FECHA DE EMISIÓN DEL INFORME O SEGUIMIENTO	**Día:**	06	**Mes:**	12	**Año:**	2024

1. No. DE INFORME O SEGUIMIENTO:	17
2. NOMBRE DEL INFORME O SEGUIMIENTO:	Seguimiento al Modelo de Seguridad y Privacidad de la Información (MSPI)
3. INTRODUCCIÓN:	Verificación y Seguimiento al Modelo de Seguridad y Privacidad de la Información (MSPI)
4. OBJETIVO:	Informe de seguimiento al Modelo de Seguridad y Privacidad de la Información MSPI de la Superintendencia de Sociedades
5. ALCANCE:	Evaluar el adecuado diseño, implementación y ejecución de los controles establecidos conforme con los lineamientos del Modelo de Seguridad y Privacidad de la información (MSPI) del MinTIC en la Superintendencia de Sociedades, para garantizar la seguridad de la información de conformidad con lo establecido en la resolución 500 de 2021, 746 de 2021, Manual de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información.
6. NORMATIVIDAD:	Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales". Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones". Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones" Decreto 1008 del 14 de junio de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones". Resolución 500 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad

	digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital" Resolución 746 de 2022 " Por la cual se fortalece el Modelo de Seguridad y Privacidad de la información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021"

7. DESARROLLO DEL INFORME O SEGUIMIENTO

El Modelo de Seguridad y Privacidad de la Información - MSPI, indica los lineamientos que las Entidades públicas deben implementar y adoptar, tomando como referencia estándares con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), para que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

El MSPI se encuentra alineado con el marco de referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y la Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas, este modelo pertenece a la Seguridad y Privacidad de la Política de Gobierno Digital y se desarrolla mediante el documento Maestro del Modelo de Seguridad y Privacidad de la Información y sus guías de orientación.

Tomando como base la Resolución 500 de 2021, Numeral 6, párrafo 1: Los sujetos obligados deben adoptar el Modelo de Seguridad y Privacidad de la Información – MSPI señalado en el Anexo 1 de la presente resolución, como habilitador de la política de Gobierno Digital y el instrumento para el diagnóstico.

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013

Para evaluar el cumplimiento del MSPI, en la Superintendencia de Sociedades, se llevó a cabo una revisión del autodiagnóstico realizado por el Grupo de Seguridad e Informática Forense, con el objetivo de verificar las evidencias y medir el nivel de madurez de los controles técnicos de seguridad de la información.

PLANIFICACIÓN

Se encontró que en materia de planificación la entidad presenta un avance del 38% respecto al 40% asignado, debido a que falta la construcción de los instrumentos de gestión, para identificar los activos asociados con la información y las instalaciones de procesamiento de información.

7. DESARROLLO DEL INFORME O SEGUIMIENTO

IMPLEMENTACIÓN

Este componente en la Entidad presenta un avance del 18% respecto al 20% asignado, debido a que es importante publicar los Indicadores de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.

EVALUACIÓN DE DESEMPEÑO

Este componente en la Entidad presenta un avance del 19% respecto al 20% asignado, debido a que es importante validar y evaluar el plan del desempeño y eficacia del MSPI a través de instrumentos que permitan determinar la efectividad de la implantación del MSPI.

MEJORA CONTINUA

Este componente en la Superintendencia presenta un avance del 18% respecto al 20% asignado, toda vez que se debe hacer seguimiento y cumplimiento de los planes de mejoramiento.

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2023	Planificación	38%	40%
	Implementación	18%	20%
	Evaluación de desempeño	19%	20%
	Mejora continua	18%	20%
TOTAL		93%	100%

Imagen 1. Avance PHVA

El porcentaje de implementación del PHVA correspondiente a la Planificación, Implementación, Evaluación de Desempeño, Mejora Continua es del 93% a corte al año 2023, por lo que se presenta un avance significativo en el ciclo del modelo de seguridad definido en el documento MSPI, el cual está alineado con las actividades que se establecieron en el Manual de Gobierno en Línea, a través del Decreto 1078 de 2015, en el Titulo 9, Capitulo 1, Sección 3.

Verificación de los Controles Administrativos

POLITICAS DE SEGURIDAD DE LA INFORMACIÓN (ISO A.5).

En este aspecto, el equipo auditor encontró un cumplimiento del 100% en materia de la política y del manual de seguridad y privacidad de la información debidamente formalizadas.

