta a las recomendaciones 2 y 3 se informa lo siguiente:

- *“2.- La “relación histórica de resoluciones 2015-2024”, no contiene identificación de los eventos de pérdidas por año, como es el caso de juicios laborales y administrativos, por lo cual, se sugiere se iguale, ya que permitirá tener información más precisa”.*

Al respecto se informa que en un periodo de veinte días hábiles contados a partir del día siguiente a la recepción del presente oficio se proporcionara la información correspondiente.

- *“3.- Para cumplir con lo establecido en el artículo 79 fracción II, inciso a), subinciso iii de las Disposiciones, la Dirección de Riesgos No Discrecionales solicita, a través de correos electrónicos a las diversas áreas del Instituto, los reportes de eventos de pérdidas, verificando que la Dirección de lo Contencioso, en el periodo del 1º de octubre de 2023 a 30 de septiembre de 2024, no proporcionó respuesta”.*

En lo subsecuente, la Dirección de lo Contencioso, proporcionará la respuesta correspondiente. “

V.1.- Comentario de la Dirección de Auditoría Interna

1. De la revisión llevada a cabo a las bases de datos proporcionadas en los Anexos 1 y 2, la Dirección de Asuntos Laborales y la Dirección de lo Contencioso, atendieron la recomendación, quedando de la siguiente manera:
 - “Base de datos histórica sobre sentencias judiciales en materia laboral” y
 - “Base de datos histórica sobre sentencias judiciales en materia administrativa”.
 - “Base de datos histórica sobre resoluciones judiciales 2015-2024”

Por lo antes expuesto, se da por atendida por ambas Direcciones la recomendación 1.

2. La Dirección de lo Contencioso indica que proporcionará información en un periodo de 20 días hábiles posteriores a la recepción del oficio.
3. Derivado de la respuesta y toda vez que se tiene conocimiento que durante la primera Sesión Ordinaria del CAIR se presenta la información referente a la estimación de pérdidas potenciales de la Dirección de lo Contencioso, se queda a la espera de la evidencia por parte de esta Dirección respecto a la respuesta a la Dirección de Riesgos No Discrecionales.

Respecto de los puntos 2 y 3 anteriores, subsiste la presente recomendación.

V.2.- Fecha compromiso para solventar

31 de enero de 2025.

