INFORME GESTIÓN DEL CAMBIO MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN "MSPI" – VIGENCIA 2024.

ELABORÓ	REVISÓ	APROBÓ
NOMBRE: Ing. Deiby Leandro Alvarado Rodríguez	**NOMBRE:** Ing. Roberto Velásquez Arango. Ing. César Adolfo González Peña.	**NOMBRE:** Ing. Ricardo Valenzuela Díaz
CARGO: Profesional Defensa – Seguridad de la Información	**CARGO:** Coordinador Grupo Informática. Coordinador Grupo de Redes e Infraestructura Tecnológica.	**CARGO:** Líder Proceso Gestión de TIC.
FIRMA: Deiby Leandro Alvarado Rodriguez Firmado digitalmente por Deiby Leandro Alvarado Rodriguez Fecha: 2025.01.28 09:07:10 -05'00'	**FIRMA:** Roberto Velasquez Arango Firmado digitalmente por Roberto Velasquez Arango Fecha: 2025.01.28 09:11:29 -05'00' César González Firmado digitalmente por César González Fecha: 2025.01.28 09:18:12 -05'00'	**FIRMA:** Ricardo Valenzuela Diaz Firmado digitalmente por Ricardo Valenzuela Diaz Fecha: 2025.01.28 12:04:07 -05'00'

1. OBJETIVO DEL INFORME

Realizar una evaluación integral de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) al corte del 28 de enero de 2025, con un enfoque en la efectividad de las medidas de seguridad aplicadas, los logros alcanzados y los desafíos identificados. El análisis abarcará la alineación del MSPI con el Plan Estratégico de Seguridad y Privacidad de la Información (PESI), comparando las acciones ejecutadas con los objetivos establecidos, evaluando el cumplimiento de las directrices planteadas y resaltando las áreas que requieren mejora. Esta evaluación proporcionará una visión completa del estado actual del modelo y su impacto en los objetivos estratégicos, contribuyendo a la toma de decisiones informadas para el fortalecimiento continuo de la seguridad y privacidad de la información en la entidad.

2. CUERPO DEL INFORME

La implementación de los lineamientos de seguridad y privacidad de la información, establecidos por el Gobierno Nacional y supervisados por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), enfrenta desafíos continuos debido a la evolución constante de los riesgos asociados con los incidentes de seguridad digital. Estos incidentes no solo ponen en riesgo la operatividad de las entidades gubernamentales, sino que también pueden tener un impacto directo en la prestación de servicios a la comunidad, lo que subraya la importancia de contar con un marco robusto para la protección de los activos informáticos.

En este contexto, el MinTIC ha desarrollado directrices específicas para fortalecer la seguridad en el entorno digital del sector público, con el fin de garantizar que las tecnologías de la información se utilicen de manera segura y eficiente. Estas directrices deben ser implementadas de manera rigurosa para salvaguardar la integridad de la información y minimizar la exposición a posibles amenazas cibernéticas.

El propósito de este informe es proporcionar una evaluación exhaustiva del avance en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) hasta el 28 de enero de 2025. Se analizará su alineación con el Plan Estratégico de Seguridad y Privacidad de la Información (PESI), identificando los logros alcanzados, los retos enfrentados y las áreas que requieren atención adicional. En un entorno cada vez más digitalizado e interconectado, la protección de la información y la privacidad de los datos sensibles son pilares fundamentales no solo para cumplir con las normativas establecidas, sino también para mantener la confianza de todas las partes interesadas, incluyendo ciudadanos, entidades gubernamentales y otros actores clave.

2.1 VISIÓN GENERAL DEL MSPI.

El Modelo de Seguridad y Privacidad de la Información (MSPI) es un marco integral y estructurado que garantiza la protección de la información confidencial y sensible dentro de la entidad, brindando un enfoque sistemático para mitigar riesgos y asegurar la privacidad de los datos. Este modelo no solo está alineado con estándares internacionales reconocidos, como la norma ISO/IEC 27001, sino que también incorpora buenas prácticas basadas en las exigencias legales y regulatorias del sector público. Su propósito fundamental es establecer una arquitectura de seguridad que aborde de manera eficaz los desafíos actuales relacionados con el manejo, almacenamiento y transmisión de información.

El MSPI tiene como finalidad fortalecer la seguridad en todos los niveles de la entidad, promoviendo la implementación de controles técnicos, operativos y administrativos que permitan reducir los riesgos asociados al uso de la información. Su diseño no solo busca prevenir incidentes de seguridad, sino también garantizar la resiliencia organizacional frente a eventos adversos que puedan comprometer la confidencialidad, integridad y disponibilidad de los datos.

Además, el MSPI fomenta una cultura organizacional en la que la gestión de la información se realiza de forma segura, confiable y transparente, alineada con las mejores prácticas y con un enfoque proactivo para la identificación y mitigación de riesgos. Al mismo tiempo, el modelo promueve la mejora continua, permitiendo que la entidad se adapte a los avances tecnológicos y a los cambios en el panorama de amenazas, asegurando que la protección de la información siga siendo una prioridad estratégica a largo plazo.

2.1.1. Controles de seguridad:

El MSPI implementa un conjunto integral de controles de seguridad que abordan de manera proactiva la prevención, detección y respuesta ante incidentes de seguridad. Uno de los pilares fundamentales de este modelo es la gestión de accesos basada en roles (RBAC), la cual restringe el acceso a la información únicamente a aquellos usuarios que cuentan con la autorización necesaria según sus responsabilidades y funciones asignadas dentro de la entidad. Este enfoque garantiza que cada funcionario solo pueda acceder a los datos relevantes para su labor, minimizando los riesgos de acceso no autorizado o uso indebido de la información.

Además, el MSPI emplea herramientas de monitorización continua, que permiten vigilar las actividades del sistema en tiempo real. Estas herramientas automatizadas son capaces de detectar patrones de comportamiento anómalos, identificar posibles vulnerabilidades y alertar sobre amenazas potenciales de manera temprana, lo que facilita la intervención inmediata para mitigar cualquier riesgo antes de que pueda comprometer la seguridad de la información.

En el caso de que ocurra un incidente de seguridad, el MSPI activa un protocolo de respuesta detallado y sistemático. Este protocolo abarca todas las fases del manejo de incidentes, desde la contención y mitigación inicial de los efectos del incidente hasta la investigación profunda de las causas, incluyendo el análisis de vulnerabilidades. El objetivo principal es minimizar el impacto sobre la operatividad de la entidad y restaurar la normalidad lo más rápidamente posible, asegurando así la continuidad de los servicios y protegiendo los activos de información críticos.

2.1.2. Políticas y procedimientos:

El MSPI establece un marco integral de políticas y procedimientos que regulan de manera rigurosa todo el ciclo de vida de la información dentro de la entidad. Estas políticas están diseñadas para proporcionar directrices claras sobre cómo se debe gestionar, proteger y acceder a la información en cada fase de su ciclo, desde su creación hasta su eliminación o archivo seguro. Cada funcionario tiene responsabilidades bien definidas respecto a la protección de la información, lo que garantiza que se cumplan con los requisitos de seguridad establecidos y que cada acción relacionada con los datos sea realizada conforme a las mejores prácticas de seguridad.

Dentro de las políticas, se abordan aspectos fundamentales como el manejo seguro de los datos, que incluye el uso de cifrado y la implementación de controles de acceso estrictos, la correcta clasificación de la información según su nivel de sensibilidad, y el establecimiento de procedimientos de almacenamiento y transmisión seguros. También se enfatiza la necesidad de utilizar contraseñas robustas, como parte de las medidas preventivas para salvaguardar el acceso a los sistemas y recursos de información.

Estas políticas no solo contribuyen a preservar la confidencialidad, la integridad y la disponibilidad de los activos de información, sino que también fomentan una cultura organizacional centrada en la seguridad, asegurando que cada funcionario de la entidad actúe de manera responsable y comprometida con la protección de los datos sensibles en todo momento.

2.1.3. Gestión de riesgos:

El enfoque del MSPI hacia la gestión de riesgos es proactivo, basado en evaluaciones continuas y en una constante revisión de las amenazas que podrían comprometer la seguridad de la información. Este enfoque no solo se limita a identificar y evaluar los riesgos asociados a amenazas tanto internas como externas, sino que también prioriza la implementación de controles de mitigación que son eficaces para reducir la probabilidad de incidentes. Más allá de la prevención, el modelo asegura que los impactos derivados de cualquier evento adverso se minimicen al máximo, gracias a la integración de medidas de respuesta y recuperación adecuadas.

Adicionalmente, el MSPI incluye un sistema de monitoreo continuo que permite detectar de manera temprana cualquier indicio de riesgo o vulnerabilidad, garantizando que los planes de tratamiento de riesgos sean actualizados de forma periódica. Este monitoreo proactivo no solo facilita la adaptabilidad frente a nuevas amenazas y vulnerabilidades emergentes, sino que también permite a la entidad ajustar su estrategia de seguridad de forma dinámica y en tiempo real. De esta manera, se asegura que la postura de seguridad de la entidad esté siempre alineada con las mejores prácticas de la industria, así como con las normativas vigentes, fortaleciendo su capacidad para afrontar los desafíos de un entorno digital cada vez más complejo.

