INSTITUTO DEL FONDO NACIONAL PARA EL CONSUMO DE LOS TRABAJADORES

INFORME DE RESULTADOS

SUPERVISIÓN Y ANÁLISIS A LOS MECANISMOS DE CONTROL EN EL MARCO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO FONACOT.

ÍNDICE

I. ANTECEDENTES

De conformidad con el artículo 172 de las Disposiciones de Carácter General aplicables a los Organismos de Fomento y Entidades de Fomento y sus reformas, se informó a la Subdirección General de Tecnologías de la Información y Comunicación del Instituto FONACOT, mediante el oficio núm. DCI/177/07/2025 de fecha 14 de julio del presente, el inicio de la Supervisión y Análisis a los Mecanismos de Control en el Marco de Gestión de Seguridad de la Información del Instituto FONACOT. Lo anterior, con el propósito de verificar la existencia de mecanismos de control suficientes, así como el cumplimiento normativo aplicable.

II. OBJETIVOS

- Identificar y verificar la suficiencia de mecanismos de control en las políticas establecidas en el Marco de Gestión de Seguridad de la Información del Instituto FONACOT.
- Comprobar el apego y cumplimiento a la normatividad aplicable.
- Verificar que no existan debilidades de control en los procedimientos sujetos a supervisión.
- Establecer recomendaciones para reforzar los controles existentes y/o proponer nuevas medidas de control, de considerarse necesario.

III. TÉRMINOS Y ABREVIATURAS

- **CEDN:** Coordinación de Estrategia Digital Nacional.
- **DCI:** Dirección de Contraloría Interna.
- **DTI:** Dirección de Tecnologías de la Información.
- **ERISC:** Equipo de Respuesta a Incidentes de Seguridad en Tecnologías de la Información y Comunicación
- **IPV6:** Protocolo de Internet versión 6.
- **MGSI:** Marco de Gestión de Seguridad de la Información.
- **OCF:** Órgano de Control y Fiscalización de las Instituciones, el cual considera a los Órganos Internos de Control y/o análogos dependientes de la Secretaría Anticorrupción y Buen Gobierno.
- **RSI:** Responsable de la Seguridad de la Información en el Instituto FONACOT.
- **SAS:** Statistical Analysis System
- **SGTIC:** Subdirección General de Tecnologías de la Información y Comunicación.
- **TIC:** Tecnologías de la Información y Comunicación.
- **UTIC:** Unidades de Tecnologías de Información y Comunicación

IV. ACCIONES REALIZADAS

Se verificó la información referente a los indicados en los objetivos de este informe (Políticas y Procedimientos) de la Información del Marco de Gestión de Seguridad de la Información vigente (MA26.01), los cuales se describen a continuación:

1. *Política de Gestión de Incidentes Cibernéticos.*

El 15 de julio de 2025 mediante oficio DCI/182/07/2025, se solicitó a la SGTIC informar cuántas personas y quiénes integraban el ERISC, derivado de lo anterior, se informó mediante nota firmada por el Subdirector General de Tecnologías de la Información y Comunicación, de fecha 23 de julio de 2025, el listado de los integrantes del ERISC; sin embargo, en dicho documento se observa que cuenta con nombres de servidores públicos que ya no laboran en el Instituto FONACOT o bien, actualmente se encuentran ocupando otros cargos.

Por otra parte, se observó que el "Documento de Integración y Operación del Equipo de Respuestas a Incidentes de Seguridad en TIC del Instituto FONACOT" presenta fecha de última actualización en enero 2024, por lo que, con las bajas del personal y los cambios de puesto de algunos de los Integrantes del ERISC, la información de los datos de contacto documentada, no corresponde a la operación actual del Instituto FONACOT.