7. DESARROLLO DEL INFORME O SEGUIMIENTO

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ISO A.6).
Se encontró un avance del 81%. Dado que no se tiene control en los permisos de los repositorios de cada una de las dependencias, cuando los funcionarios se trasladan.

SEGURIDAD DE LOS RECURSOS HUMANOS (ISO A.7).
Se encontró un avance del 96%, por cuanto se recomienda definir el Plan de Sensibilización en Seguridad de la Información, establecer un indicador de avance en la implementación e Indicar las responsabilidades de acuerdo a los Roles.

GESTIÓN DE ACTIVOS (ISO A.8).
Se encontró un avance del 95% en este dominio y se recomienda realizar la revisión de la información clasificada y reservada e identificar medios de protección.

CONTROL DE ACCESO (ISO A.9)
Se encontró un avance del 80% dado que se debe realizar la definición a través de un procedimiento o guía que permita el monitoreo de los accesos de red, realizar la actualización de la política de redes para incluir las inalámbricas y crear un proceso de monitoreo de los accesos otorgados en las aplicaciones.

CRIPTOGRAFÍA (ISO A.10)
Se encontró un avance del 80% debido a que se debe hacer revisión del uso de controles criptográficos en los procesos de la Entidad y el monitoreo de las páginas web expuestas a la internet, e incluir un proceso de monitoreo para el manejo de las llaves.

SEGURIDAD FÍSICA Y DEL ENTORNO (ISO A.11)
Se encontró un avance del 91% y se recomienda realizar la revisión del proceso para garantizar que se controle el acceso a las instalaciones y se asigne o retire el carnet a los usuarios de manera controlada, definir la revisión anual de las áreas que se consideren de manejo de información confidencial, realizar el monitoreo preventivo de las instalaciones para validar su cumplimiento y solicitar actas de pruebas de equipos e informes de mantenimiento al proveedor.

SEGURIDAD DE LAS OPERACIONES (ISO A.12)
Se encontró un avance del 81% dado que falta definir los procedimientos de reinicio y recuperación del sistema, realizar la documentación de los playbooks de los diferentes intentos de fraude y validar los controles implementados en las diferentes aplicaciones o sistemas de información a través de un procedimiento documentado de monitoreo de controles.

SEGURIDAD DE LAS COMUNICACIONES (ISO A.13)
Se encontró un avance del 85% dado que se deben actualizar los lineamientos y modelos definidos para las redes, realizar la inclusión dentro del procedimiento de monitoreo y aseguramiento de los sistemas, validar los controles implementados en las diferentes aplicaciones o sistemas de información a través de un procedimiento documentado de monitoreo y configuración de eventos

7. DESARROLLO DEL INFORME O SEGUIMIENTO

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS (ISO A.14)
Se encontró un avance del 84%, por lo que se debe garantizar la inclusión de los requisitos de seguridad en los procesos de contratación y la entrega formal de las responsabilidades del sistema, realizar la revisión de los requisitos criptográficos en las aplicaciones expuestas a internet, contar con el monitoreo de vulnerabilidades en las aplicaciones de negocio, definir las actividades de monitoreo de los controles establecidos y realizar actualización documental.

RELACIONES CON LOS PROVEEDORES (ISO A.15)
Se encontró un avance del 80%, dado que es importante realizar la revisión al cumplimiento de los requisitos de seguridad en los proveedores, revisar los formatos de incidentes creados para la vigencia 2024 y definir los planes de respuesta para cada uno de los incidentes

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (ISO A.16)
Se encontró un avance del 80%, por lo que es importante actualizar el procedimiento para realizar la inclusión del formato de incidentes de seguridad, realizar el proceso de divulgación del procedimiento dentro del plan de sensibilización, definir los planes de respuesta para cada uno de los incidentes y se debe crear y hacer seguimiento a los indicadores.

ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO (ISO A.17).
Este dominio presenta un avance del (70%), dado que se debe realizar la actualización del PCN (Plan Continuidad del Negocio) de la Entidad, teniendo en cuenta un sitio alterno que permita contar con los aplicativos misionales, a falta de servicio en los servidores ON PREMISE y Participar en la definición de pruebas del PCN y del PRD (Plan Recuperación de Desastres) de la Entidad.

