RENOBO EMPRESA DE RENOVACIÓN Y DESARROLLO URBANO DE BOGOTÁ

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Dirección Administrativa y TICS

Versión 1
Enero, 2025

Tabla de contenido

1. Objetivos

Definir los lineamientos para la gestión integral los riesgos de seguridad y privacidad de la información de RenoBo, mediante la identificación, valoración, clasificación y tratamiento de dichos riesgos de acuerdo con lo establecido en PL-08 Política para la Administración de Riesgos y la guía para la administración de riesgos de seguridad y privacidad de la información, la cual será documentada en 2025.

Orientar a los procesos de la Empresa para que implementen actividades para mitigar los riesgos identificados y realicen seguimiento de las medidas de control y la evaluación de su efectividad en la reducción de impactos.

Fortalecer conocimientos del talento humano sobre la gestión de riesgos de seguridad y privacidad de la información, alineado con las mejores prácticas y normativas vigentes, como la NTC/IEC ISO 27001:2013, garantizando la continuidad de los servicios críticos de TI y la eficiencia operativa de RenoBO.

2. Alcance

El alcance de este plan es para todos los procesos de la Empresa. Contiene lineamientos para la gestión integral de los riesgos de Seguridad y Privacidad de la Información, integra buenas prácticas en los procesos de la Renobo para prevenir incidentes que puedan afectar el logro de los objetivos.

Se enfoca en los riesgos identificados como Altos y Extremos, siguiendo los lineamientos establecidos por el Ministerio de TIC, y priorizando aquellos riesgos que podrían impactar de manera significativa los servicios y la operación institucional de acuerdo con el análisis de impacto para los procesos de negocio (BIA) del proyecto Plan de recuperación y Desastres (DRP) contemplado en el PETI.

3. Alineación estratégica – entendimiento estratégico

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información aporta al pilar de "Excelencia operacional**"** y contribuye al objetivo de "Tecnología: que busca aumentar la eficiencia operativa, la disponibilidad, la confidencialidad y la integridad de la información, actualizando la infraestructura tecnológica de la Empresa, implementando un Sistema de Gestión de Seguridad de la Información (SGI) y desarrollando planes de recuperación de desastres", adicionalmente ha adoptado la estrategia de gestión de riesgos, siguiendo las recomendaciones del Departamento Administrativo de la Función Pública DAFP y la Política de Gestión de Riesgos PL-08_Pol_Admon_Riesgos_V3. Estas acciones buscan atender las necesidades de prevención que hacen parte de la estrategia de apoyo a todos los objetivos estratégicos de la Entidad.

4. Glosario

Además de las definiciones contenidas en la PL-08 Política para la Administración de Riesgos V 03 y en la guía que, para la administración de riesgos de seguridad y privacidad de la información, la cual será documentada en 2025, se incluyen las siguientes definiciones:

Concepto	Definición
Riesgo	Es toda posibilidad de ocurrencia de aquella situación que puede afectar el desarrollo normal de la entidad y el logro de sus objetivos.
Seguridad de la Información	Conjunto de técnicas y métodos encaminados a la prevención de la confidencialidad, integridad y disponibilidad de la información en cualquiera de sus estados, medios de almacenamiento y/o difusión.

Tabla 1. Definiciones

5. Normatividad Aplicable

Normatividad	Descripción
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
ISO 27001 de 2013	Requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información.
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.
Decreto 612 de 2018	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	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
Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6 - noviembre de 2022	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 6 - noviembre de 2022.

Tabla 2. Normatividad aplicable

6. Desarrollo

6.1 Diagnóstico actual

Para la priorización de las actividades a ejecutar en la vigencia 2025 en el marco del "**Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información"** se analizaron las siguientes fuentes diagnósticas:

Recomendaciones Departamento Administrativo de la Función Pública Política Gobierno Digital

No	Recomendación FURAG 2023 Política Gobierno Digital
1	Aprobar, clasificar y actualizar mediante un proceso de mejora continua el inventario de activos de seguridad y privacidad de la información de la entidad.
2	Capacitar a servidores y contratistas de la entidad en temáticas de Seguridad y Privacidad de la Información.
3	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.
4	Cargar el registro de activos de la información y el análisis de criticidad de la entidad a través de la herramienta dispuesta en el Portal de Datos Abiertos www.datos.gov.co
5	Realizar auditorías internas, externas y de certificación o recertificación respecto al estándar ISO 27001 en la entidad.

Tabla 3 Recomendaciones FURAG 2023_ Política Gobierno Digital

De la tabla 3 se identifican actividades a priorizar en la planeación 2025, en materia de continuar **actualizando los inventarios de activos de seguridad y privacidad de la información** de la Empresa, **capacitando al talento humano** en uso y apropiación de la seguridad y privacidad de la información, **actualizando el diagnóstico de seguridad y privacidad de la información** a través de la herramienta Modelo de Seguridad y privacidad de la información MSPI, **mediante reuniones con los procesos** Gestión de Talento humano, Gestión de servicios administrativos y logísticos, Evaluación y seguimiento, Gestión Contractual. Éste diagnóstico se **presentará en el Comité Institucional de Gestión y Desempeño para su aprobación**. Adicionalmente se continuará analizando la criticidad de los activos de información a través de la articulación de lineamientos del portal de datos abiertos y aplicando buenas prácticas de seguridad y privacidad de la información teniendo como referente el estándar ISO 27001.