2.1.4. Concienciación y capacitación del personal:

El componente humano es un pilar fundamental para garantizar la efectividad del MSPI, ya que los usuarios, con sus conocimientos y comportamientos, desempeñan un papel crucial en la protección de la información. Por ello, se pone un énfasis particular en la concienciación y capacitación continua del personal, proporcionando formación regular en prácticas de seguridad cibernética, detección temprana de amenazas y procedimientos de manejo de incidentes. Esta formación se extiende a todos los niveles de la entidad, con el objetivo de que cada funcionario esté preparado para identificar posibles riesgos y responder adecuadamente ante cualquier eventualidad.

Además, se refuerza de manera constante la concienciación sobre la importancia de la privacidad, promoviendo que los funcionarios comprendan no solo la necesidad de proteger la información corporativa, sino también la información personal sensible. Esto implica un enfoque integral que abarca tanto la protección de datos internos como la gestión adecuada

de la información externa. Este compromiso con la seguridad y privacidad crea un ambiente de trabajo donde la protección de los activos de información se percibe como responsabilidad de todos los integrantes de la entidad. A través de este enfoque, se fomenta una cultura de seguridad sólida que asegura la integridad de la información y contribuye a consolidar un entorno seguro y confiable en todos los niveles organizacionales.

2.2 EVALUACIÓN DEL PROGRESO DE IMPLEMENTACIÓN.

Hasta la fecha, la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) ha progresado de manera significativa, gracias a la ejecución de una serie de actividades clave orientadas a reforzar la protección de la información sensible dentro de la entidad. Estas actividades se han centrado en varias áreas estratégicas, tales como el establecimiento de controles de seguridad, la definición de políticas y procedimientos claros, la gestión activa de riesgos, y el fortalecimiento de la sensibilización y capacitación del personal. A lo largo de este proceso, se ha priorizado la integración de las mejores prácticas en seguridad y privacidad, con un enfoque continuo en la adaptación a las normativas vigentes y las amenazas emergentes.

A continuación, se presenta un análisis exhaustivo de los logros alcanzados hasta el momento, detallando los avances realizados en cada una de las áreas mencionadas, así como una evaluación de la efectividad de las medidas implementadas. Este análisis se realizará en función de los objetivos establecidos en el Plan Estratégico de Seguridad y Privacidad de la Información (PESI), con el fin de valorar el impacto de las acciones realizadas y la alineación con los lineamientos estratégicos establecidos para el fortalecimiento continuo de la seguridad y la privacidad de la información en la entidad.

2.2.1. Establecimiento de controles de seguridad:

Se ha logrado un avance significativo en la implementación de controles de seguridad fundamentales para la protección de la información, tales como firewalls avanzados para la defensa perimetral, Sistemas de Detección y Prevención de Intrusiones (IDS/IPS) y sistemas de control de acceso basados en roles. Estos controles han demostrado ser efectivos en la mitigación de riesgos asociados a accesos no autorizados y en la protección de la información sensible frente a amenazas tanto internas como externas. No obstante, es fundamental continuar con la actualización y mejora constante de estas herramientas para asegurar que se mantengan alineadas con las nuevas amenazas cibernéticas. Asimismo, es necesario reforzar la vigilancia y los procesos de monitoreo continuo para identificar y mitigar rápidamente posibles vulnerabilidades emergentes, garantizando de esta forma una protección proactiva y adaptable frente a los riesgos de seguridad.

2.2.2. Definición de políticas y procedimientos:

Se ha establecido un marco sólido y bien documentado de políticas y procedimientos que regulan el manejo adecuado de la información sensible. Estas políticas abarcan áreas clave como el acceso y control de la información, el intercambio seguro de datos, la gestión de contraseñas robustas y los procedimientos de respuesta ante incidentes de seguridad.

Dichas directrices han proporcionado un enfoque estructurado y coherente para el uso y la protección de los datos, lo que ha sido fundamental para garantizar el cumplimiento normativo y la consistencia en las operaciones diarias. Sin embargo, durante la evaluación,

se identificó la necesidad de implementar un proceso de revisión periódica de estas políticas para asegurar que se mantengan actualizadas, vigentes y alineadas con posibles cambios regulatorios, operativos y tecnológicos. Esta actualización continua permitirá adaptar las políticas a nuevas amenazas y requerimientos, garantizando su efectividad en el largo plazo.

2.2.3. Gestión de riesgos:

La gestión de riesgos ha seguido un enfoque proactivo y continuo, con evaluaciones regulares de las vulnerabilidades asociadas a la información sensible. Este proceso ha implicado la identificación, clasificación y evaluación de riesgos en función de su impacto potencial y probabilidad de ocurrencia. Gracias a esta metodología, se han implementado medidas de mitigación específicas que han permitido adoptar controles preventivos efectivos, mejorar la capacidad de respuesta ante incidentes y reducir significativamente el impacto en caso de materialización de amenazas. Sin embargo, dado que el entorno digital está en constante evolución, es crucial mantener una actualización periódica de los planes de tratamiento de riesgos y los planes de continuidad del negocio correspondiente al proceso. Esta actualización debe contemplar los cambios en el panorama de amenazas, ajustando las medidas de seguridad de manera ágil y anticipada para abordar riesgos emergentes y garantizar la protección continua de los activos de información.

2.2.4. Sensibilización del personal:

La concienciación y capacitación del personal es un componente esencial del MSPI, ya que el factor humano juega un papel clave en la protección de la información. A lo largo de la implementación del modelo, se han realizado sesiones de formación regulares enfocadas en prácticas de seguridad de la información, detección de amenazas, y procedimientos de respuesta ante incidentes. Estas capacitaciones han sido fundamentales para crear una cultura sólida de seguridad dentro de la entidad, promoviendo una comprensión generalizada entre los funcionarios sobre la importancia de proteger la información y adherirse a las políticas y directrices establecidas. Sin embargo, el reto persiste en mantener al personal actualizado respecto a las últimas tendencias y amenazas cibernéticas, y en fortalecer su capacidad de respuesta para actuar con mayor agilidad y eficacia en la gestión de incidentes. La capacitación continua y la simulación de incidentes en tiempo real pueden ser medidas clave para mejorar la capacidad de respuesta y adaptabilidad del equipo frente a nuevas amenazas.

2.3 ANÁLISIS DE LA EJECUCIÓN DE ACTIVIDADES DEL PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN.

Durante la vigencia 2024, se llevó a cabo la ejecución de actividades conforme a lo establecido en el Plan Estratégico de Seguridad y Privacidad de la Información (PESI). A la fecha, se ha alcanzado un cumplimiento del 100% de las actividades programadas para este periodo, lo que refleja un avance significativo en la implementación de las iniciativas planteadas y evidencia el firme compromiso de la entidad con la mejora continua en materia de seguridad y privacidad de la información.

No obstante, aunque el cumplimiento general es positivo, se ha observado que algunas actividades fueron completadas fuera de los plazos planificados. Esta situación puede ser atribuida a diversos factores, tales como la falta de personal adecuado o herramientas necesarias para llevar a cabo las actividades dentro del tiempo previsto, la complejidad

técnica de ciertas tareas que requirieron más tiempo del anticipado, o la necesidad de coordinar acciones con otros procesos que implicaron ajustes en el cronograma. Además, en algunos casos, la dinámica interna de la entidad llevó a redirigir recursos hacia actividades más urgentes, lo que afectó el cumplimiento de los plazos establecidos.

Identificar y abordar estos retrasos es un paso fundamental para fortalecer el PESI y asegurar la eficacia de sus medidas. Para mejorar el desempeño en la próxima vigencia, se implementarán varias acciones correctivas. Se establecerán reuniones de seguimiento más frecuentes para monitorear de cerca el progreso de las actividades y resolver posibles inconvenientes de manera oportuna. Además, se analizará la posibilidad de incrementar los recursos disponibles y mejorar la capacitación del personal, con el fin de optimizar la capacidad operativa y asegurar el cumplimiento de los plazos establecidos. También se llevará a cabo una reevaluación de las actividades planificadas y su cronograma, realizando ajustes donde sea necesario para garantizar que los plazos sean realistas y alcanzables.

A través de estas medidas, se pretende no solo mejorar el cumplimiento de las actividades programadas, sino también optimizar la eficacia del PESI, asegurando que las iniciativas de seguridad y privacidad se implementen de manera eficiente y en el tiempo adecuado. Esto contribuirá de manera significativa a la protección de la información dentro de la entidad, un aspecto clave para mantener la confianza de los usuarios y cumplir con las normativas vigentes.

A continuación, se presenta un análisis detallado de la ejecución de las actividades establecidas en el Plan Estratégico de Seguridad y Privacidad de la Información (PESI) 2024. Este análisis tiene como objetivo evaluar la alineación entre las actividades ejecutadas y los objetivos estratégicos definidos en el plan, con el fin de identificar áreas de mejora y asegurar el cumplimiento de las metas propuestas.

Para realizar esta evaluación, se llevó a cabo una comparación exhaustiva entre las tareas planificadas y aquellas que se han completado efectivamente hasta la fecha, permitiendo medir el progreso real frente a lo estipulado en el PESI.

