AUDITORÍA A LAS POLÍTICAS DE SEGURIDAD EN LOS COMPONENTES TECNOLÓGICOS DE REDES Y COMUNICACIONES EN EL MHCP

Objetivo y Alcance

Evaluar de manera razonable la implementación de las políticas de seguridad en los componentes tecnológicos de redes y comunicaciones, verificando el cumplimiento de políticas, procedimientos y normativa aplicable. Para ello, se realizarán pruebas de auditoría orientadas a determinar el nivel de control en la gestión y a identificar oportunidades de mejora.

El periodo de evaluación está comprendido entre el 1 de enero al 31 de diciembre de 2025.

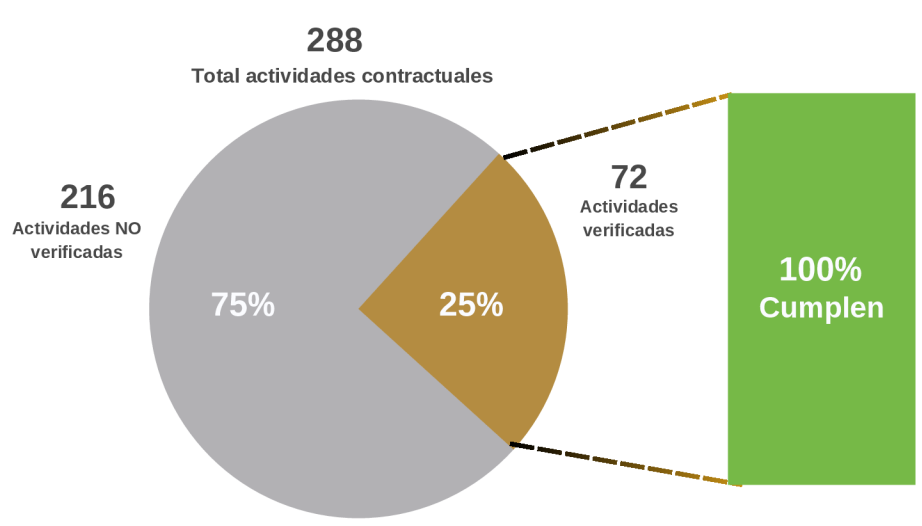
Resultado de la actividad realizada

Verificación de la información soporte de la ejecución contractual del contrato 3.368.2024, relacionado con redes y comunicaciones

Se realizó la verificación del soporte de ejecución del contrato No. 3.368.2024, asociado a los servicios de redes y comunicaciones.

Al respecto, de las 288 actividades establecidas para el citado contrato, la OCI verificó 72, equivalentes al **25%**, las cuales estan centradas en los servicios tecnológicos asociados a redes y comunicaciones.

En términos generales, el proveedor **cumple** con las obligaciones revisadas.



Controles del Modelo de Seguridad y Privacidad de la Información MSPI relacionados con los componentes tecnológicos de redes y comunicaciones

Aspectos verificados

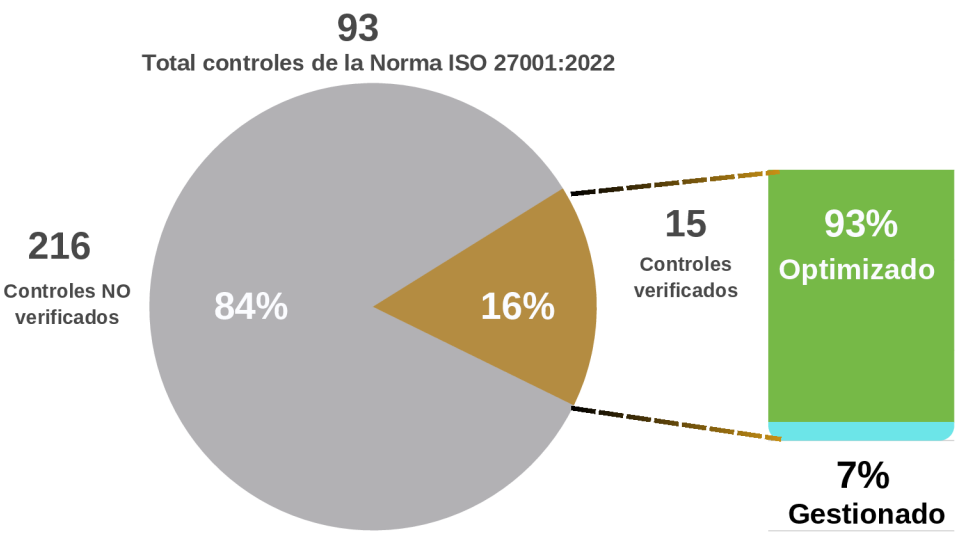
De los noventa y tres (93) controles establecidos en la Norma ISO 27001:2022, la OCI verificó quince (15), equivalentes al **16%,** evidenciando que:

- El 93% presenta un nivel de madurez **optimizado**.
- El 7% restante, se encuentra en un nivel **gestionado**.