2. *Determinación para la Gestión de Vulnerabilidades.*

Mediante oficio DCI/182/07/2025 de fecha 15 de julio de 2025 se requirió a la SGTIC, el Plan Anual de Vulnerabilidades 2025 sobre la infraestructura tecnológica, bases de datos, aplicativos web y móviles considerados críticos y evidencia de su presentación a las Unidades Administrativas involucradas, así como una base de datos del control sobre el seguimiento de las vulnerabilidades, indicando la recurrencia por vulnerabilidad y el tiempo de atención con relación a la criticidad.

Por lo anterior, por medio de nota firmada, de fecha 23 de julio de 2025 la SGTIC proporcionó su Plan Anual 2025 de Análisis de Vulnerabilidades, así como evidencia de la presentación y comunicación a las Unidades Administrativas involucradas. De igual manera, proporcionó una base de datos en formato Excel sobre las vulnerabilidades identificadas en los análisis ejecutados durante el primer trimestre de 2025.

Por medio de oficio DCI/208/08/2025, con fecha 25 de agosto de 2025 se realizó un segundo requerimiento de información, en el cual se solicitó a la SGTIC complementar la información anteriormente proporcionada con el periodo del segundo trimestre; asimismo, se solicitó informar si se cuenta con indicadores/estadísticas de la recurrencia por vulnerabilidad, a lo que la SGTIC a través de una nota con fecha 29 de agosto de 2025, informó que el "Servicio Administrado de Análisis de Vulnerabilidades y Pruebas de Penetración", concluyó al cierre del mes de marzo de 2025, por término de contrato, por lo que la ejecución de análisis de vulnerabilidades y pruebas de penetración se reanudarán una vez que haya concluido el proceso de licitación para un nuevo servicio.

Es importante hacer mención que, con fecha 12 de septiembre del presente año se emitió el fallo para llevar a cabo la adjudicación del contrato por dicho servicio.

3. *Política de Control de Accesos, Procedimiento de Gestión de Cuentas y Procedimiento de Contraseñas.*

El 15 de julio de 2025, mediante oficio DCI/182/07/2025, se solicitó a la SGTIC proporcionar evidencia de las revisiones de los derechos de acceso privilegiados del personal del Instituto, correspondiente al primer semestre del 2025, así como evidencia de la última revisión en la que se identificaron e inhabilitaron cuentas genéricas y en desuso.

De lo anterior, se recibió como respuesta el 23 de julio de 2025 una nota firmada por el Subdirector General de Tecnologías de la Información y Comunicación con los registros de sus revisiones mensuales e indicando que no se tienen cuentas genéricas en los servidores de producción, preproducción o desarrollo del Instituto.

De igual manera con fecha del 15 de julio de 2025, mediante el oficio DCI/183/07/2025, se requirió a la Dirección de Recursos Humanos proporcionar un listado de las personas servidoras públicas que causaron alta y/o baja del Instituto FONACOT en el primer semestre del 2025, obteniendo como respuesta una base de datos con 74 registros.

Asimismo, la SGTIC proporcionó una lista de 69 cuentas eliminadas, así como una nota en la cual informa que, de manera mensual, las cuentas en servidores por inactividad, cuentas asociadas a colaboradores o proveedores que ya no cuentan con una relación laboral con el Instituto FONACOT, así como cuentas duplicadas o que no tengan justificación vigente de acceso, son deshabilitadas y posteriormente eliminadas del sistema.

Por lo anterior, mediante una validación de la información proporcionada por ambas áreas, se identificó que la cuenta del usuario con número de gafete 7962 se eliminó el 14 de abril de 2025, siendo que en el Instituto FONACOT causó baja el 15 de febrero de 2025, es decir, casi dos meses después.

4. *Política de Seguridad en las Comunicaciones.*

Mediante oficio DCI/182/07/2025, de fecha 15 de julio de 2025 se solicitó a la SGTIC proporcionar una base de datos de los contratos celebrados en el primer semestre de 2025, indicando lo siguiente: objeto, número de contrato, vigencia y proveedor adjudicado.

En este sentido, mediante nota firmada por el Subdirector General de Tecnologías de la Información y Comunicación, con fecha del 23 de julio de 2025 se informó que por parte del área de Seguridad de la Información no se celebraron contratos en dicho periodo.