En el marco de la gestión del PESI, se identificaron un total de 57 tareas proyectadas para su ejecución durante la vigencia del plan. Estas tareas fueron diseñadas específicamente para respaldar el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) y aumentar la madurez del modelo, lo que a su vez garantiza la efectividad y la mejora continua de las medidas de seguridad y privacidad implementadas en la entidad.

Hasta el periodo analizado, con corte al 20 de enero de 2025, se tenían programadas un total de 57 tareas para este intervalo de tiempo. De estas, las 57 tareas fueron ejecutadas de manera apropiada, lo que representa un avance real del 100% respecto a las actividades previstas en este período. Si bien este avance es óptimo, también pone en evidencia la necesidad de adoptar un enfoque más riguroso y enfocado para asegurar el cumplimiento de los plazos y metas establecidos.

Este análisis no solo refleja los logros alcanzados hasta la fecha, sino que también resalta la importancia de intensificar los esfuerzos en las áreas pendientes para asegurar que el PESI se ejecute de forma exitosa en su totalidad. A continuación, se presenta un desglose de las actividades ejecutadas, con detalles sobre el estado de cada una de ellas, las causas de

posibles retrasos y las acciones correctivas que se están implementando para mejorar la ejecución del plan.

2.3.1. Actividades completadas con éxito.

Se han identificado un total de cincuenta y siete (57) actividades que han sido completadas con éxito dentro del marco del Plan Estratégico de Seguridad y Privacidad de la Información (PESI) 2024. Estas actividades han cumplido con los criterios evaluables establecidos, respetando tanto los tiempos como los recursos asignados, y han contribuido de manera significativa al logro de los objetivos estratégicos de la entidad. Este avance refleja el compromiso con la mejora continua en la protección de la información y el cumplimiento de los estándares de seguridad establecidos.

Con la reciente actualización de la norma ISO 27001, se ha decidido que la gestión y aplicación de controles se realizará también utilizando la nueva versión del Anexo "A". Esta decisión estratégica tiene como objetivo asegurar la compatibilidad con las versiones anteriores de la norma ISO/IEC 27001:2013, dado que el Modelo de Seguridad y Privacidad de la Información (MSPI) aún no ha sido actualizado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Es importante destacar que esta actualización ofrecerá un marco más robusto para la implementación de controles de seguridad, lo cual permitirá a la entidad adaptarse de manera más eficiente a los nuevos desafíos del entorno digital, mejorando continuamente su postura de seguridad y garantizando la protección de la información sensible.

Además, se está considerando que la transición a esta nueva versión de la norma sea lo más fluida posible, con el fin de evitar dificultades en el momento en que los entes reguladores implementen las mejoras correspondientes al MSPI en el futuro. De esta manera, la entidad podrá mantener su alineación con los estándares internacionales y garantizar que sus procesos de seguridad y privacidad estén siempre a la vanguardia.

Tabla 1.
Actividades finalizadas vigencia 2024.

ACTIVIDADES COMPLETADAS					
ÍTEM	**TAREA**	**FECHA INICIO**	**FECHA FINAL**	**ENTREGABLE**	**PROCESO EJECUTOR**
01	Plan de actividades de sensibilización y concientización en temas relacionados a seguridad digital y de la información dirigido a todos los funcionarios de la entidad (Elaboración del Plan).	01/02/2024	07/03/2024	Plan de sensibilización y capacitación a los funcionarios de la ALFM.	Proceso Gestión de TIC.
	Análisis del avance.				
	La actividad termino a tiempo, finalizada el día 26 de febrero de 2024, cuya aprobación fue realizada el mismo día. Con el desarrollo de esta actividad se pretende incrementar la madurez de los siguientes controles: - **A.7.2.2 (ISO/IEC:2013):** Toma de conciencia, educación y formación en la seguridad de la información.				

- **A.6.3 (ISO/IEC:2022):** Sensibilización, educación y formación en temas de seguridad de la información.

Nivel de cumplimiento MSPI: 80%

Impacto: Este control se centra en la necesidad de asegurar que todos los funcionarios entiendan la importancia de la seguridad de la información y estén capacitados para actuar de manera adecuada. La elaboración del Plan de sensibilización y concientización es fundamental para cumplir con este control, ya que proporciona el marco necesario para educar a los funcionarios sobre las políticas, procedimientos y mejores prácticas de seguridad.

- **A.8.2.1 (ISO/IEC:2013):** Clasificación de la información.
- **A.5.12 (ISO/IEC:2022):** Clasificación de la información.

Nivel de cumplimiento MSPI: 80%

Impacto: Aunque no se refiere directamente a la sensibilización, la capacitación en seguridad digital puede incluir temas sobre la clasificación de la información, ayudando a los funcionarios a comprender cómo manejar adecuadamente la información sensible de acuerdo con su clasificación. Esto contribuye a la protección de la información y la reducción del riesgo de incidentes.

- **A.15.1.1 (ISO/IEC:2013):** Política de seguridad de la información para las relaciones con los proveedores.
- **A.5.19 (ISO/IEC:2022):** Seguridad de la información en las relaciones con los proveedores.

Nivel de cumplimiento MSPI: 60%

Impacto: La concienciación sobre la seguridad de la información también puede abarcar cómo interactuar con terceros y la importancia de proteger la información en esas relaciones. Aumentar la sensibilización en este aspecto puede ayudar a prevenir incidentes relacionados con la transferencia de información.

- **A.16.1.1 (ISO/IEC:2013):** Responsabilidades y procedimientos.
- **A.5.24 (ISO/IEC:2022):** Planificación y preparación de la gestión de incidentes de la seguridad de la información.

Nivel de cumplimiento MSPI: 100%

Impacto: Este control aborda la necesidad de que el personal esté informado sobre cómo manejar incidentes de seguridad. A través de la sensibilización, los funcionarios aprenden a identificar, reportar y reaccionar adecuadamente ante incidentes de seguridad, contribuyendo así a una gestión más efectiva de los mismos.

ÍTEM	TAREA	FECHA INICIO	FECHA FINAL	ENTREGABLE	PROCESO EJECUTOR
02	Seguimiento al estado de avance de implementación del MSPI. (Trimestral).	01/02/2024 01/04/2024 01/07/2024 01/10/2024	05/04/2024 08/07/2024 04/10/2024 09/01/2025	Informe de seguimiento implementación MSPI, anexando el instrumento de evaluación del MSPI actualizado.	Proceso Gestión de TIC.
	Análisis del avance.				
	Primer trimestre: La actividad correspondiente al primer trimestre terminó después de la fecha planificada, finalizada el día 08 de abril de 2024 y la aprobación fue gestionada el día 09 de abril de 2024. **Segundo trimestre:** La actividad correspondiente al segundo trimestre termino a tiempo, finalizada el día 03 de julio de 2024, cuya aprobación fue realizada el mismo día. **Tercer trimestre:** La actividad correspondiente al tercer trimestre termino a tiempo, finalizada el día 04 de octubre de 2024, cuya aprobación fue gestionada el día 16 de octubre de 2024. **Cuarto trimestre:** La actividad correspondiente al cuarto trimestre terminó después de la fecha				

planificada, finalizada el día 20 de enero de 2025, cuya aprobación fue realizada el mismo día.

Con el desarrollo de esta actividad se pretende incrementar la madurez de los siguientes controles:

- **A.6.1.1 (ISO/IEC:2013):** Funciones y responsabilidades de seguridad de la información.
- **A.5.2 (ISO/IEC:2022):** Funciones y responsabilidades en materia de seguridad de la información.

Nivel de cumplimiento MSPI: 80%

Impacto: Esta actividad involucra la verificación de que los roles y responsabilidades definidos en el MSPI se estén cumpliendo. Es clave asegurar que los responsables del seguimiento y la implementación estén llevando a cabo sus funciones de manera adecuada, lo cual está directamente relacionado con la correcta asignación de roles en la seguridad de la información.

- **A.16.1.6 (ISO/IEC:2013):** Aprendizaje obtenido de los incidentes de seguridad de la información.
- **A.5.27 (ISO/IEC:2022):** Aprendizaje de los incidentes de seguridad de la información.

Nivel de cumplimiento MSPI: 60%

Impacto: Durante el seguimiento al MSPI, es posible que se identifiquen incidentes pasados o áreas de mejora. Este control promueve el aprendizaje a partir de incidentes anteriores para optimizar los controles y procesos. Si se revisa el progreso del MSPI, también se puede evaluar cómo se han gestionado incidentes y si se ha aprendido de ellos.

- **A.18.2.1 (ISO/IEC:2013):** Revisión independiente de la seguridad de la información.
- **A.5.35 (ISO/IEC:2022):** Revisión independiente de la seguridad de la información.

Nivel de cumplimiento MSPI: 80%

Impacto: El seguimiento al estado de implementación del MSPI podría implicar una revisión o auditoría interna para evaluar el avance del modelo. Este control se refiere a la necesidad de realizar auditorías periódicas para asegurar que las medidas de seguridad se implementen adecuadamente.

