INSTITUTO DEL FONDO NACIONAL
PARA EL CONSUMO DE LOS TRABAJADORES

INFORME DE RESULTADOS

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

Subdirección General de Contraloría, Planeación y Evaluación.
Dirección de Contraloría Interna.
Marzo, 2026.

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/019/01/2026 de fecha 20 de enero del presente año, el inicio de la Supervisión y Análisis a los Mecanismos de Control de las Políticas del 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

- **DCI:** Dirección de Contraloría Interna.
- **DIT:** Dirección de Infraestructura Tecnológica.
- **DRP:** Disaster Recovery Plan.
- **KIO:** SixSigma Networks México S.A. de C.V.
- **MGSI:** Marco de Gestión de Seguridad de la Información.
- **RSI:** Responsable de la Seguridad de la Información en el Instituto FONACOT.
- **SGTIC:** Subdirección General de Tecnologías de la Información y Comunicación.
- **TI:** Tecnologías de la Información.
- **URL:** Uniform Resource Locator.

IV. ACCIONES REALIZADAS

Se verificó la información referente a lo indicado en los objetivos de esta supervisión y análisis a los mecanismos de control del Marco de Gestión de Seguridad de la Información vigente, los cuales se describen a continuación:

1. *Política de Gestión de Activos de la Información.*

El 22 de enero de 2026, mediante oficio DCI/020/01/2026, se solicitó a la SGTIC informar si se cuenta con un inventario de activos tecnológicos, e indicar la periodicidad con la que se actualiza, derivado de lo anterior, se comunicó a ésta DCI, mediante nota de fecha 30 de enero de 2026, firmada por el Subdirector de Infraestructura Tecnológica (y personal de apoyo para el debido cumplimiento de las funciones al cargo de Oficial de Seguridad de la Información en el Instituto FONACOT, mediante oficio No. SGTIC.402.06.2025), que el Instituto cuenta con dicho inventario, el cual se mantiene actualizado de manera periódica, con una revisión mensual, conforme al MGSI.

Por otra parte, el inventario presentado contiene cinco datos: No, *Hostname*, Ambiente, Sistema Operativo y *Site*, por lo que no cumple con las características indicadas en la Política del MGSI, la cual señala que el inventario debe cumplir con lo estipulado en el "Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos" y su Anexo "Identificación de Activos Esenciales de Información de los Múltiples Involucrados", debiendo contener al menos la siguiente información: *Site*, Origen, Unidad de procesamiento, Estatus, *Hostname*, Aplicación, Nube, Descripción, Plataforma, Ubicación física, Máscara de subred, *Gateway*, VLAN ID, Ambiente, IP Producción, IP *backup*/mgt, IP pública, Marca/Modelo, número de serie, Hardware físico/virtual y Sistema Operativo.

2. *Política de Criptografía.*

Mediante oficio DCI/020/01/2026, de fecha 22 de enero de 2026, se solicitó a la SGTIC indicar de qué manera determinan a los responsables de custodia de los sistemas de encriptación, por lo que mediante nota firmada, de fecha 30 de enero de 2026, el Subdirector de Infraestructura Tecnológica informó que la custodia de los mecanismos de cifrado se asignan a las áreas responsables de la administración de los sistemas, aplicaciones y plataformas que los implementan, en función de sus atribuciones y uso, conforme a lo establecido en el apartado 2. Uso de Cifrado.

De igual manera, se requirió informar de qué manera se realiza el análisis de riesgos en temas de uso y administración de tecnologías de encriptación, y cuál es la periodicidad con que se realiza, a lo que por medio de nota firmada, de fecha 30 de enero de 2026, el Subdirector de Infraestructura Tecnológica comunicó que el Instituto realiza análisis de

riesgos tecnológicos, los cuales se enfocan en los activos tecnológicos mediante la identificación de amenazas y vulnerabilidades técnicas, mencionando que dichos análisis no se realizan de manera específica sobre los mecanismos de cifrado, sino sobre los activos tecnológicos en los que estos se encuentran implementados. En este caso, la revisión de los mecanismos de cifrado se aborda a través de evaluaciones técnicas complementarias, como los análisis de vulnerabilidades (cuando el alcance de dichas pruebas así lo requiere) que se realizan con una periodicidad mensual y de manera programada, donde se puede revisar: protocolos inseguros deshabilitados, cifrado débil en servicios expuestos, cifrados mal configurados, algoritmos obsoletos, etc., y los riesgos asociados a estos.