5. *Política de Desarrollo Seguro y Procedimiento de Desarrollo Seguro.*

El 15 de julio de 2025 mediante oficio DCI/182/07/2025, se solicitó a la SGTIC proporcionar evidencia de la validación que realiza el RSI con las respectivas áreas para dar cumplimiento al numeral 3.1 de esta política y la correspondiente evidencia del seguimiento al cumplimiento que realiza el RSI al numeral 3.7 de esta política documentada en el MGSI. Con lo cual, la SGTIC mediante una nota firmada por el Subdirector General de Tecnologías de la Información y Comunicación de fecha 23 de julio de 2025, proporcionó 5 archivos electrónicos con los mecanismos de revisión que implementan para dar cumplimiento a las obligaciones institucionales relativas al desarrollo seguro de sistemas internos o subcontratados.

Por lo anterior, derivado de la revisión del Análisis de código estático y dinámico de mayo de 2025 elaborado por IQSEC, mismo que fue proporcionado por la SGTIC, se observa que se detectaron 7 vulnerabilidades altas, 5 medias y 3 bajas.

De igual forma, se verificó que las pruebas de seguridad se solicitaron a equipos diferentes de los que desarrollaron, cumpliendo así con la segregación de funciones y minimizando conflictos de interés.

Asimismo, se revisó la base de datos de vulnerabilidades identificadas al cierre de marzo 2025 visualizando que, de un total de 247, un 68% son de criticidad media, alta y crítica, mientras que el 32% restante son de criticidad baja, informativa o no aplica.

Posteriormente, el 25 de agosto de 2025, por medio del oficio DCI/208/08/2025 se solicitó a la SGTIC en un segundo requerimiento, indicar el estatus actual de las vulnerabilidades detectadas en el primer y segundo trimestre de 2025, un listado del software desarrollado o adquirido y la evidencia de que se cuenta con las patentes o licencias requeridas para su uso, así como un listado de todas las licencias de software y los certificados de seguridad que usan en la SGTIC.

A lo cual, la SGTIC mediante nota de fecha 29 de agosto de 2025 informó que el "Servicio Administrado de Análisis de Vulnerabilidades y Pruebas de Penetración", concluyó por término de contrato al cierre del mes de marzo de 2025, por lo que la ejecución de análisis de vulnerabilidades y pruebas de penetración se reanudarán una vez que se cuente con un nuevo proveedor, cabe mencionar que el fallo del proceso de licitación se llevó a cabo el 12 de septiembre de 2025; sin embargo, de acuerdo a lo establecido en el numeral 6, apartado VI. Políticas de las Políticas, Bases y Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto FONACOT, se sugiere **realizar las gestiones necesarias por lo menos con tres meses de anticipación al vencimiento del contrato, a efecto de garantizar la continuidad de la prestación de servicios.**

Respecto al estado actual de los ID de vulnerabilidades, la SGTIC proporcionó una base de datos con estatus en atención/en curso, en el cual señala que, el "Servicio Administrado de Análisis de Vulnerabilidades y Pruebas de Penetración" es necesario para el proceso de seguimiento de las vulnerabilidades y en específico para la verificación de la remediación de estas.

Con relación a la solicitud de proporcionar un listado del software desarrollado o adquirido y la evidencia de que se cuenta con las patentes o licencias requeridas para su uso, se informó mediante nota que la DTI no adquirió software en el primer semestre del 2025; sin embargo, el software administrado por dicha Dirección se tiene en su modalidad de suscripción; a través de la figura de contrato marco y bajo el contrato denominado "Contrato Abierto para la Prestación de los Servicios y Adquisición de Productos de Licenciamiento Microsoft bajo un Esquema de Suscripción y Soporte de Derechos de Uso" con vigencia al 31 de diciembre de 2025.

De igual manera se cuenta con el contrato denominado Contrato Cerrado para la Prestación del Servicio de Uso y Soporte de Licencia SAS con una vigencia al 31 de diciembre de 2025.