- **A.18.2.2 (ISO/IEC:2013):** Cumplimiento con las políticas y normas de seguridad.
- **A.5.36 (ISO/IEC:2022):** Cumplimiento de políticas, reglas y normas de seguridad de la información.

Nivel de cumplimiento MSPI: 60%

Impacto: Evaluar el progreso de la implementación del MSPI permite verificar el cumplimiento de los controles de seguridad establecidos. Este control se enfoca en asegurar que los controles implementados estén siendo seguidos de manera correcta y cumplan con los requisitos normativos.

ÍTEM	TAREA	FECHA INICIO	FECHA FINAL	ENTREGABLE	PROCESO EJECUTOR
03	Actualización del inventario de activos de información (Guía para la gestión de activos de información).	01/02/2024	05/04/2024	Guía para la gestión y clasificación de activos de información actualizada.	Proceso Gestión de TIC.
	Actualización del inventario de activos de información. (Oficina Principal - Regionales). (Semestral)	01/02/2024 01/07/2024	08/07/2024 09/01/2025	Matriz de activos de información actualizada.	Todos los Procesos.
	Análisis del avance.				
	La actividad termino después de la fecha planificada, finalizada el día 15 de abril de 2024, cuya aprobación fue realizada el mismo día. Con el desarrollo de esta actividad se pretende incrementar la madurez de los siguientes controles: - **A.8.1.1 (ISO/IEC:2013):** Inventario de activos.				

- **A.5.9 (ISO/IEC:2022):** Inventario de activos de información y otros activos asociados.

Nivel de cumplimiento MSPI: 80%

Impacto: Este control requiere que se mantenga un inventario preciso de los activos importantes para la seguridad de la información. La actividad de actualización del inventario de activos está directamente alineada con este control, ya que implica la identificación y documentación de los activos de información, lo que permite gestionarlos de forma adecuada y garantizar su protección.

- **A.8.1.2 (ISO/IEC:2013):** Propiedad de los activos.
- **A.5.9 (ISO/IEC:2022):** Inventario de activos de información y otros activos asociados.

Nivel de cumplimiento MSPI: 80%

Impacto: El control establece que se debe asignar un responsable para cada activo, garantizando que haya una persona o entidad encargada de su protección y mantenimiento. La actualización del inventario debe reflejar la asignación clara de propietarios para cada activo, lo que asegura un control más eficaz sobre los activos de información.

- **A.8.1.3 (ISO/IEC:2013):** Uso aceptable de los activos.
- **A.5.10 (ISO/IEC:2022):** Uso aceptable de la información y los activos asociados.

Nivel de cumplimiento MSPI: 80%

Impacto: La guía de gestión de activos actualizada incluye reglas sobre el uso aceptable de los activos de información. Este control busca garantizar que los activos se utilicen solo de forma autorizada y conforme a las políticas definidas, protegiendo así su integridad, confidencialidad y disponibilidad.

- **A.8.2.1 (ISO/IEC:2013):** Clasificación de la información.
- **A.5.12 (ISO/IEC:2022):** Clasificación de la información.

Nivel de cumplimiento MSPI: 80%

Impacto: La actividad de actualización del inventario también considera la clasificación de los activos de información según su nivel de sensibilidad. Este control exige que los activos de información se clasifiquen para asegurar que se les dé el nivel adecuado de protección. Actualizar el inventario permite asegurar que la clasificación sea correcta y se mantenga al día.

- **A.8.2.3 (ISO/IEC:2013):** Manejo de activos.
- **A.5.10 (ISO/IEC:2022):** Uso aceptable de la información y los activos asociados.

Nivel de cumplimiento MSPI: 80%

Impacto: El control exige la adecuada gestión de los activos durante todas las fases de su ciclo de vida, desde su adquisición hasta su disposición final. La actividad de actualización del inventario debe reflejar el estado de cada activo y asegurar que se sigan los procedimientos adecuados en cada etapa de su ciclo de vida.

- **A.8.3.1 (ISO/IEC:2013):** Gestión de medios removibles.
- **A.7.10 (ISO/IEC:2022):** Medios de almacenamiento.

Nivel de cumplimiento MSPI: 60%

Impacto: Este control se refiere específicamente a la protección y uso correcto de medios removibles, lo cual es clave en la gestión de activos.

ÍTEM	TAREA	FECHA INICIO	FECHA FINAL	ENTREGABLE	PROCESO EJECUTOR
04	Seguimiento gestión plan de continuidad del negocio TIC ALFM (Gestión de formatos).	01/02/2024	05/04/2024	Documentos ajustados. (En caso de requerirse).	Proceso Gestión de TIC.

	Seguimiento gestión plan de continuidad del negocio TIC ALFM. (Semestral).	01/02/2024 01/07/2024	08/07/2024 09/01/2025	Informe de seguimiento al cumplimiento de actividades establecidas, mediante el Plan de Continuidad del negocio TIC ALFM.	

Análisis del avance.

Gestión de formatos: La actividad correspondiente a la gestión de formatos termino después de la fecha planificada, finalizada el día 15 de abril de 2024, cuya aprobación fue realizada el mismo día.

Primer Semestre: La actividad correspondiente al primer semestre terminó a tiempo, finalizada el día 04 de julio de 2024 y la aprobación fue gestionada el mismo día.

Segundo semestre: La actividad correspondiente al segundo semestre terminó después de la fecha planificada, finalizada el día 20 de enero de 2025, cuya aprobación fue realizada el mismo día.

Con el desarrollo de esta actividad se pretende incrementar la madurez de los siguientes controles:

- **A.12.3.1 (ISO/IEC:2013):** Respaldo de la información.
- **A.8.13 (ISO/IEC:2022):** Copias de seguridad de la información.

Nivel de cumplimiento MSPI: 80%

Impacto: Como parte de los planes de continuidad, la gestión de copias de seguridad de los sistemas y la información es clave. La actividad de seguimiento incluye garantizar que los formatos incluyan las estrategias adecuadas para la copia de seguridad y la recuperación de la información crítica.

- **A.16.1.5 (ISO/IEC:2013):** Respuesta a incidentes de seguridad de la información.
- **A.5.26 (ISO/IEC:2022):** Respuesta a incidentes de seguridad de la información.

Nivel de cumplimiento MSPI: 80%

Impacto: Aunque está más enfocado en la respuesta a incidentes de seguridad, este control es relevante porque el plan de continuidad del negocio también incluye cómo manejar incidentes críticos que afectan la disponibilidad de los servicios TIC. El seguimiento de los formatos garantiza que los procedimientos para mitigar el impacto de incidentes estén claros y listos para ser ejecutados.

- **A.17.1.1 (ISO/IEC:2013):** Planificación de la continuidad de la seguridad de la información.
- **A.5.29 (ISO/IEC:2022):** Seguridad de la información durante una interrupción.

Nivel de cumplimiento MSPI: 80%

Impacto: Este control requiere que se establezcan procesos para la continuidad de la seguridad de la información dentro de la entidad, asegurando que se mantenga incluso en situaciones adversas. El seguimiento y la gestión del plan de continuidad del negocio TIC directamente contribuye a la evaluación y adecuación de las medidas para asegurar la disponibilidad de los sistemas críticos, en línea con este control.

- **A.17.1.2 (ISO/IEC:2013):** Implementación de la continuidad de la seguridad de la información.
- **A.5.29 (ISO/IEC:2022):** Seguridad de la información durante una interrupción.

Nivel de cumplimiento MSPI: 40%

Impacto: Este control se enfoca en implementar y mantener procedimientos para garantizar la continuidad de la seguridad de la información en eventos de interrupción o desastre. El seguimiento de la gestión del plan de continuidad del negocio asegura que estos procedimientos estén documentados, actualizados y efectivos, lo cual es clave para la recuperación rápida de los servicios TIC en ALFM.

- **A.17.1.3 (ISO/IEC:2013):** Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- **A.5.29 (ISO/IEC:2022):** Seguridad de la información durante una interrupción.

Nivel de cumplimiento MSPI: 60%

Impacto: Este control requiere la verificación y evaluación regular de los planes de continuidad para asegurarse de que sean efectivos y estén alineados con los riesgos. La actividad de seguimiento de los formatos de gestión del plan de continuidad está directamente relacionada con este control, ya que garantiza la revisión periódica de los procedimientos y la mejora continua en respuesta a incidentes o simulacros.

- **A.17.2.1 (ISO/IEC:2013):** Disponibilidad de instalaciones de procesamiento de información.
- **A.8.14 (ISO/IEC:2022):** Redundancia de las instalaciones de tratamiento de información.

Nivel de cumplimiento MSPI: 80%

Impacto: Este control establece que se deben identificar y asignar los recursos necesarios para garantizar la continuidad de los sistemas de información críticos. La gestión del plan de continuidad incluye asegurar que los formatos y procedimientos tengan los recursos adecuados asignados para que sean implementados correctamente en caso de incidentes.

ÍTEM	TAREA	FECHA INICIO	FECHA FINAL	ENTREGABLE	PROCESO EJECUTOR
05	Revisión acuerdos de confidencialidad y no divulgación a funcionarios y contratistas.	01/02/2024	05/04/2024	Acuerdos de confidencialidad y no divulgación ajustados. (En caso de requerirse).	Proceso Gestión de TIC.