También se solicitó informar con que periodicidad el RSI identifica que se cumpla con los estándares de cifrado, a lo cual, mediante nota firmada por el Subdirector de Infraestructura Tecnológica, de fecha 30 de enero de 2026, informó que el cumplimiento de los mecanismos de cifrado se realiza de manera mensual a través de los resultados de los análisis de vulnerabilidades realizados sobre los activos tecnológicos. Dichos análisis permiten verificar diferentes aspectos relacionados con los mecanismos de cifrado, tales como: la deshabilitación de protocolos inseguros, el uso de versiones y configuraciones adecuadas, así como la detección de algoritmos obsoletos o configuraciones de cifrado débil, como evidencia se entregó el Reporte de Vulnerabilidades IP 128.160.201.33, correspondiente a la última evaluación, en la que se pudieron visualizar la revisión de estos mecanismos de cifrado.

3. *Política de Seguridad en las Comunicaciones y Procedimiento de Políticas de Comunicación.*

El 22 de enero de 2026, mediante oficio DCI/020/01/2026, se solicitó a la SGTIC indicar la periodicidad con que se realiza el inventario de todos los componentes de red, por lo que mediante nota firmada, de fecha 30 de enero de 2026, el Subdirector de Infraestructura Tecnológica respondió que de acuerdo con el esquema de arrendamiento de los activos tecnológicos, la gestión del inventario de los componentes de red se realiza conforme a lo previsto en los instrumentos contractuales, mediante la entrega mensual de un listado actualizado de los activos arrendados que el proveedor realiza. El cual permite a la Dirección de Infraestructura, contar con visibilidad y control sobre los componentes de red disponibles.

Adicionalmente, se solicitó informar si durante el 2025 los operadores de red habían realizado algún plan de la capacidad de las redes en el Instituto FONACOT; a lo que, mediante nota firmada por el Subdirector de Infraestructura Tecnológica, con fecha 30 de enero de 2026, informa que el operador de red, en su carácter de proveedor de servicios de red, elabora el plan de capacidad (*Capacity Planning*, por sus siglas en inglés) de la red al cierre de cada semestre, conforme al esquema de prestación del servicio. Dicho plan es recibido por el Instituto y validado en cuanto a su consistencia y alcance, y posteriormente

es comunicado vía correo electrónico a la DIT para su conocimiento, conforme a los lineamientos Institucionales.

De igual manera, en el tema de seguridad de los servicios de red, se solicitó informar si llevan a cabo evaluaciones de riesgo y quién o quiénes las realizan, por lo que, mediante nota firmada por el Subdirector de Infraestructura Tecnológica, con fecha 30 de enero de 2026, se informó que la evaluación de riesgos sobre los servicios de red del Instituto, se realiza de manera mensual y programada, a través de los resultados de los análisis de vulnerabilidades ejecutados por el proveedor del "Servicio Administrado de Análisis de Vulnerabilidades y Pruebas de Penetración", en los que se proporciona la revisión de los atributos de seguridad asociados a los servicios de red del Instituto y los riesgos asociados.

Aunado a lo anterior, se requirió informar si se elaboraron acuerdos de confidencialidad relacionados con seguridad de la información, para lo cual el Subdirector de Infraestructura Tecnológica, con fecha 30 de enero de 2026, respondió mediante nota firmada que se incluyen en los instrumentos contractuales aplicables a las relaciones con terceros, tal como se establece en los lineamientos, para lo cual se entregó como evidencia captura de pantalla del contrato "FNCOT/LP/212/2025" del "Servicio Administrado de Análisis de Vulnerabilidades y Pruebas de Penetración", donde se muestra la inclusión del acuerdo de confidencialidad en cuestión.

4. *Política de Relación con Terceros.*

Mediante oficio DCI/020/07/2025, de fecha 22 de enero de 2026, se solicitó a la SGTIC informar de que manera, mediante sus áreas internas, da seguimiento al cumplimiento de los lineamientos para la confidencialidad y seguridad de la información de los clientes del Instituto FONACOT. En virtud de lo anterior, a través de nota firmada, de fecha 30 de enero de 2026, por el Subdirector de Infraestructura Tecnológica, comunicó que:

> *… "el control en materia de confidencialidad y seguridad de la información se realiza mediante mecanismos de revisión que se llevan a cabo cuando se presentan cambios en el alcance de la relación, incidentes de seguridad, renovación o cierre de contrato, etc.*
> *En este sentido, la SGTIC da seguimiento al lineamiento asegurando su aplicación y mediante mecanismos de revisión asociados a escenarios relevantes para la seguridad de la información."*

