

Plan de Seguridad Y Privacidad de la Información

Dirección Administrativa y TICS

**Versión 1
Enero, 2025**

Tabla de contenido

1. Objetivo	2
2. Alcance.....	2
3. Alineación estratégica.....	3
4. Glosario	3
5. Normatividad Aplicable	4
6. Desarrollo	5
7. Actividades	8
8. Anexos	12
9. Control de cambios.....	12

1. Objetivo

Establecer las actividades contempladas en el Modelo de Seguridad y Privacidad de la Información (MSPI) y los lineamientos para su implementación en RenoBO, alineado con la Norma Técnica Colombiana NTC/ISO 27001, las Políticas de Gobierno Digital y Seguridad Digital, continuidad del servicio y protección de datos personales, las buenas prácticas en gestión administrativa, tecnológica y de riesgos, para garantizar la confidencialidad, integridad, disponibilidad y protección de la información.

2. Alcance

El presente documento establece las directrices para la adopción y operación del Modelo de Seguridad y Privacidad de la Información (MSPI), alineado con la norma NTC/IEC ISO 27001 y las disposiciones de la Política de Gobierno Digital, aplicable a todos los procesos, activos de información y sistemas integrados de gestión de la entidad.

Este alcance abarca:

1. Gestión de seguridad y privacidad: La identificación, valoración y tratamiento de riesgos relacionados con la confidencialidad, integridad y disponibilidad de la información.
2. Cumplimiento normativo: Lo dispuesto en los decretos y resoluciones aplicables, como el Decreto Único Reglamentario del Sector de Función Pública, el Decreto 1078 de 2015 y la Resolución 500 de 2021.
3. Gestión operativa: La implementación de políticas, planes de trabajo, controles, y subsistemas que permitan cumplir con la estrategia de Seguridad Digital y los objetivos del Sistema Integrado de Gestión (SIG).
4. Cobertura: Todas las dependencias, procesos y actores de la entidad, incluyendo directivos, funcionarios, contratistas y terceros que tengan relación con los activos de información.

Con estos lineamientos se busca garantizar un nivel adecuado de protección en todos los niveles de operación mediante actividades específicas, como el despliegue de controles, la gestión de activos de información, y el monitoreo continuo de los sistemas de información estratégicos, misionales y transversales de la Empresa.

3. Alineación estratégica

El Plan de Seguridad y Privacidad de la Información (PSPI) contribuye al pilar de “Excelencia Operacional” y respalda el cumplimiento del objetivo estratégico de “Tecnología”, que tiene como propósito aumentar la eficiencia operativa, garantizar la disponibilidad, confidencialidad e integridad de la información, actualizar la infraestructura tecnológica de la empresa, implementar un Sistema de Gestión de Seguridad de la Información (SGSI) y desarrollar planes de recuperación ante desastres.

De esta manera, el PSPI busca apoyar y contribuir directamente al desarrollo y cumplimiento de los objetivos estratégicos de la empresa, proporcionando un nivel de confianza adecuado en el manejo de la información para todas las partes interesadas.

4. Glosario

Concepto	Definición
Activo	En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tenga valor para la organización (ISO/IEC 27000).
Ciberseguridad	Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.
Confidencialidad	Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.
Disponibilidad	Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.
Incidentes de seguridad de la información	Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.
Integridad	Propiedad de exactitud y completitud (GUIA N°5 MINTIC).
Riesgos de Seguridad de la Información	Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias que afecta la confidencialidad, integridad o disponibilidad de la información.
MSPI	Recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información, formulado por el Ministerio de las Tecnologías de la Información y Comunicación del Gobierno Colombiano (Modelo de Seguridad y Privacidad de la Información, MINTIC).
Seguridad de la Información	Conjunto de técnicas y métodos encaminados a la preservación de la confidencialidad, integridad y disponibilidad de la información en cualquiera de sus estados, medios de almacenamiento y/o difusión.