Análisis del avance.

La actividad termino después de la fecha planificada, finalizada el día 15 de abril de 2024, cuya aprobación fue realizada el mismo día.

Con el desarrollo de esta actividad se pretende incrementar la madurez de los siguientes controles:

- **A.7.1.2 (ISO/IEC:2013):** Términos y condiciones del empleo.
- **A.6.2 (ISO/IEC:2022):** Condiciones del empleo.

Nivel de cumplimiento MSPI: 100%

Impacto: Este control establece que todos los funcionarios y contratistas deben estar sujetos a términos y condiciones de empleo que incluyan obligaciones sobre la seguridad de la información. Los acuerdos de confidencialidad y no divulgación aseguran que funcionarios y contratistas comprendan sus responsabilidades en cuanto a la protección de la información sensible, reduciendo riesgos de fuga de información.

- **A.8.1.3 (ISO/IEC:2013):** Uso aceptable de los activos.
- **A.5.10 (ISO/IEC:2022):** Uso aceptable de la información y los activos asociados.

Nivel de cumplimiento MSPI: 80%

Impacto: Este control asegura que se definan y comuniquen claramente las reglas para el uso de los activos de información, incluyendo acuerdos de confidencialidad. La revisión de estos acuerdos verifica que todos los involucrados entienden y aceptan las reglas de uso adecuado, lo que protege los activos de información de la entidad.

- **A.13.2.4 (ISO/IEC:2013):** Acuerdos de confidencialidad o de no divulgación.
- **A.6.6 (ISO/IEC:2022):** Acuerdos de confidencialidad o no divulgación.

Nivel de cumplimiento MSPI: 100%

	Impacto: Este control exige que se establezcan acuerdos de confidencialidad o no divulgación para proteger la información intercambiada entre la organización y terceros. La revisión de estos acuerdos garantiza que estén actualizados y alineados con las necesidades de protección de la entidad, cubriendo aspectos clave sobre el manejo de la información sensible por parte de contratistas y funcionarios. - **A.15.1.1 (ISO/IEC:2013):** Política de seguridad de la información para las relaciones con proveedores. - **A.5.19 (ISO/IEC:2022):** Seguridad de la información en las relaciones con los proveedores. **Nivel de cumplimiento MSPI:** 60% **Impacto:** Este control establece que la seguridad de la información debe ser considerada en las relaciones con proveedores. Los acuerdos de confidencialidad para contratistas son una parte fundamental para asegurar que los proveedores y terceros no divulguen información sensible o la utilicen de manera indebida. - **A.15.1.2 (ISO/IEC:2013):** Tratamiento de la seguridad dentro de los acuerdos con proveedores. - **A.5.20 (ISO/IEC:2022):** Abordar la seguridad de la información en los acuerdos con los proveedores. **Nivel de cumplimiento MSPI:** 60% **Impacto:** Este control se refiere a la obligación de garantizar que los acuerdos con proveedores cubran todas las obligaciones relacionadas con la seguridad de la información. La revisión de los acuerdos de no divulgación garantiza que las expectativas sobre la protección de la información se definan claramente y se gestionen de manera adecuada en el contexto de las relaciones contractuales. - **A.16.1.4 (ISO/IEC:2013):** Evaluación de eventos de seguridad de la información y decisiones sobre ellos. - **A.5.25 (ISO/IEC:2022):** Evaluación y decisión sobre eventos de seguridad de la información. **Nivel de cumplimiento MSPI:** 80% **Impacto:** Aunque relacionado con la gestión de incidentes, este control se ve afectado de forma indirecta, ya que la existencia de acuerdos de confidencialidad y no divulgación ayuda a prevenir incidentes relacionados con el mal uso o la divulgación no autorizada de la información. En caso de incidentes, estos acuerdos también determinan las responsabilidades legales y correctivas.

ÍTEM	TAREA	FECHA INICIO	FECHA FINAL	ENTREGABLE	PROCESO EJECUTOR
06	Reporte de novedades de personal (retiros, incapacidades, licencias, vacaciones, entre otros). (Trimestral).	01/02/2024 01/04/2024 01/07/2024 01/10/2024	05/04/2024 08/07/2024 07/10/2024 09/01/2025	Soportes del reporte previo mediante correo electrónico de las novedades de personal emitidos a la Oficina TIC.	Proceso Gestión de Talento Humano.
	Análisis del avance.				
	Primer Trimestre: La actividad correspondiente al primer trimestre terminó después de la fecha planificada, finalizada el día 08 de mayo de 2024, su revisión fue efectuada el día 10 de mayo de 2024 y la aprobación fue realizada el mismo día. **Segundo Trimestre:** La actividad correspondiente al segundo trimestre terminó después de la fecha planificada, finalizada el día 09 de julio de 2024, su revisión fue efectuada el día 11 de julio de 2024 y la aprobación fue realizada el día 12 de julio de 2024. **Tercer Trimestre:** La actividad correspondiente al tercer trimestre terminó después de la fecha planificada, finalizada el día 01 de noviembre de 2024, su revisión fue efectuada el día 05 de noviembre de 2024 y la aprobación fue realizada el día 08 de noviembre de 2024. **Cuarto Trimestre:** La actividad correspondiente al cuarto trimestre terminó después de la fecha planificada, finalizada el día 20 de enero de 2024, su revisión y aprobación fue realizada el mismo día.				

Con el desarrollo de esta actividad se pretende incrementar la madurez de los siguientes controles:

- **A.7.1.1 (ISO/IEC:2013):** Selección.
- **A.6.1 (ISO/IEC:2022):** Selección.

Nivel de cumplimiento MSPI: 100%

Impacto: Este control cubre el proceso de selección de personal y la formalización de las condiciones laborales. Si bien está más centrado en la incorporación de personal, el reporte de novedades garantiza que los términos de salida, como retiros o licencias, se gestionen adecuadamente y se cumplan todas las condiciones relacionadas con la seguridad de la información.

- **A.7.3.1 (ISO/IEC:2013):** Terminación o cambio de responsabilidades de empleo.
- **A.6.5 (ISO/IEC:2022):** Responsabilidades después de la terminación o cambio de empleo.

Nivel de cumplimiento MSPI: 80%

Impacto: Este control requiere la implementación de procesos para gestionar la seguridad de la información cuando un funcionario cambia de rol o deja la entidad. El reporte de novedades, como los retiros, asegura que se tomen las medidas necesarias para desactivar cuentas, recuperar activos y garantizar que no quede ningún acceso pendiente o información en manos de un exfuncionario.

- **A.9.2.1 (ISO/IEC:2013):** Registro y cancelación del registro de usuarios.
- **A.5.16 (ISO/IEC:2022):** Gestión de identidades.

Nivel de cumplimiento MSPI: 80%

Impacto: El control exige la creación, modificación y eliminación de usuarios de acuerdo con su situación laboral. La información proporcionada en el reporte de novedades permite que el Proceso Gestión de TIC ajuste los accesos, inactivando aquellos de funcionarios retirados, en licencia o incapacidad, minimizando riesgos de accesos no controlados.

- **A.9.2.3 (ISO/IEC:2013):** Gestión de derechos de acceso privilegiado.
- **A.8.2 (ISO/IEC:2022):** Derechos de acceso privilegiados.

Nivel de cumplimiento MSPI: 60%

Impacto: Este control establece la necesidad de gestionar los derechos de acceso de los usuarios cuando hay cambios en su rol o cuando finaliza su relación con la organización. Los reportes de novedades de personal, como retiros o incapacidades, deben desencadenar acciones para ajustar o revocar los accesos de los usuarios de forma oportuna, reduciendo el riesgo de acceso no autorizado a la información.

- **A.13.2.4 (ISO/IEC:2013):** Acuerdos de confidencialidad o de no divulgación.
- **A.6.6 (ISO/IEC:2022):** Acuerdos de confidencialidad o no divulgación.

Nivel de cumplimiento MSPI: 100%
Impacto: Este control también es relevante cuando se produce un retiro o cambio en las responsabilidades laborales. Se debe garantizar que los acuerdos de confidencialidad y no divulgación se mantengan vigentes y que los funcionarios que dejan la entidad sigan respetando estos acuerdos.

ÍTEM	TAREA	FECHA INICIO	FECHA FINAL	ENTREGABLE	PROCESO EJECUTOR
07	Seguimiento al estado avance del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. (Cuatrimestral).	01/02/2024 01/05/2024 01/09/2024	08/05/2024 06/09/2024 09/01/2025	Informe de seguimiento ejecución del Plan.	Proceso Gestión de TIC.
	Análisis del avance.				
	Primer Cuatrimestre: La actividad correspondiente al primer cuatrimestre terminó a tiempo, finalizada el				

día 06 de mayo de 2024 y la aprobación fue realizada el mismo día.

Segundo Cuatrimestre: La actividad correspondiente al segundo cuatrimestre terminó después de la fecha planificada, finalizada el día 13 de septiembre de 2024 y la aprobación fue realizada el mismo día.