De igual manera, se requirió hacer de conocimiento de qué forma se lleva a cabo la eliminación de accesos a la Infraestructura Informática y Devolución de Activos, por lo que, mediante nota firmada, de fecha 30 de enero de 2026, por el Subdirector de Infraestructura Tecnológica, comunicó que los proveedores cuentan con usuarios controlados mediante el Directorio Activo, el cual se encuentra vinculado a un sistema de control de accesos privilegiados, con permisos puntualmente proporcionados por el Instituto; por lo que al

término de cualquier relación con el mismo, se realiza la eliminación de cuentas y contraseñas, evitando así el acceso a información institucional.

En complemento a lo anterior, señaló que el Instituto no proporciona activos informáticos a los proveedores o terceros para el desarrollo de sus actividades. En el caso de los proveedores que suministran al Instituto equipos informáticos que puedan contener información institucional previo a su retiro y terminación de la relación contractual se solicita la ejecución de un borrado seguro, para mayor referencia se anexa certificado.

5. *Política de Seguridad Física de la Información.*

El 22 de enero de 2026, por conducto del oficio DCI/020/01/2026, se solicitó a la SGTIC indicar de qué manera se ha controlado y registrado el acceso a los cuartos de resguardo (en KIO) de los servidores, por lo que mediante nota firmada, de fecha 30 de enero de 2026, el Subdirector de Infraestructura Tecnológica proporcionó el procedimiento de registro que se realiza a través de la plataforma web denominada "*Kio Link*", a la cual se accede por medio de URL, ingresando correo electrónico para poder iniciar sesión, como usuarios KIO o usuarios cliente, y se continúa con el proceso de acceso al *Data Center KIO*, en donde se hace una solicitud para visita, misma que está sujeta a un proceso de autorización, y en caso de autorizarse se genera un folio. Posteriormente, se genera un listado de los escaneos de los *racks* o jaulas realizados en la visita, los cuales incluyen información del *rack*, el usuario que realizó el escaneo y la fecha del movimiento.

Asimismo, se solicitó indicar quién se encarga de establecer los perímetros de seguridad de las instalaciones que procesan información, a lo cual se comunicó que el Instituto FONACOT cuenta con el contrato FNCOT/LP/213/2025, denominado "Contratación abierta del servicio administrado de Centro de Datos, nube híbrida (pública y/o privada) y DRP del Instituto del Fondo Nacional para el Consumo de los Trabajadores (INFONACOT)", mediante el cual se proporciona el servicio administrado de Centro de Datos y de Recuperación ante Desastres (DRP). Dentro del alcance de dicho contrato se incluye la seguridad física de los equipos albergados en el Centro de Datos, así como la seguridad perimetral de las instalaciones.

De igual manera, con el fin de reducir riesgos de accesos no autorizados a información asegurada y protección contra pérdida y daño de equipo de TI periférico, se solicitó se informara de qué manera se protege físicamente a dicho equipo. A lo cual el Subdirector de Infraestructura Tecnológica informó que para asegurar los equipos de cómputo (Laptop y Equipos de escritorio) se cuenta con un servicio que proporciona Candados Físicos, los cuales se asignan al personal que tiene equipo de cómputo y requieren de un candado para evitar el robo o extravío del mismo. Para equipos de cómputo que implique la entrega de un periférico *Docking*, se entrega un candado por parte del proveedor de servicios de equipos de cómputo y periféricos para el aseguramiento de dicho periférico

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: Se constató la existencia de un inventario de activos tecnológicos donde mencionaron que la actualización es mensual; no obstante, el mismo no integra la totalidad de los campos establecidos en la Política de Gestión de Activos del MGSI ni en el instrumento normativo complementario citado en la misma. El inventario presentado contiene información básica (*Hostname*, Ambiente, Sistema Operativo, *Site*), sin incluir elementos como direcciones IP, clasificación del activo, ubicación física detallada, características técnicas ampliadas y demás datos mínimos requeridos. Lo anterior puede impactar en procesos de gestión de riesgos e incidentes. **Recomendación:** Se deberá actualizar el inventario de activos tecnológicos institucional para alinearlo integralmente con los campos mínimos establecidos en la normativa aplicable, así como contener los datos y firma de quién lo elaboró y quién lo verificó, mensualmente.