En cuanto a los certificados de seguridad que se utilizan en la SGTIC, se proporcionó evidencia del certificado que opera el Instituto FONACOT para el dominio principal fonacot.gob.mx, con vigencia al 17 de julio de 2026.

6. *Política de Seguridad en las Operaciones.*

Mediante oficio DCI/182/07/2025 de fecha 15 de julio de 2025, se solicitó a la SGTIC proporcionar las actividades maliciosas potenciales detectadas en enero de 2025, así como evidencia de su mitigación, a lo que mediante nota firmada por el Subdirector General de Tecnologías de la Información y Comunicación, de fecha 23 de julio de 2025 se entregó el registro y evidencia de su mitigación; por lo que se validó la base de datos recibida con 50 actividades maliciosas, comprobándose que se cuenta con el análisis realizado por IQSEC con las recomendaciones correspondientes

7. *Política de Protección contra Ciberamenazas.*

Con fecha del 15 de julio de 2025, a través del oficio DCI/182/07/2025, se solicitó a la SGTIC proporcionar registro de las ciberamenazas detectadas en enero de 2025, a lo que el 23 de julio de 2025, mediante nota firmada por el Subdirector General de Tecnologías de la Información y Comunicación se informó lo detectado en dicho periodo, con lo cual se procedió a revisar y comprobar el seguimiento proporcionado.

Asimismo, mediante un segundo requerimiento el 25 de agosto de 2025, a través del oficio DCI/208/08/2025 se solicitó a la SGTIC, en cuanto a temas de la Inteligencia operativa, proporcionar evidencia de los indicadores técnicos que utilizan y los registros/estadísticas de los mismos, así como informar si cuentan con un mecanismo de control de los registros. Por lo anterior, el 29 de agosto de 2025 por medio de una nota la SGTIC nos proporcionó la pantalla del "Executive-Dashboard" misma que utilizan para la inteligencia operativa del Instituto FONACOT, en el cual se muestran los indicadores operativos que se monitorean.

8. *Política de Cumplimiento.*

A través del oficio DCI/182/07/2025, de fecha 15 de julio de 2025, se solicitó a la SGTIC informar, en cuanto a la protección de registros de la organización, si se cuenta con un inventario de datos protegidos, así como proporcionar el plan de revisión predefinido por la SGTIC para el 2025. Por medio de nota firmada por el Subdirector General de Tecnologías de la Información y Comunicación, de fecha 23 de julio de 2025, se proporcionó inventario y capturas de pantalla de eventos que se monitorean a través del Firewall de Bases de Datos.

Por lo anterior, con el inventario recibido se pudo validar que se cuenta con bases de datos protegidas (registros de la organización) a efecto de evitar la alteración de información indebida o no autorizada. De igual manera se pudo observar que se tienen implementadas reglas en el Firewall.

Asimismo, mediante un segundo requerimiento el 25 de agosto de 2025, a través del oficio DCI/208/08/2025 se solicitó a la SGTIC proporcionar evidencia de las revisiones que ejecutan para verificar el cumplimiento del estándar técnico de controles mínimos de seguridad de la información establecidos por la CEDN e indicar la periodicidad de dichas revisiones, esto en apego a 9. Política de Cumplimiento, numeral 3.3. Comprobación del Cumplimiento Técnico. El 29 de agosto de 2025, a través de una nota, la SGTIC compartió el comunicado de la Coordinación de Estrategia Digital Nacional CEDN/0489/2024 de fecha 31 de diciembre de 2024, en el cual se menciona:

> *"A partir de esta fecha y de forma indefinida, se suspenden las fechas y plazos relativos a las actividades, trámites, procesos y procedimientos inherentes a la Herramienta de Gestión de Política TIC, que se encuentran previstos en el Acuerdo de TIC, a saber, los siguientes:*
>
> 1. *La emisión de oficios de autorización de alta y baja de usuarios titulares capturistas de UTIC y OCF;*
> 2. *Pronunciamiento sobre los Portafolios de Proyectos de Tecnologías de la Información y Comunicación;*
> 3. *La emisión de Dictámenes Técnicos sobre solicitudes enviadas por las Dependencias y Entidades de la Administración Pública Federal;*
> 4. *Pronunciamiento sobre la actualización del Marco de Gestión de Seguridad de la Información;*
> 5. *Pronunciamiento sobre la actualización del protocolo de internet IPV6; y*
> 6. *Los demás que establezca el presente Acuerdo, y la Agencia de Transformación Digital y Telecomunicaciones."*

Por lo anterior, la SGTIC argumenta que se suspendieron de forma indefinida, las fechas y plazos relativos a las actividades, trámites, procesos y procedimientos inherentes a la Herramienta de Gestión de Política TIC, donde el Instituto FONACOT realizaba el cumplimiento del estándar técnico de los controles mínimos de seguridad; sin embargo, en el mismo comunicado se reitera que la disposición no exime a las Dependencias, Entidades y Órganos Administrativos Desconcentrados de la Administración Pública Federal del cumplimiento de las obligaciones estipuladas en el referido Acuerdo, por lo que se continúan realizando acciones al respecto.

9. *Política de Seguridad en los Recursos Humanos.*

En el MGSI, 10. Política de Seguridad en los Recursos Humanos, en su numeral 2.1.1 Políticas e Investigación del Personal, se indica que las personas candidatas/postulantes a ocupar una vacante están sujetos a cumplir con los niveles básicos de investigación por parte del Instituto FONACOT. El proceso de investigación es aplicado al personal laboral de nuevo ingreso, esta actividad es realizada por un tercero y validada por la Dirección de Recursos Humanos del Instituto FONACOT.

Por lo que, el 15 de julio de 2025 mediante oficio DCI/183/07/2025 se solicitó a la Dirección de Recursos Humanos, proporcionar el contrato correspondiente al proveedor encargado de realizar la investigación al personal de nuevo ingreso; sin embargo, mediante documento firmado por el Director de Recursos Humanos se informó que en el proceso de personal de nuevo ingreso no se realiza la investigación de personal, por lo que no se cuenta con un proveedor ni contrato.

El 15 de julio de 2025 mediante oficio DCI/182/07/2025 se solicitó a la SGTIC proporcionar un listado de las capacitaciones en materia de Seguridad de la Información que se ha brindado al personal de esa unidad administrativa en el primer semestre de 2025, obteniendo como respuesta el 23 de julio de 2025 a través de una nota firmada por el Subdirector General de Tecnologías de la Información y Comunicación la evidencia de la difusión de infografías en el Instituto FONACOT, así como el curso de inducción para personal de nuevo ingreso al Instituto FONACOT actualizado, resultado de la colaboración con la Dirección de Recursos Humanos.

Con base en la Política 3. Seguridad Durante el Empleo, numeral 3.1 Responsabilidad de la Dirección, en la cual se indica que, la Dirección General, a través de la Dirección de Recursos Humanos, se asegura que todo el personal del Instituto FONACOT es consciente de las amenazas que giran en torno a la seguridad de la información, así como sus responsabilidades, y están provistos con lo necesario para dar cumplimiento con las políticas de seguridad en sus labores, y así reducir el riesgo de errores humanos, el 15 de julio de 2025, mediante oficio DCI/183/07/2025 se solicitó a la Dirección de Recursos Humanos un listado de las capacitaciones en materia de Seguridad de la Información que se ha brindado al personal de la SGTIC en el primer semestre de 2025, a lo cual, mediante documento firmado por el Director de Recursos Humanos se indica que al primer semestre de 2025, no se ha llevado a cabo ninguna capacitación en materia de Seguridad de la Información, ni se proyectó en el Programa Anual de Capacitación por parte del área en la Capacitación Técnica.