SGSI	Un Sistema de Gestión de Seguridad de la Información (SGSI) es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio.
-------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Tabla 1. Definiciones

5. Normatividad Aplicable

Normatividad	Descripción
Ley 527 de 1999	Ley de comercio electrónico - Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 1273 de 2009	Ley de delitos informáticos - Por la que se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -llamado "de la protección de la información y de los datos"- y se preservan los sistemas de las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1581 de 2012	Ley de la protección de los datos personales - Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712 de 2014	Por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Ley 2108 de 2021	Ley de Internet como servicio público esencial y universal - "Ley de Internet como servicio público esencial y universal" o por medio de la cual se modifica la Ley 1341 de 2009 y se dictan otras disposiciones.
Ley 2195 de 2022	Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones.
Decreto 19 de 2012	Ley Anti-trámites - Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
Decreto 103 de 2015	Regulación de la ley de transparencia - Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1078 de 2015	Decreto único de las TIC - Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1083 de 2015	Sector de Función Pública - Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.
Decreto 415 de 2016	Adiciona Decreto 1083 de 2015 Sector de Función Pública - Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
Decreto 612 de 2018	Gestor Normativo de la Función Pública - Por el cual se fijan directrices para la integración de los planes institucionales y

	estratégicos al Plan de Acción por parte de las entidades del Estado.
Decreto 1008 de 2018	Decreto del Gobierno Digital - 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 número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. Política de Gobierno Digital.
Decreto 767 de 2022	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 1509 de 2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
Resolución MINTIC 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.
NTC – ISO 27001	Requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información

Tabla 2. Normatividad aplicable

6. Desarrollo

De acuerdo al autodiagnóstico realizado en el mes de junio de 2024, utilizando la herramienta diseñada por MINTIC para evaluar la implementación y el nivel de madures del MSPI el porcentaje de efectividad en la implementación de los controles de la Norma NTC/ISO 27001:2013 se toman como referentes los siguientes resultados a priorizar en la definición de las actividades estratégicas que direccionen la seguridad y privacidad de la información para la vigencia 2025:

No.	Evaluación de Efectividad de controles			EVALUACIÓN DE EFECTIVIDAD DE CONTROL
	DOMINIO	Calificación Actual	Calificación Objetivo	
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	85	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	80	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	72	100	GESTIONADO
A.9	CONTROL DE ACCESO	80	100	GESTIONADO
A.10	CRIPTOGRAFÍA	30	100	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	76	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	68	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	81	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	79	100	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	60	100	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	46	100	EFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	54	100	EFECTIVO
A.18	CUMPLIMIENTO	73,5	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		70	100	GESTIONADO

BRECHA ANEXO A ISO 27001:2013



Adicionalmente se considera el estado actual del Modelo de Seguridad y Privacidad de la Información (MSPI) y las recomendaciones que para su mejoramiento han resultado de las auditorías realizadas por la Oficina de Control Interno

Análisis recomendaciones índice de desempeño Política seguridad de la información 2023

A continuación, se relacionan las recomendaciones que en la vigencia 2023 realizó el Departamento Administrativo de la Función Pública para mejorar el desempeño de la **Política seguridad de la información**:

Recomendaciones
Contar con un Plan de Recuperación de Desastres DRP, definido, documentado e implementado para todos los procesos
Elaborar un diagnóstico de seguridad y privacidad de la información para la entidad a través de la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI). Posteriormente, presentar y lograr la aprobación del diagnóstico en el Comité de Gestión y Desempeño Institucional.
Establecer, documentar e implementar un procedimiento para la gestión de incidentes de seguridad digital (Ciberseguridad) que incluya la notificación a las autoridades pertinentes (CSIRT Gobierno / COLCERT)
Identificar y gestionar los posibles riesgos de seguridad digital (Ciberseguridad) de sus infraestructuras on premise
Identificar y gestionar los posibles riesgos de seguridad digital (Ciberseguridad) en los servicios de Nube Pública/Privada que utiliza
Realizar análisis de vulnerabilidades para Portal Web, Sede electrónica y Servicios expuestos en Internet
Realizar análisis de vulnerabilidades de seguridad a los activos de información de su infraestructura en Nube Pública/Privada
Realizar pruebas de recuperación de cada una de los sistemas de información críticos
Separar los equipos que realizan las copias de respaldo de la información, del software e imágenes de los sistemas de la red de servidores y computadores.