CUMPLIMIENTO NORMATIVO (ISO A.18).
Se encontró un avance del 96.5%, debido a que es importante hacer revisión de los controles establecidos y del procedimiento asociado y crear los indicadores correspondientes.

En la siguiente tabla se resume el análisis de evaluación del año 2023.

7. DESARROLLO DEL INFORME O SEGUIMIENTO

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	81	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	96	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	95	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	80	100	GESTIONADO
A.10	CRIPTOGRAFÍA	80	100	GESTIONADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	91	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	81	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	85	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	84	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	80	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	70	100	GESTIONADO
A.18	CUMPLIMIENTO	96,5	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		86	100	OPTIMIZADO

Imagen 2. Efectividad de controles

En la imagen anterior, se puede evidenciar la calificación de la evaluación de efectividad en cada uno de los controles:

- Políticas de seguridad de la información
- Organización de la seguridad de la información
- Seguridad de los recursos humanos
- Gestión de activos
- Control de acceso
- Criptografía
- Seguridad física y del entorno
- Seguridad de las operaciones
- Seguridad de las comunicaciones
- Adquisición, desarrollo y mantenimiento de sistemas
- Relaciones con los proveedores
- Gestión de incidentes de seguridad de la información
- Aspectos de seguridad de la información de la gestión de la continuidad del negocio
- Cumplimiento

Con un promedio de evaluación en los controles del 86%, se puede observar que la Superintendencia de Sociedades se encuentra acorde con los requisitos normativos relacionados con la Seguridad y privacidad de la información y en proceso de mejora continua.

7. DESARROLLO DEL INFORME O SEGUIMIENTO

GESTIÓN DEL RIESGO

Se encontró en documento sobre la gestión de riesgos elaborado por el ingeniero Mario Latorre que con corte a 31 de diciembre de 2023, el sistema de Riesgos y Auditoria (ITS) arroja 363 activos de información, de acuerdo con la clasificación y valoración por parte de los gestores de riesgos de los procesos, refleja la siguiente situación.

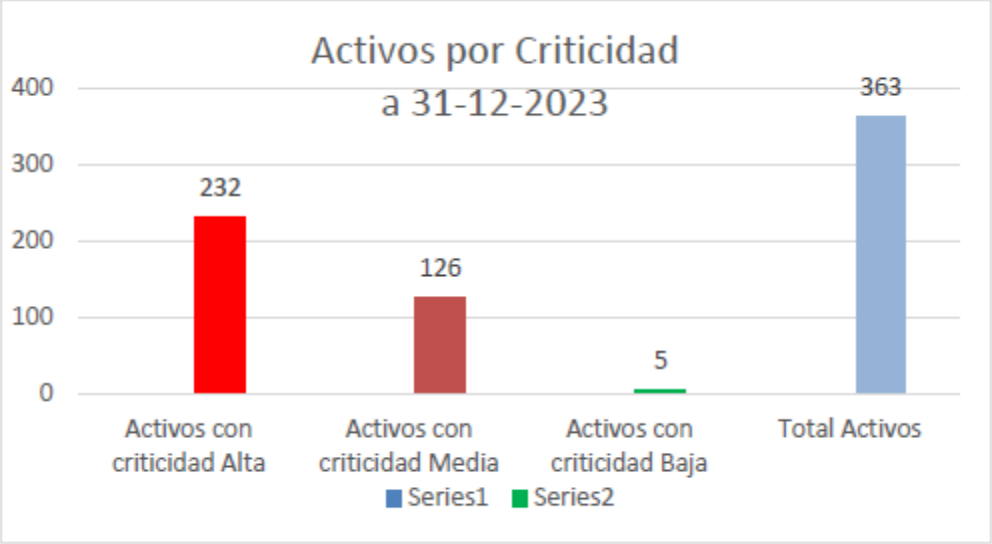


Imagen 3. Activos por Criticidad

Asimismo, sobre estos activos los gestores de los procesos han realizado análisis de riesgo con la identificación de los siguientes riesgos inherentes, de acuerdo a su criticidad.