Tercer Cuatrimestre: La actividad correspondiente al segundo cuatrimestre terminó después de la fecha planificada, finalizada el día 20 de enero de 2025 y la aprobación fue realizada el mismo día.

Con el desarrollo de esta actividad se pretende incrementar la madurez de los siguientes controles:

- **6.1.3 (ISO/IEC:2013):** Tratamiento de riesgos de la seguridad de la información.

  Nivel de cumplimiento MSPI: 100%

  Impacto: Este control establece la necesidad de implementar un proceso formal para la gestión de riesgos relacionados con la seguridad de la información, lo que incluye identificar, evaluar y tratar los riesgos de manera sistemática. El seguimiento del estado del Plan de Tratamiento de Riesgos asegura que los riesgos identificados se estén gestionando conforme a los controles establecidos, y que las medidas de mitigación estén en progreso o se hayan implementado correctamente.

- **A.8.1.1 (ISO/IEC:2013):** Inventario de activos.
- **A.5.9 (ISO/IEC:2022):** Inventario de activos de información y otros activos asociados.

  Nivel de cumplimiento MSPI: 80%

  Impacto: Aunque no directamente un control de gestión de riesgos, este control es clave en la etapa inicial del tratamiento de riesgos. El seguimiento del plan incluye la correcta identificación y categorización de los activos, de modo que los riesgos asociados a cada uno se traten de acuerdo con su criticidad y valor para la entidad.

- **A.12.6.1 (ISO/IEC:2013):** Gestión de las vulnerabilidades técnicas.
- **A.8.8 (ISO/IEC:2022):** Gestión de las vulnerabilidades técnicas.

  Nivel de cumplimiento MSPI: 80%

  Impacto: Durante el seguimiento del Plan de Tratamiento de Riesgos, se incluye la evaluación y gestión de vulnerabilidades técnicas identificadas. Este control exige que las vulnerabilidades conocidas sean gestionadas a tiempo, lo cual se asegura mediante la verificación continua del plan, permitiendo a la entidad ajustar los controles en función de nuevas amenazas y vulnerabilidades.

- **A.16.1.1 (ISO/IEC:2013):** Responsabilidades y procedimientos.
- **A.5.24 (ISO/IEC:2022):** Planificación y preparación de la gestión de incidentes de la seguridad de la información.

  Nivel de cumplimiento MSPI: 100%

  Impacto: La actividad de seguimiento permite identificar posibles incidentes o eventos que podrían convertirse en incidentes si no se gestionan adecuadamente los riesgos. Este control establece la necesidad de un proceso de gestión de incidentes que sea coherente con el tratamiento de riesgos, garantizando que cualquier incidente relacionado con los riesgos identificados sea tratado con prontitud.

- **A.17.1.1 (ISO/IEC:2013):** Planificación de la continuidad de la seguridad de la información.
- **A.5.29 (ISO/IEC:2022):** Seguridad de la información durante una interrupción.

  Nivel de cumplimiento MSPI: 80%

  Impacto: La planificación de la continuidad de la seguridad de la información está estrechamente relacionada con el tratamiento de riesgos. El seguimiento del estado del plan debe asegurar que los riesgos que pueden afectar la continuidad del negocio se gestionen de forma adecuada y que los controles de mitigación estén bien implementados.

	- **A.18.1.3 (ISO/IEC:2013):** Protección de registros. - **A.5.33 (ISO/IEC:2022):** Protección de los registros. **Nivel de cumplimiento MSPI:** 60% **Impacto:** El seguimiento del plan de tratamiento incluye la verificación de que los registros y evidencias relacionados con la gestión de riesgos se mantengan íntegros y protegidos. Este control exige que los registros sobre el tratamiento de riesgos sean protegidos, garantizando la trazabilidad y el cumplimiento normativo.				
ÍTEM	**TAREA**	**FECHA INICIO**	**FECHA FINAL**	**ENTREGABLE**	**PROCESO EJECUTOR**
08	Plan de actividades de sensibilización y concientización en temas relacionados a seguridad digital y de la información dirigido a todos los funcionarios de la entidad. (Cuatrimestral).	01/02/2024 01/05/2024 01/09/2024	08/05/2024 06/09/2024 09/01/2025	Informes de seguimiento a la ejecución del plan de actividades de sensibilización y concientización.	Proceso Gestión de TIC.
	Análisis del avance.				
	Primer Cuatrimestre: La actividad correspondiente al primer cuatrimestre terminó a tiempo, finalizada el día 06 de mayo de 2024 y la aprobación fue realizada el mismo día. **Segundo Cuatrimestre:** La actividad correspondiente al segundo cuatrimestre terminó después de la fecha planificada, finalizada el día 13 de septiembre de 2024 y la aprobación fue realizada el mismo día. **Tercer Cuatrimestre:** La actividad correspondiente al tercer cuatrimestre terminó después de la fecha planificada, finalizada el día 20 de enero de 2025 y la aprobación fue realizada el mismo día. Con el desarrollo de esta actividad se pretende incrementar la madurez de los siguientes controles: - **A.6.1.1 (ISO/IEC:2013):** Roles y responsabilidades para la seguridad de la información. - **A.5.2 (ISO/IEC:2022):** Funciones y responsabilidades en materia de seguridad de la información. **Nivel de cumplimiento MSPI:** 80% **Impacto:** La sensibilización de los funcionarios en temas de seguridad refuerza este control, que exige una asignación clara de roles y responsabilidades. El plan de sensibilización asegura que los funcionarios sean conscientes de sus responsabilidades específicas en cuanto a la protección de la información y el cumplimiento de las políticas de seguridad de la entidad. - **A.7.2.2 (ISO/IEC:2013):** Toma de conciencia, educación y formación en la seguridad de la información. - **A.6.3 (ISO/IEC:2022):** Sensibilización, educación y formación en temas de seguridad de la Información. **Nivel de cumplimiento MSPI:** 80% **Impacto:** Este control se centra en garantizar que todos los funcionarios reciben formación adecuada y están concienciados sobre los riesgos de seguridad de la información, así como sobre las políticas, procedimientos y responsabilidades que deben cumplir. El desarrollo de un plan de actividades de sensibilización y concienciación responde directamente a este control, ya que busca capacitar a los funcionarios para que comprendan su papel en la protección de los activos de información de la entidad. - **A.8.2.1 (ISO/IEC:2013):** Clasificación de la información. - **A.5.12 (ISO/IEC:2022):** Clasificación de la información. **Nivel de cumplimiento MSPI:** 80% **Impacto:** Aunque este control está directamente relacionado con la clasificación de la información, la				

formación y concienciación de los funcionarios en cuanto a cómo manejar adecuadamente la información de acuerdo con su nivel de clasificación es esencial. Un plan de concienciación asegura que los empleados comprendan las políticas de clasificación y protección de la información sensible, confidencial y pública.

- **A.16.1.4 (ISO/IEC:2013):** Evaluación de eventos de seguridad de la información y decisiones sobre ellos.
- **A.5.25 (ISO/IEC:2022):** Evaluación y decisión sobre eventos de seguridad de la información.

Nivel de cumplimiento MSPI: 80%

Impacto: La capacitación de los funcionarios también cubre la capacidad de identificar, reportar y responder a incidentes de seguridad de la información. El plan de sensibilización ayuda a asegurar que el personal sea consciente de los procedimientos adecuados para la detección y notificación de incidentes de seguridad, lo que fortalece la respuesta rápida y efectiva ante cualquier evento.

- **A.17.2.1 (ISO/IEC:2013):** Disponibilidad de instalaciones de procesamiento de información.
- **A.8.14 (ISO/IEC:2022):** Redundancia de las instalaciones de tratamiento de información.

Nivel de cumplimiento MSPI: 80%

Impacto: En situaciones de contingencia o desastre, la concienciación del personal sobre sus responsabilidades y la correcta implementación de los planes de continuidad son clave. El plan de formación refuerza el conocimiento sobre cómo mantener la seguridad de la información incluso durante situaciones críticas.

- **A.18.2.2 (ISO/IEC:2013):** Cumplimiento con las políticas y normas de seguridad.
- **A.5.36 (ISO/IEC:2022):** Cumplimiento de políticas, reglas y normas de seguridad de la información.

Nivel de cumplimiento MSPI: 60%

Impacto: El cumplimiento de los requisitos legales, regulatorios y contractuales depende en gran medida de que los funcionarios conozcan y sigan las normativas aplicables. El plan de concienciación ayuda a garantizar que los funcionarios comprendan y respeten las obligaciones relacionadas con la seguridad de la información, reduciendo el riesgo de incumplimientos.