Con lo anterior, se priorizan para 2025 acciones que contribuyen en alto grado con el objetivo de llevar a la entidad a un nivel de madurez del MSPI calificado como "optimizado", mediante la implementación de controles adecuados y alineados con los lineamientos establecidos por la entidad.

Auditorías Internas al “Plan Seguridad y Privacidad de la Información” en la vigencia 2024

A través de los informes de auditoría se identifican las siguientes observaciones que orientan actividades de este Plan en la vigencia 2025.

No	Requisito observación para la mejora	Actividad propuesta para mejorar
1	<p>Principio de publicidad “Plan de Seguridad y Privacidad de la Información - PSPI”</p> <p>Inconsistencia en la versión publicada en el sitio web y la Intranet de la Empresa.</p> <p>Revisado el sitio web y la Intranet de la Empresa, se observa inconsistencia en la versión de publicación del documento “Plan de Seguridad y Privacidad de la Información - PSPI”, lo que conlleva a tener repositorios desactualizados y a que se pueda concluir y tomar acciones sobre versiones obsoletas de documentos.</p>	<p>Formular el Plan de comunicaciones TI: comunicación interna y externa</p>
2	<p>Numeral 2.1 Objetivos específicos del MSPI “Plan de Seguridad y Privacidad de la Información - PSPI”</p> <p>Presentación de información incompleta relacionada con los mecanismos definidos por la Empresa para garantizar la disponibilidad, confidencialidad y privacidad de la información.</p>	<p>Documentar lineamientos para la disponibilidad, confidencialidad y privacidad de la información.</p>
3	<p>Numeral 5 Plan de implementación del Modelo de Seguridad y Privacidad de la Información - MSPI “Plan de Seguridad y Privacidad de la Información - PSPI”</p> <p>No presentación de los Informes de resultado de las pruebas vulnerabilidades para las vigencias 2023 y 2024.</p>	<p>Formular indicadores para el seguimiento asociado a las pruebas de vulnerabilidades.</p> <p>Documentar informes de pruebas de vulnerabilidades.</p>
4	<p>Numeral 5 Plan de implementación del Modelo de Seguridad y Privacidad de la Información - MSPI “Plan de Seguridad y Privacidad de la Información - PSPI”</p> <p>Presentación de información incompleta relacionada con el estado de actualización</p>	<p>Elaborar informes de seguimiento a contratos con terceros - software antivirus Kaspersky utilizado por la Empresa.</p>

	del software antivirus Kaspersky utilizado por la Empresa.	
5	<p>Numeral 5 Plan de implementación del Modelo de Seguridad y Privacidad de la Información - MSPI “Plan de Seguridad y Privacidad de la Información - PSPI”</p> <p>Presentación de información incompleta relacionada con los resultados del autodiagnóstico del MSPI realizado con la herramienta provista por el MinTIC, que permite evaluar el nivel de madurez de la Empresa.</p>	<p>Documentar la fase diagnóstica del “Plan de Seguridad y Privacidad de la Información - PSPI” 2025 con los resultados del Autodiagnóstico MSPI realizado con la herramienta provista por el MinTIC.</p>

Con los anteriores diagnósticos y observaciones de auditorías internas del Plan de Seguridad y Privacidad de la Información - PSPI”, las actividades priorizadas para 2025 se agrupan en los siguientes requisitos del Modelo de Seguridad y Privacidad de la Información – MSPI:

- Mecanismos disponibilidad, confidencialidad y privacidad de la información en RENOBO
- Identificación y valoración de riesgos de seguridad de la información de la Empresa.
- Estrategia para la seguridad de la información:
- Estrategia para la privacidad y datos personales:
- Estrategia para la seguridad digital
- Estrategia para la arquitectura de la información
- Estrategia para la seguridad de datos
- Estrategia para la transparencia

Para cada estrategia desde la Dirección Administrativa proceso Gestión de TIC se brinda soporte y acompañamiento para que los procesos realicen las siguientes gestiones:

- Gestión de activos de información
- Gestión del cambio y cultura
- Gestión de riesgos
- Gestión del cumplimiento
- Gestión de la continuidad

Este proceso busca fortalecer la gestión de seguridad y privacidad de la información, garantizar el cumplimiento normativo y mejorar la confianza de todas las partes interesadas en la protección de los activos de información.

7. Actividades

Con los anteriores lineamientos, diagnósticos y recomendaciones para la mejora, para la vigencia 2025 se priorizan las siguientes actividades para potenciar los niveles de madurez y los controles establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI), integrando de manera efectiva la Estrategia de Seguridad Digital:

No	Actividad	Meta/ Producto	Evidencia	Responsable	Fecha Inicio	Fecha Fin
1	Recolección y actualización de la información de las bases de datos personales, existentes en todas las dependencias de la entidad, con el propósito de garantizar la precisión, integridad y cumplimiento de la normativa vigente sobre protección de datos.	Actualización de inventario de bases de datos personales manejadas en la entidad	Informe detallado de las bases existentes por cada dependencia	Todas las Dependencias Dirección Administrativa y de TI- Proceso Gestión de TIC	01/02/2025	28/02/2025
2	Socialización sobre el manejo responsable de las bases de datos personales y la publicación ante el Registro Nacional de Bases de Datos (RNBD)	Charla Informativa	Lista de Asistentes	Dirección Administrativa y de TI- Proceso Gestión de TIC	01/02/2025	28/02/2025
3	Publicación en la Superintendencia de Industria y Comercio (SIC) los reclamos presentados por los titulares de acuerdo a la circular externa 003 de 2018 (SIC)	Recolección de información de posibles reclamos de titulares de información	Publicación de información en la SIC los posibles reclamos de titulares durante los meses de julio a diciembre de 2024 y enero a junio de 2025	Oficina de Participación Ciudadana y Asuntos Sociales Dirección Administrativa y de TI- Proceso Gestión de TIC	01/02/2025 01/08/2025	14/02/2025 14/08/2025
4	Publicación de información en la SIC en el Registro nacional de	Publicación de la información recolectada y depurada por	Certificado emitido por la Superintendencia de Industria y Comercio	Dirección Administrativa y de TI- Proceso	01/03/2024	31/03/2024

	Bases de Datos (RNBD)	todas las dependencias sobre las bases de datos existentes En RenoBo	(SIC) de la publicación de información de bases de datos existentes en RenoBo	Gestión de TIC Espitia		
5	Elaboración de la Guía de Gestión de Activos de la Información	Documento Guía de Gestión de Activos de la Información	Documento Guía aprobado	Dirección Administrativa y de TI-Proceso Gestión de TIC	01/03/2025	31/03/2025
6	Actualización de herramienta o formato para el inventario de activos de información	Herramienta o formato actualizado	Archivo actualizado	Dirección Administrativa y de TI-Proceso Gestión de TIC	01/04/2025	30/04/2025
7	Sensibilización	Capacitación sobre diligenciamiento correcto de la herramienta o formato de activos de información	Listado de asistencia	Dirección Administrativa y de TI-Proceso Gestión de TIC	01/05/2025	30/05/2025
8	Actualización de inventario de activos de información	Inventario actualizado de activos de información por proceso o dependencia	Archivo diligenciado	Todos los procesos y dependencias de la Entidad	01/06/2025	30/07/2025
9	Publicación activos de información	Revisar y actualizar la información proporcionada por las dependencias, en coordinación con el proceso de gestión documental, con el fin de garantizar su adecuada publicación en la página web de la entidad y en la plataforma de datos abiertos	Publicación de Archivos	Todas las dependencias Proceso de Gestión Documental	01/07/2025	31/12/2025