Aspectos por mejorar

Como resultado de la verificación del control tecnológico correspondiente al numeral 8.6 “Gestión de la Configuración” de la Norma ISO 27001:2022, la OCI valoró dicho control en estado “Gestionado”, debido a que:

- El MHCP no cuenta con un procedimiento formal para la Gestión de la Capacidad.
- Las reglas de seguridad de los firewalls de las infraestructuras tecnológicas del SIIF Nación, el Sistema General de Regalías y el MHCP se administran de manera manual.



Gestión del Riesgo

Al revisar el mapa de riesgos asociado al proceso evaluado en la auditoría interna, se identificaron los siguientes riesgos:

- *"Posibilidad de afectación económica y reputacional del MHCP debido a la Interrupción masiva no programada de algún servicio tecnológico que haga parte del catálogo de servicios TIC."*

- *"Posibilidad de afectación económica o de imagen por tener soluciones en ambiente productivo en desuso no programado."*

De acuerdo a la verificación realizada en la auditoría y lo documentado en el SMGI, no se evidenció materilización de los riesgos asociados al proceso Apo.1.3 Gobierno y Gestión TIC.

Resultado de la Evaluación

Observaciones

Como resultado de la Auditoría Interna, no se identificaron observaciones que requieran la suscripción de un plan de mejoramiento interno en el SMGI.

Oportunidades de Mejora y Recomendaciones

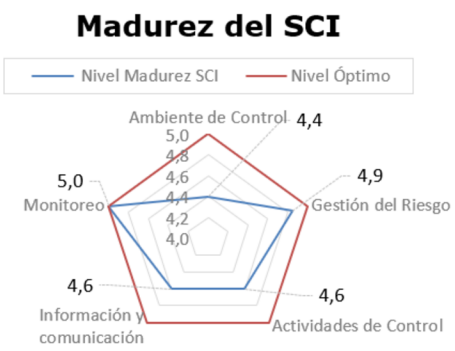
Se identificó la siguiente oportunidad de mejora, la cual se espera se analice por parte de los responsables:

OM-2026-AI-05-01: Como resultado de la verificación del control tecnológico correspondiente al numeral 8.6 "Gestión de la Configuración" de la Norma ISO 27001:2022, la Oficina de Control Interno valoró dicho control en estado "Gestionado", debido a que el MHCP no cuenta con un procedimiento formal para la Gestión de la Capacidad. Dado lo anterior, las reglas de seguridad de los firewalls de las infraestructuras tecnológicas del SIIF Nación, el Sistema General de Regalías y el MHCP se administran de manera manual.

A partir de esta situación, la Oficina de Control Interno identificó como **oportunidad de mejora** analizar la viabilidad de documentar el proceso de Gestión de la Capacidad, así como fortalecer la revisión y depuración de las reglas de seguridad en los firewalls. En este sentido, **se recomienda** a la Dirección de Tecnología la viabilidad de documentar el proceso de gestion de la Capacidad, evaluar la implementación de mecanismos que permitan realizar una revisión integral de las configuraciones técnicas y reglas de acceso de los firewalls, y efectuar la depuración periódica de dichas reglas.

Estado de madurez del Sistema de Control Interno del proceso

En el marco de la evaluación realizada al proceso Apo.1.3 Gobierno y Gestión TIC se presenta a continuación el resultado del análisis del estado de madurez del Sistema de Control Interno, con base en los criterios establecidos por el modelo de referencia adoptado por la OCI. Nivel de madurez de los componentes del SCI en "**Óptimo**" con una calificación de 4.6/5.0



Conclusiones

De acuerdo con el resultado de la Auditoría Interna a la Política de Seguridad de la Información en lo que concierne a los componentes tecnológicos de redes y comunicaciones, la OCI evidenció que la Dirección de Tecnología ha implementado adecuadamente los controles relacionados con la supervisión del servicio de mesa de ayuda, cumpliendo las obligaciones contractuales y alcanzando un nivel de madurez optimizado conforme a la Norma ISO 27001:2022.

Ahora bien, en relación con la gestión de los riesgos asociados al proceso APO.1.3 Gobierno y Gestión de TIC, no se evidenció la materialización de los riesgos, en particular aquellos relacionados con la interrupción masiva de los servicios tecnológicos, la existencia de soluciones en desuso en ambientes productivos, ni otros riesgos vinculados a la seguridad de la información, la disponibilidad de los servicios, la integridad de los sistemas y la continuidad operativa.

Como resultado de la presente auditoría, no se identificaron aspectos que requieran la suscripción de un plan de mejoramiento interno en el SMGI. Sin embargo, se identificó una (1) oportunidad de mejora relacionada con: analizar la viabilidad de documentar y formalizar el proceso de Gestión de la Capacidad, así como fortalecer la revisión y depuración de las reglas de seguridad en los firewalls con el propósito identificar exposiciones a riesgos asociados a la seguridad de la información de la entidad, que permitiría avanzar de estado "Gestionado" a "Optimizado" en el control 8.6 "Gestión de la Capacidad" en el cumplimiento a los requisitos de la ISO 27001:2022.