ÍTEM	TAREA	FECHA INICIO	FECHA FINAL	ENTREGABLE	PROCESO EJECUTOR
09	Intercambiar y/o compartir con el CSIRT, COLCERT, CAIVIRUTAL, (DIJIN) y CCOC para apoyar la gestión de riesgos y la toma de decisiones (priorización, tratamiento y aceptación, respuesta a incidentes), especialmente, para prevenir interna y externamente amenazas cibernéticas. (Cuatrimestral).	01/02/2024 01/05/2024 01/09/2024	08/05/2024 06/09/2024 09/01/2025	Soportes mensajes de correos electrónicos generados.	Proceso Gestión de TIC.
	Análisis del avance.				
	Primer Cuatrimestre: La actividad correspondiente al primer cuatrimestre terminó a tiempo, finalizada el día 03 de mayo de 2024 y la aprobación fue realizada el día 06 de mayo de 2024. **Segundo Cuatrimestre:** La actividad correspondiente al segundo cuatrimestre terminó a tiempo, finalizada el día 04 de septiembre de 2024 y la aprobación fue realizada el día 05 de septiembre de 2024. **Tercer Cuatrimestre:** La actividad correspondiente al tercer cuatrimestre terminó a tiempo, finalizada el día 08 de enero de 2025 y la aprobación fue realizada el día 09 de enero de 2025.				

Con el desarrollo de esta actividad se pretende incrementar la madurez de los siguientes controles:

- **A.6.1.4 (ISO/IEC:2013):** Contacto con grupos de interés especial.
- **A.5.6 (ISO/IEC:2022):** Contacto con grupos de interés especial.

Nivel de cumplimiento MSPI: 80%

Impacto: Este control establece que la entidad debe mantener contactos apropiados con las autoridades relevantes. En este caso, la interacción con entidades como COLCERT, DIJIN y CCOC fortalece el cumplimiento de este control, ya que permite una comunicación efectiva con las autoridades nacionales para prevenir amenazas cibernéticas, gestionar riesgos y coordinar la respuesta ante incidentes.

- **A.16.1.1 (ISO/IEC:2013):** Responsabilidades y procedimientos.
- **A.5.24 (ISO/IEC:2022):** Planificación y preparación de la gestión de incidentes de la seguridad de la información.

Nivel de cumplimiento MSPI: 100%

Impacto: Este control establece la necesidad de contar con procedimientos claros para la gestión de incidentes de seguridad de la información. La colaboración con entidades como el CSIRT y COLCERT mejora la capacidad de la entidad para detectar, responder y mitigar incidentes de seguridad cibernética, asegurando que los procedimientos internos estén alineados con las mejores prácticas y los recursos disponibles a nivel nacional o internacional.

- **A.16.1.2 (ISO/IEC:2013):** Reporte de eventos de seguridad de la información.
- **A.6.8 (ISO/IEC:2022):** Informes de eventos de seguridad de la información.

Nivel de cumplimiento MSPI: 100%

Impacto: La actividad de intercambio de información con organismos externos refuerza la capacidad de notificar adecuadamente los incidentes a las autoridades pertinentes, como lo establece este control. Colaborar con equipos como el CSIRT y otros entes permite a la entidad mejorar la velocidad y efectividad de la respuesta ante incidentes, ayudando en la recolección y análisis de datos sobre las amenazas.

- **A.16.1.4 (ISO/IEC:2013):** Evaluación de eventos de seguridad de la información y decisiones sobre ellos.
- **A.5.25 (ISO/IEC:2022):** Evaluación y decisión sobre eventos de seguridad de la información.

Nivel de cumplimiento MSPI: 80%

Impacto: Este control implica la evaluación detallada de los incidentes y la toma de decisiones informadas. El intercambio de información con entidades especializadas fortalece la capacidad de la entidad para analizar incidentes y adoptar decisiones estratégicas en la priorización y tratamiento de los riesgos asociados a los incidentes de seguridad cibernética.

ÍTEM	TAREA	FECHA INICIO	FECHA FINAL	ENTREGABLE	PROCESO EJECUTOR
10	Informes de seguimiento a los eventos de seguridad presentados (Fortisandbox). (Cuatrimestral).	01/02/2024 01/05/2024 01/09/2024	08/05/2024 06/09/2024 09/01/2025	Informes de seguimiento de eventos de seguridad.	Proceso Gestión de TIC.
	Análisis del avance.				
	Primer Cuatrimestre: La actividad correspondiente al primer cuatrimestre terminó después de la fecha planificada, finalizada el día 09 de mayo de 2024 y la aprobación fue realizada el mismo día. **Segundo Cuatrimestre:** La actividad correspondiente al segundo cuatrimestre terminó después de la fecha planificada, finalizada el día 09 de septiembre de 2024 y la aprobación fue realizada el día 10 de septiembre de 2024.				

Tercer Cuatrimestre: La actividad correspondiente al tercer cuatrimestre terminó a tiempo, finalizada el día 09 de enero de 2025 y la aprobación fue realizada el mismo día.

Con el desarrollo de esta actividad se pretende incrementar la madurez de los siguientes controles:

- **A.12.4.1 (ISO/IEC:2013):** Registro de eventos.
- **A.8.15 (ISO/IEC:2022):** Registros.

Nivel de cumplimiento MSPI: 60%

Impacto: Este control establece que los eventos en los sistemas de información deben ser registrados y revisados regularmente para garantizar su integridad y disponibilidad. El uso de FortiSandbox, una herramienta avanzada para analizar archivos sospechosos y detectar amenazas, permite generar informes sobre eventos de seguridad, asegurando que todos los incidentes y actividades anómalas sean monitoreados y documentados. El seguimiento de estos eventos facilita la identificación de patrones de comportamiento malicioso.

- **A.12.6.1 (ISO/IEC:2013):** Gestión de las vulnerabilidades técnicas.
- **A.8.8 (ISO/IEC:2022):** Gestión de las vulnerabilidades técnicas.

Nivel de cumplimiento MSPI: 80%

Impacto: Este control establece que los eventos en los sistemas de información deben ser registrados y revisados regularmente para garantizar su integridad y disponibilidad. El uso de FortiSandbox, una herramienta avanzada para analizar archivos sospechosos y detectar amenazas, permite generar informes sobre eventos de seguridad, asegurando que todos los incidentes y actividades anómalas sean monitoreados y documentados. El seguimiento de estos eventos facilita la identificación de patrones de comportamiento malicioso.

- **A.13.1.1 (ISO/IEC:2013):** Controles de redes.
- **A.8.20 (ISO/IEC:2022):** Seguridad de las redes.

Nivel de cumplimiento MSPI: 80%

Impacto: FortiSandbox, como parte de un ecosistema de seguridad, está estrechamente vinculado con la protección de la red. Este control garantiza que existan medidas adecuadas para proteger la seguridad de la red. El análisis de eventos de seguridad relacionados con la red ayuda a identificar y bloquear ataques avanzados, como malware de día cero y ataques dirigidos, mejorando la seguridad general de la infraestructura de red.

- **A.16.1.2 (ISO/IEC:2013):** Reporte de eventos de seguridad de la información.
- **A.6.8 (ISO/IEC:2022):** Informes de eventos de seguridad de la información.

Nivel de cumplimiento MSPI: 100%

Impacto: El análisis de eventos de seguridad mediante FortiSandbox puede revelar vulnerabilidades técnicas presentes en el entorno, ayudando a este control a identificar, priorizar y mitigar vulnerabilidades explotadas por posibles amenazas. Al seguir estos eventos y producir informes, la organización puede priorizar las actualizaciones de seguridad y remediar fallos antes de que se conviertan en incidentes graves.

- **A.18.1.3 (ISO/IEC:2013):** Protección de registros.
- **A.5.33 (ISO/IEC:2022):** Protección de los registros.

Nivel de cumplimiento MSPI: 60%

Impacto: La generación de informes de eventos de seguridad implica la creación de registros que deben ser protegidos adecuadamente. Este control establece que los registros deben ser protegidos contra modificaciones no autorizadas, y el uso de FortiSandbox para generar informes de eventos contribuye a garantizar que la información relacionada con la seguridad sea accesible solo para personal