Recomendaciones Departamento Administrativo de la Función Pública Política Seguridad Digital

Otra fuente de información para la priorización de actividades que se tuvo en cuenta en el "**Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información"** son las recomendaciones del Departamento Administrativo de la Función Pública para la Política Seguridad Digital 2023 que se relacionan a continuación:

No	Recomendaciones
1	Contar con un Plan de Recuperación de Desastres DRP, definido, documentado e implementado para todos los procesos
2	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)
3	Identificar y gestionar los posibles riesgos de seguridad digital (Ciberseguridad) de sus infraestructuras on premise
4	Identificar y gestionar los posibles riesgos de seguridad digital (Ciberseguridad) en los servicios de Nube Pública/Privada que utiliza
5	Realizar **análisis de vulnerabilidades para Portal Web**, Sede electrónica y Servicios expuestos en Internet
6	Realizar **análisis de vulnerabilidades de seguridad a los activos de información** de su infraestructura en Nube Pública/Privada
7	Realizar pruebas de recuperación de cada uno de los sistemas de información críticos
8	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.

Tabla 4 Recomendaciones FURAG 2023_ Política Seguridad Digital

Las anteriores recomendaciones orientan actividades en materia contar con un **Plan de Recuperación de Desastres – DRP** que se encuentra dentro de PETI sujeto a la disponibilidad de recursos y alineado con los Planes Distritales de Desarrollo para la vigencia 2024-2027. Documentar procedimientos para la **gestión de incidentes y riesgos de seguridad digital** (Ciberseguridad) en los canales de comunicación y analizar las vulnerabilidades de seguridad de los activos de información.

Auditorías Internas al "Plan de Tratamiento de Riesgos de 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:

Requisito evaluado	Observaciones Auditoría Interna 2024
Numeral 4 Políticas de Administración de Riesgos “Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	Identificar riesgos de seguridad de la información para todos los procesos de la Empresa.
	Valorar riesgos.
	Incorporar los riesgos de seguridad de la información al Mapa de Riesgos Institucional.
	Documentar tratamientos riesgos seguridad de la información asociados a posibles actos de corrupción
Numeral 4 Políticas de Administración de Riesgos “Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información - PTRSPI”	Identificar necesidades de compartir y transferir parte del riesgo de seguridad y privacidad de la información.
Numeral 4 Políticas de Administración de Riesgos “Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información - PTRSPI”	Planear la contratación requerida para transferir parte del riesgo de seguridad y privacidad de la información.

Tabla 5 Observaciones Auditoria Interna al “Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información - PTRSPI” 2024

La tabla 5 orienta la necesidad de ejecutar actividades de documentación de lineamientos para que los procesos apliquen la PL-08 Política para la Administración de Riesgos V 03, y en la guía que, para la administración de riesgos de seguridad y privacidad de la información, la cual será documentada en 2025.

en lo correspondiente a Riegos de Seguridad de la Información, acompañar a los procesos en cada una de las fases definidas en esta política institucional e incorporar al mapa de riesgos institucional los riesgos de seguridad de la información identificados en una **primera fase para los procesos críticos,** mediante el análisis de impacto para los procesos de negocio (BIA) contemplado en el proyecto Plan de recuperación y Desastres (DRP) contemplado en el PETI y que se ejecutará en el mes de septiembre de 2025.

6.2 Desarrollo Metodológico

La administración de riesgos de seguridad y privacidad de la información se encuentra enfocada en identificar, analizar, valorar y tratar las amenazas y vulnerabilidades de los activos de información de la entidad, teniendo presente su criticidad y protección de los activos más significativos de los diferentes procesos. Las fases o etapas presentes en la gestión de riesgos permiten alinearlas con los objetivos, estrategias y políticas corporativas, logrando un nivel de riesgo que pueda aceptar o asumir la Alta Dirección.

- **Fase 1: Identificación de los activos de seguridad de la información**

  En esta fase se identifican los activos de información de todos los procesos de la entidad, con el objetivo de garantizar el funcionamiento interno de la empresa y de cara al ciudadano.