7. DESARROLLO DEL INFORME O SEGUIMIENTO

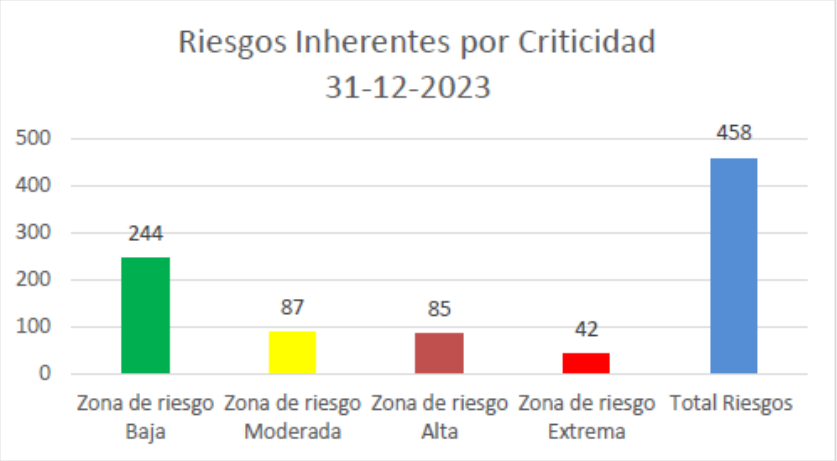


Imagen 4. Riesgos Inherentes por Criticidad

En la siguiente imagen se puede evidenciar que los gestores de riesgo han actualizado los activos, riesgos y controles, en sus procesos, con los cuales se pretende disminuir el grado de exposición o de materialización. Los controles aplicados se reflejan en la siguiente gráfica.

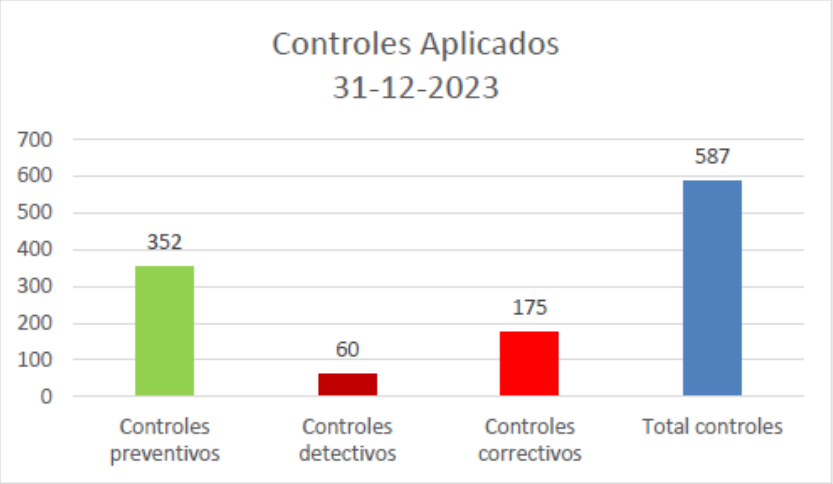


Imagen 5. Controles Aplicados

Con los controles aplicados a los riesgos el Sistema de Riesgos y Auditoria (ITS), se realiza una proyección del riesgo residual, cuyos resultados se reflejan en la siguiente gráfica.

7. DESARROLLO DEL INFORME O SEGUIMIENTO

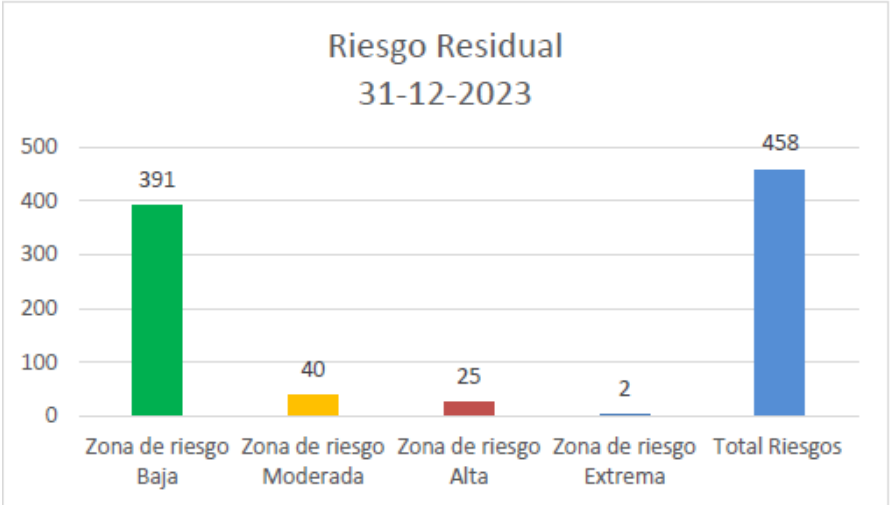


Imagen 6. Riesgo Residual

Se puede observar que se presentan 2 riesgos extremos y 25 riesgos altos, que deben ser revisados, para entender porqué al aplicarles controles aún continúan con criticidad elevada.