10	Identificar el nivel de madurez del MSPI	Realizar el autodiagnóstico del MSPI con la herramienta proporcionada por Mintic	Archivo Actualizado	Dependencias involucradas. Dirección Administrativa y de TI- Proceso Gestión de TIC	01/06/2024	30/06/2025
11	Monitoreo de Controles Norma ISO 27001:2013	Actualizar y Monitorear controles de la norma aplicables en la Entidad.	Actas de reunión con las dependencias.	Todas las dependencias Dirección Administrativa y de TI- Proceso Gestión de TIC	01/05/2025	31/12/2025
12	Auditorías Internas y Externas	Participar en las auditorías programadas	Informe de Auditoría	Oficina de Control Interno	01/01/2025	31/12/2025
13	Solicitudes de novedades de acceso lógico	Atender las necesidades a usuarios y contratistas en la creación y asignación de perfiles de acuerdo a lo solicitado en el formato de novedad de acceso lógico.	Solicitudes atendidas	Proceso de Gestión de TICS	01/01/2025	31/12/2025
14	Implementar doble factor de autenticación.	Implementar doble factor de autenticación en las cuentas de correo institucional.	Cuentas de correo institucional con doble factor de autenticación.	Proceso de Gestión de TICS	01/04/2025	30/11/2025
15	Consola Antivirus	Monitorear y actualizar las licencias y bases de datos de antivirus con el fin de tener actualizado los equipos de cómputo de la entidad	Actualización Bases de Datos Antivirus	Proceso de Gestión de TICS	01/01/2025	31/12/2025
16	Divulgar y promover controles de	Publicar piezas sobre la divulgación	Correos enviados	Oficina Asesora de Relacionamie	01/02/2025	31/12/2025

	seguridad y privacidad de la información	de controles de Seguridad de la Información		nto y Comunicacion es Proceso de Gestión de TICS		
17	Revisar y/o Actualizar Documentos alineados al MSPI.	Revisar y/o Actualizar las Políticas, procedimientos, guías, manuales y lineamientos de ser necesario asociados al MSPI.	Documentos Actualizados	Todas las Dependencias Oficina Asesora de Planeación	01/03/2025	31/12/2025

8. Anexos

Autodiagnóstico implementación y el nivel de madures del MSPI 2024

9. Control de cambios

Fecha	Cambio
21/12/2020	Documento Original
09/04/2022	Actualización Plan de Trabajo Plan de Seguridad y Privacidad de la Información Vigencia 2022
16/01/2023	Actualización Plan de Trabajo Plan de Seguridad y Privacidad de la Información Vigencia 2023.
25/01/2024	Actualización Plan de Trabajo Plan de Seguridad y Privacidad de la Información Vigencia 2024.
30/01/2024	Aprobación actualizaciones Plan de Trabajo Plan de Seguridad y Privacidad de la Información Vigencia 2024.
31/01/2025	Se actualiza la alineación estratégica, dada la formulación del PEI Revitalización Urbana 2024-2027.

Elaboró	Revisó	Aprobó
----------------	---------------	---------------

Nombre: Holman Barrera Espitia Cargo/Rol: Gestor Junior 3 Área: Dirección Administrativa y TICS	Nombre: Alicia Rico Atencio Cargo/Rol: Contratista Área: Subgerencia de Gestión Corporativa	Nombre: Cargo/Rol: Área:
-------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------	--------------------------------

Nota: El presente plan se aprueba y/o actualiza en el marco del Comité Institucional de Gestión y Desempeño Institucional de la Empresa.