Los campos mínimos para la identificación de los activos de información son los siguientes:

1. Listar los activos por cada proceso
2. Identificar el dueño de los activos
3. Clasificar los activos
4. Clasificar la información
5. Determinar la criticidad del activo
6. Identificar si existe infraestructura critica cibernética

- **Fase 1.1: Identificación del riesgo**

  se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

  - ✓ Pérdida de la confidencialidad
  - ✓ Pérdida de la integridad
  - ✓ Pérdida de la disponibilidad

  Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

- **Fase 2: Valoración del riesgo**

En esta etapa se identifica y define el nivel de severidad del riesgo de seguridad de la información identificado en la metodología para la administración del riesgo contemplada en la "En la Guía para la administración del riesgo y el diseño

de controles en entidades públicas del Departamento Administrativo de la Función Pública – DAFP del 2022" Nov-2022, en la cual se establecen los siguientes pasos:

2.1 Análisis de Riesgos
2.2 Evaluación del Riesgo
2.3 Estrategia para combatir el riesgo
2.4 Herramientas para la gestión del riesgo
2.5 Monitoreo y revisión

- **Fase 3: Definir los Controles asociados a la seguridad de la información**

En esta etapa los riesgos de Seguridad y Privacidad de la Información identificados y calificados en la zona moderada a extrema, se debe establecer controles para mitigar o tratar los riesgos empleando como mínimo los controles del anexo A establecidos en la norma ISO 27001:2013.

7. Plan de implementación

A continuación, se presenta la relación de las actividades que deben desarrollarse para minimizar la posibilidad de materialización de riesgos de seguridad y privacidad de la información.

No.	Actividad	Meta/ Producto	Evidencia	Responsable	Fecha Inicio	Fecha Fin
1	Actualización de herramienta o formato para el inventario de activos de información y presentar este diagnóstico al Comité Institucional de Gestión y Desempeño para su aprobación.	Herramienta o formato actualizado.	Archivo actualizado. Acta Comité Institucional de Gestión y Desempeño	Dirección Administrativa y de TIC	01/04/2025	30/06/2025
2	Sensibilización	Capacitación sobre diligenciamiento correcto de la herramienta o formato de activos de información	Listado de asistencia	Ing. Holman Barrera Espitia Dirección Administrativa y de TIC	01/05/2025	30/05/2025
3	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
4	Actualización de riesgos de seguridad de la información que se hayan priorizado con el Análisis de Impacto del Negocio.	Inventario actualizado de riesgos de seguridad de la información para los procesos críticos priorizados.	Archivo diligenciado	Todos los procesos y dependencias de la Entidad	01/07/2025	30/09/2025
5	Monitoreos y Controles	Asignación de controles en activos identificados de moderado a extremos	Actas de reuniones con los procesos o dependencias.	Ing. Holman Barrera Espitia Dirección Administrativa y de TIC	01/08/2025	31/12/2025

				Dependencias involucradas		
6	Verificar la Política de gestión el riesgo, con el fin de realizar actualizaciones en materia de riesgos de seguridad de la información el caso de ser requeridas, y socializar los cambios que se puedan generar.	Documento actualizado de ser necesario.	Documento actualizado a una nueva versión. Listado de asistencia a socialización	Dirección Administrativa y de TIC Oficina Asesora de Planeación y procesos vinculados	01/06/2025	30/10/2025
7	Articular con la Alta Consejería Distrital de TIC, los avances progresivos en materia de publicaciones de los conjuntos de datos abiertos de RenoBo, priorizando el análisis, la criticidad y vulnerabilidad de los activos de información a través de la articulación de lineamientos del portal de datos abiertos, teniendo como referente el estándar ISO 27001	Informe criticidad activos de información Informe vulnerabilidad	Informes actualizados.	Dirección Administrativa y de TIC	1/08/2025	30/10/2025
8	Documentar la guía que, para la administración de	Construcción de la Guía para la	Formalización de la guía.	Dirección Administrativa y de TIC	1/01/2025	31/10/2025

	riesgos de seguridad y privacidad de la información, incorporando lineamientos para la **gestión de incidentes y riesgos de seguridad digital** (Ciberseguridad) en los canales de comunicación y analizar las vulnerabilidades de seguridad de los activos de información.	administración de riesgos.				
10	Incorporar al mapa de riesgos institucional los riesgos de seguridad de la información identificados en una **primera fase para los procesos críticos,** mediante el análisis de impacto para los procesos de negocio (BIA) contemplado en el proyecto Plan de recuperación y Desastres (DRP) contemplado en el PETI y que se ejecutará en el mes de septiembre de 2025	Políticas de Riesgos de Seguridad de la Información.	Documento de las políticas.	Dirección Administrativa y de TIC	1/01/2025	31/10/2025

8. Anexos

<<No aplica>>.

9. Control de cambios

Fecha	Cambio
27//01/2022	Documento Original
16/01/2023	Actualización Plan de Trabajo Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información Vigencia 2023.
25/01/2024	Actualización Plan de Trabajo Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información Vigencia 2024.
24/01/2025	Actualización Plan de Trabajo Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información Vigencia 2025.

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: SGC Cesar Aldana, contratista Área: DATIC Ivan Ceballos, Gestor senior I Área: DATIC	Nombre: Hernán Velandia Pérez Cargo/Rol: director Administrativo y de TIC Área: Dirección Administrativa y de TIC

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