V. SITUACIONES DETECTADAS Y RECOMENDACIONES

Con el propósito de contribuir en la mejora de los mecanismos de control, así como de cumplimiento normativo a las políticas objetivo de esta supervisión correspondientes al Marco de Gestión de Seguridad de la Información, se ponen a disposición de la SGTIC del Instituto FONACOT, las siguientes recomendaciones de control:

RECOMENDACIÓN 1
Situación detectada: De acuerdo a la "Política de Gestión de Incidentes Cibernéticos", el Instituto FONACOT, debe establecer una base de datos de contactos para la identificación de los responsables del ERISC y del RSI y mantenerla actualizada; sin embargo, en la evidencia proporcionada, se visualiza que, su última actualización se llevó a cabo en enero de 2024, por lo que algunos de los integrantes del ERISC ya no laboran en el Instituto FONACOT o bien, tienen otros cargos en el Instituto FONACOT. **Recomendación:** Se deberá actualizar el "Documento de Integración y Operación del Equipo de Respuestas a Incidentes de Seguridad en TIC del Instituto FONACOT" de acuerdo a los cargos del personal actual y hacer llegar a ésta Dirección la evidencia; asimismo, considerar llevar a cabo una revisión constante de acuerdo a la ocupación de plazas vigente.
RECOMENDACIÓN 2
Situación detectada: Derivado de la revisión a la base de datos con las altas y bajas del personal del Instituto FONACOT la cual fue proporcionada por la Dirección de Recursos Humanos así como un listado de 69 registros de cuentas eliminadas proporcionada por la SGTIC donde informa que de manera mensual las cuentas en servidores por inactividad, cuentas asociadas a colaboradores o proveedores que ya no cuentan con una relación laboral con el Instituto FONACOT, cuentas duplicadas o que no tengan justificación vigente de acceso son deshabilitadas y posteriormente eliminadas del sistema, se identificó que la cuenta de un usuario con número de gafete 7962 se eliminó el 14 de abril de 2025, siendo que causó baja el 15 de febrero de 2025. **Recomendación:** A fin de dar cumplimiento a la política 2. Control de Accesos, numeral 2.2 Acceso a la información del Instituto FONACOT, en la cual se indica que los controles de acceso para el personal laboral que terminó su relación con el Instituto FONACOT deben eliminarse inmediatamente, así como los proveedores que dejan de prestar sus bienes o servicios para el Instituto FONACOT, se recomienda llevar a cabo revisiones mensuales del acceso privilegiado donde identifican y remueven cuentas de las personas que ya no laboran en el Instituto FONACOT, cambios de puesto, funciones de trabajo y cuentas en desuso.

RECOMENDACIÓN 3
Situación detectada: Se revisó la base de datos de vulnerabilidades identificadas en los análisis al cierre de marzo 2025; visualizándose que, de un total de 247, un 68% son de criticidad media, alta y crítica, mientras que el 32% restante son de criticidad baja, informativa o no aplica. La SGTIC informó que el "Servicio Administrado de Análisis de Vulnerabilidades y Pruebas de Penetración", concluyó por término de contrato al cierre del mes de marzo de 2025, por lo que la ejecución de análisis de vulnerabilidades y pruebas de penetración se reanudarán una vez que haya concluido el proceso de licitación para un nuevo servicio. Respecto al estado actual de los ID de vulnerabilidades se proporcionó una base de datos con estatus en atención/en curso; sin embargo, se señala que, el "Servicio Administrado de Análisis de Vulnerabilidades y Pruebas de Penetración" es necesario para el proceso de seguimiento de las vulnerabilidades y en específico para la verificación de la remediación de estas. Por lo anterior, no se pudo validar que las vulnerabilidades del primer trimestre del 2025 se encuentren cerradas, y no se pudo informar las vulnerabilidades del segundo trimestre del 2025. **Recomendación:** Se deberá informar a ésta Dirección las vulnerabilidades detectadas en el primer trimestre de servicio del nuevo proveedor del "Servicio Administrado de Análisis de Vulnerabilidades y Pruebas de Penetración", indicando ID y el estatus de las mismas.

- **Termina Informe** -