Se sugiere que para la vigencia 2024 es necesario que los procesos realicen el monitoreo de los controles para verificar si estos están funcionando o no. En caso negativo se deben realizar los planes de mejoramiento respectivos.

8. RECOMENDACIONES

Dentro del proceso de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) y el soporte del Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC, se recomienda actualizar los procedimientos, guías, manuales y formatos que se encuentran en el Sistema de Gestión Integrado de acuerdo con los controles de la Norma ISO 27001:2022.

En el año 2025, se recomienda realizar una nueva medición del MSPI, para monitorear y evaluar el cumplimiento de la misma, teniendo en cuenta la actualización de la Norma ISO 27001:2022.

En los activos de información, cuya calificación de los riesgos sea ALTA, se debe realizar la identificación de riesgos de seguridad de la información, de acuerdo al Instructivo para la gestión de riesgos de seguridad de la información.

Para la vigencia 2024, sería necesario que en los procesos, se realice el monitoreo de controles de los riesgos con el fin de monitorearlos, controlarlos y mitigarlos.

8. RECOMENDACIONES

En caso de que se materialicen los riesgos, se deben gestionar los respectivos planes de mejoramiento.

Se recomienda validar los controles implementados en las diferentes aplicaciones, contar con monitoreo de vulnerabilidades en las aplicaciones, definir los planes de respuesta para cada uno de los incidentes, crear y hacer seguimiento a los indicadores de seguridad, realizar la actualización del PCN (Plan Continuidad del Negocio) y el PRD (Plan Recuperación de Desastres) con sus respectivas pruebas, hacer seguimiento al control de acceso físico y lógico, identificar medios de protección, crear procedimientos y guías que permita el monitoreo de acceso de red LAN, WAN tanto física como inalámbrica.

Se recomienda crear un cronograma de actividades para hacer seguimiento a la actualización de la Norma ISO 27001:2013 hacía la Norma ISO 27001:2022 en la Entidad.

9. CONCLUSIONES

Una vez evaluado el avance de la implementación del MSPI en la Superintendencia de Sociedades, se concluye:

El resultado de la evaluación efectuada al modelo de seguridad y privacidad de la información en la Superintendencia de Sociedades, por el Grupo de Seguridad e Informática Forense, tiene una calificación cuantitativa del 86% para el año 2023, evidenciando un avance significativo y optimizado.

Con un porcentaje del 86% y de acuerdo con la tabla de calificación del MSPI, la Entidad se encuentra en una calificación de Optimizado y cuenta con un valor agregado por la aplicación de Seguridad de la Información por medio del mejoramiento continuo del MSPI.

El avance en PHVA se encuentra en un 93% del 100%, lo que significa que la Superintendencia aplica los lineamientos conforme al MSPI.

En la evaluación de efectividad de controles, se identificó que se han implementado controles de seguridad de la información de acuerdo con el Anexo A de la norma ISO 27001:2013, con una calificación del 86% sobre el 100%, lo que indica un nivel de madurez optimo en la implementación de las medidas de seguridad.

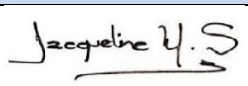
La Entidad debe ejecutar las acciones necesarias que permitan mantener actualizadas las plataformas de Tecnología de la Información y continuar con un soporte profesional aplicando Acuerdos de Niveles de Servicio, para optimizar los tiempos de respuesta y asegurar el correcto funcionamiento.

9. CONCLUSIONES

Debido al alto número de controles, se recomienda continuar con la revisión al detalle de las recomendaciones tanto de los controles administrativos como técnicos del Instrumento MSPI.

Para constancia se firma en Bogotá D.C., a los 6 días del mes de diciembre del año 2024

10. RESPONSABLE DEL INFORME O SEGUIMIENTO

Nombre Completo	Responsabilidad	Firma
Jacqueline Murillo Sanchez	**Jefe de la Oficina de Control Interno**	
Diana Paola Aguasaco Munevar	**Auditora**