	autorizado y esté protegida contra alteraciones.				
ÍTEM	**TAREA**	**FECHA INICIO**	**FECHA FINAL**	**ENTREGABLE**	**PROCESO EJECUTOR**
11	Actualización política de tratamiento de datos personales.	01/02/2024	17/06/2024	Política tratamiento de datos personales actualizada.	Proceso Gestión de TIC.
	Análisis del avance.				
	La actividad termino a tiempo, finalizada el día 17 de junio de 2024, cuya aprobación fue realizada el día 18 de junio de 2024. Con el desarrollo de esta actividad se pretende incrementar la madurez de los siguientes controles: - **A.8.2.3 (ISO/IEC:2013):** Manejo de activos. - **A.5.10 (ISO/IEC:2022):** Uso aceptable de la información y los activos asociados. **Nivel de cumplimiento MSPI:** 80% **Impacto:** La actualización de la política de tratamiento de datos personales también impacta en la clasificación de la información. Este control indica que la información debe ser clasificada de acuerdo con los requisitos legales, contractuales y de negocios. Los datos personales son un tipo de información sensible que requiere una protección específica, y la política actualizada debe reflejar cómo se clasificarán y manejarán estos datos de acuerdo con su nivel de sensibilidad. - **A.18.1.1 (ISO/IEC:2013):** Identificación de la legislación aplicable y de los requisitos contractuales. - **A.5.31 (ISO/IEC:2022):** Requisitos legales, reglamentarios y contractuales. **Nivel de cumplimiento MSPI:** 100% **Impacto:** La actualización de la política de tratamiento de datos personales ayuda a cumplir con las leyes y regulaciones locales e internacionales relacionadas con la protección de datos personales. Este control garantiza que las actividades de la entidad, incluidas las políticas de tratamiento de datos, cumplan con los marcos regulatorios y legales, como las leyes de protección de datos. - **A.18.1.4 (ISO/IEC:2013):** Privacidad y protección de información de datos personales. - **A.5.34 (ISO/IEC:2022):** Privacidad y protección de la Información de identificación personal – IIP. **Nivel de cumplimiento MSPI:** 60% **Impacto:** Este control exige que las entidades aseguren la privacidad y la protección de la información personal en cumplimiento con leyes y regulaciones aplicables. La actualización de la política de tratamiento de datos personales está directamente relacionada con este control, ya que establece los lineamientos para proteger los datos personales y garantizar que el manejo de la IIP cumpla con los requisitos legales y regulatorios vigentes.				
ÍTEM	**TAREA**	**FECHA INICIO**	**FECHA FINAL**	**ENTREGABLE**	**PROCESO EJECUTOR**
12	Revisión y seguimiento al uso de navegación web, de acuerdo con los perfiles asignados a los funcionarios. (Cuatrimestral).	01/02/2024 01/05/2024 01/09/2024	08/05/2024 06/09/2024 09/01/2025	Informes de revisión y seguimiento al uso de red (Perfiles de navegación medio y alto).	Proceso Gestión de TIC.
	Análisis del avance.				
	Primer Cuatrimestre: La actividad correspondiente al primer cuatrimestre terminó después de la fecha planificada, finalizada el día 18 de julio de 2024, la revisión y la aprobación fueron realizadas el mismo día. **Segundo Cuatrimestre:** La actividad correspondiente al segundo cuatrimestre terminó después de la fecha planificada, finalizada el día 18 de noviembre de 2024, la revisión fue el día 19 de noviembre de 2024 y la aprobación fue realizada el día 22 de noviembre de 2024.				

Tercer Cuatrimestre: La actividad correspondiente al tercer cuatrimestre termino a tiempo, finalizada el día 09 de enero de 2025, su revisión y aprobación fueron el día 10 de enero de 2025.

Con el desarrollo de esta actividad se pretende incrementar la madurez de los siguientes controles:

- **A.8.1.3 (ISO/IEC:2013):** Uso aceptable de los activos.
- **A.5.10 (ISO/IEC:2022):** Uso aceptable de la información y los activos asociados.

Nivel de cumplimiento MSPI: 80%

Impacto: Este control implica asegurar que los activos de información, incluidos los servicios de navegación web, se utilicen de manera adecuada de acuerdo con las políticas de la entidad. La revisión del uso de la web según los perfiles asignados busca garantizar que los funcionarios usen los recursos de Internet de manera coherente con las políticas de uso aceptable, asegurando que no se acceda a sitios web que puedan poner en riesgo la seguridad de la entidad.

- **A.9.4.1 (ISO/IEC:2013):** Restricción de acceso a la información.
- **A.8.3 (ISO/IEC:2022):** Restricciones de acceso a la información.

Nivel de cumplimiento MSPI: 60%

Impacto: Este control establece que el acceso a la información y a los servicios debe estar restringido en función de los perfiles y roles definidos para los usuarios. La revisión y seguimiento al uso de la navegación web se asegura de que los funcionarios tengan acceso solo a los recursos de Internet que son relevantes para sus funciones, y que se limiten accesos no autorizados a sitios web que puedan comprometer la seguridad.

- **A.12.4.1 (ISO/IEC:2013):** Registro de eventos.
- **A.8.15 (ISO/IEC:2022):** Registros.

Nivel de cumplimiento MSPI: 60%

Impacto: El monitoreo del uso de la navegación web implica el registro y seguimiento de las actividades en los sistemas. Este control especifica que las actividades del sistema deben ser monitoreadas y registradas para identificar accesos inapropiados o comportamientos anómalos. Revisar el uso de la navegación web según perfiles asignados contribuye a la detección de posibles abusos o incumplimientos de las políticas de seguridad.

- **A.12.6.2 (ISO/IEC:2013):** Restricciones sobre la instalación de software.
- **A.8.19 (ISO/IEC:2022):** Instalación de software en sistemas operativos.

Nivel de cumplimiento MSPI: 80%

Impacto: Aunque está relacionado con el software, este control incluye la restricción de comportamientos en la red que puedan llevar a la instalación de aplicaciones no autorizadas o malware. El seguimiento del uso de la navegación web puede identificar intentos de acceder a sitios maliciosos o de descargar software inseguro, mitigando el riesgo de que los usuarios instalen aplicaciones no aprobadas por la entidad.

- **A.13.1.1 (ISO/IEC:2013):** Controles de redes.
- **A.8.20 (ISO/IEC:2022):** Seguridad de las redes.

Nivel de cumplimiento MSPI: 80%

Impacto: La navegación web se lleva a cabo a través de la red corporativa, y es fundamental asegurar que esta actividad esté controlada para prevenir accesos a sitios web peligrosos o inadecuados. Este control exige la implementación de medidas de seguridad adecuadas en las redes para proteger la integridad y confidencialidad de la información, lo cual es parte del seguimiento y revisión del uso de la web según perfiles.

3. CONCLUSIONES Y/O RECOMENDACIONES

3.1 CONCLUSIONES:

El Modelo de Seguridad y Privacidad de la Información (MSPI) ha mostrado un progreso significativo en la ejecución de las actividades programadas, alcanzando el 100% de las metas establecidas para 2024. Sin embargo, algunas tareas fueron completadas fuera de los plazos estipulados, lo que evidencia la necesidad de fortalecer la planificación y gestión de recursos.

Los controles implementados, como la gestión de accesos, los sistemas de monitoreo y las políticas de seguridad, han demostrado ser efectivos en la mitigación de riesgos asociados a accesos no autorizados y la protección de la información sensible. Sin embargo, la dinámica del entorno digital exige una actualización constante para mantenerse al día con nuevas amenazas.

El enfoque proactivo hacia la gestión de riesgos ha permitido identificar y mitigar vulnerabilidades de manera oportuna, fortaleciendo la resiliencia de la entidad. Sin embargo, es necesario ajustar los planes de tratamiento de riesgos para abordar cambios en el panorama de amenazas.

Las actividades de sensibilización y capacitación han promovido una mayor conciencia entre los funcionarios sobre la importancia de la seguridad y privacidad de la información. Sin embargo, es crucial intensificar las sesiones de actualización para garantizar que el personal esté preparado ante amenazas emergentes.

3.2 RECOMENDACIONES:

Implementar herramientas y metodologías que faciliten el monitoreo en tiempo real del progreso de las actividades, realizando evaluaciones periódicas para ajustar cronogramas y mitigar posibles retrasos en la ejecución de tareas.

Priorizar la revisión y actualización de los controles de seguridad críticos, asegurando su alineación con los cambios en la normativa ISO 27001, incrementando la inversión en herramientas de monitoreo avanzadas que detecten amenazas emergentes en tiempo real.

Reforzar los mecanismos de evaluación de riesgos, incorporando análisis predictivos y simulaciones de incidentes.

Revisar y ajustar los planes de tratamiento de riesgos, asegurando su capacidad para abordar amenazas futuras.

Establecer programas de formación continua que incluyan simulaciones prácticas de gestión de incidentes.

Diseñar contenidos específicos para reforzar la comprensión de las políticas de seguridad y el manejo de la información clasificada.

4. OBSERVACIONES

La eficacia ha sido calificada como satisfactoria. Se logró un incremento en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), alcanzando un 71% según los resultados del autodiagnóstico, lo que evidencia una mejora significativa en la aplicabilidad de los controles establecidos. Para el cierre del plan de gestión del cambio, se aclara que el 29% restante, que no fue ejecutado durante la vigencia 2024, será desarrollado de manera progresiva a partir de la vigencia 2025 mediante el Plan Estratégico de Seguridad y Privacidad de la Información.

Aunque las actividades relacionadas con la actualización de políticas y procedimientos se han completado, es fundamental mantener un seguimiento constante para garantizar su vigencia frente a cambios regulatorios.

La falta de personal y herramientas adecuadas ha afectado los tiempos de ejecución en algunos casos. Es necesario evaluar la capacidad operativa y considerar la asignación de recursos adicionales.

La integración del MSPI con el Plan Estratégico de Seguridad y Privacidad de la Información (PESI) ha sido efectiva, pero se deben continuar los esfuerzos para asegurar una alineación dinámica que responda a las prioridades estratégicas de la entidad.

La transición hacia la nueva versión del Anexo "A" de la ISO 27001 representa un desafío que debe abordarse con un plan de acción específico, evitando interrupciones en la operatividad del MSPI y garantizando su compatibilidad futura.

La entidad se encuentra a la espera de los ajustes que determine el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) en relación con la actualización de la norma ISO 27001:2022. Estos ajustes serán fundamentales para asegurar la alineación del modelo con los estándares internacionales y fortalecer la postura de seguridad de la información en la entidad.

5. ANEXOS

Instrumento de identificación de la línea base de seguridad (Autodiagnóstico MSPI).

Informe presentado el día 28 del mes de enero del año 2025.