Política general de seguridad y privacidad de la información

1. Objetivo

Establecer el marco general que orienta la seguridad y privacidad de la información en la Empresa de Renovación y Desarrollo Urbano de Bogotá, en adelante **RenoBo**, mediante la definición de principios, compromisos y directrices para proteger la confidencialidad, integridad y disponibilidad de la información institucional y de los activos que la soportan, a lo largo de todo su ciclo de vida.

2. Alcance

Esta política aplica a:

- **Toda la información institucional**, en cualquier formato o medio, incluyendo información física, digital, verbal, audiovisual y electrónica, así como registros, bases de datos, documentos, aplicaciones, sistemas de información, servicios tecnológicos y evidencias del SGSI.
- **La información que contenga datos personales y datos sensibles**, conforme a la normativa vigente, independientemente de que estos se encuentren en bases de datos estructuradas, archivos físicos, sistemas de información, plataformas en la nube, herramientas colaborativas, correos electrónicos u otros medios de tratamiento.
- **Todos los procesos de la Empresa**, así como las actividades de planeación, operación, control y mejora que involucren el uso, almacenamiento, transmisión o eliminación de información.
- **Todos los funcionarios, contratistas y terceros**, incluidos proveedores, aliados, operadores tecnológicos y encargados del tratamiento, que accedan, administren, procesen o custodien información institucional o datos personales en desarrollo de relaciones laborales, contractuales o funcionales.
- **Los servicios tecnológicos internos y externos**, infraestructura, plataformas en la nube, sistemas tercerizados, integraciones, APIs y soluciones administradas por terceros, cuando impliquen tratamiento de información o datos personales por cuenta de la Entidad.

El alcance de esta política cubre la totalidad del ciclo de vida de la información, desde su recolección o generación hasta su conservación, transferencia, transmisión, archivo y disposición final. En este marco, incorpora el componente ambiental como criterio transversal, limitado al uso responsable de los recursos tecnológicos y a la consideración de factores del entorno que puedan afectar la disponibilidad, integridad o continuidad de los activos de información. Esta incorporación se desarrolla de manera articulada con los procesos institucionales competentes y no implica la asunción, por parte del SGSI, de responsabilidades propias de otros sistemas de gestión. Así mismo, el alcance se articula con los lineamientos, procedimientos y controles específicos del SGSI que desarrollan operativamente lo aquí establecido.

3. Excepciones

Las excepciones al cumplimiento de esta política solo podrán autorizarse de manera **excepcional, justificada, temporal y documentada**, cuando exista imposibilidad técnica, legal o contractual debidamente sustentada.

Toda excepción deberá:

- Contar con solicitud escrita y justificación de riesgo.
- Definir controles compensatorios proporcionales.
- Ser aprobada por la instancia competente del SGSI.
- Quedar registrada como evidencia trazable en el repositorio oficial del SGSI.
- Considerarse en el análisis y tratamiento del riesgo correspondiente.

Las excepciones que impliquen **riesgos altos**, afectación a datos personales o posibles incumplimientos legales deberán ser elevadas al **Comité Institucional de Gestión y Desempeño** para su evaluación y decisión.

4. Marco de implementación

La presente política soporta la implementación, operación y mejora continua de las brechas identificadas en los autodiagnósticos de la Entidad al Modelo de Seguridad y Privacidad de la Información (MSPI), de los resultados en el desempeño del **Sistema de Gestión de Seguridad de la Información (SGSI)**, mediante la gestión del riesgo de seguridad y privacidad de la información, el análisis de vulnerabilidades, la aplicación de controles de seguridad, la atención de incidentes , la continuidad tecnológica y el cumplimiento de los requisitos legales, regulatorios, contractuales y administrativos aplicables.

La política incorpora la **protección de la información personal y la privacidad** como un componente específico del SGSI, asegurando su tratamiento conforme a los principios de necesidad, proporcionalidad y minimización, sin perjuicio de la protección integral de la información institucional, los servicios digitales, los procesos de la Empresa y sus recursos tecnológicos.

5. Marco normativo

Ver Normograma de la Empresa de Renovación y Desarrollo Urbano de Bogotá.

6. Instrumentos institucionales

Los siguientes documentos institucionales brindan lineamientos para la correcta implementación de los lineamientos descritos en esta política:

- **Estructura documental SGSI (norma interna)**: regla maestra para identificación, codificación, metadatos, control de cambios, estados, retención y publicación exclusiva en el Repositorio SGSI.
- **Declaración de Aplicabilidad – SOA** (**SGSI-SOA-GOV-001-v1**): establece los **controles aplicables**, su estado de implementación, la **justificación** y la **trazabilidad, control, documento y evidencia** (revisión semestral o por cambio material).

- **Acuerdo 59 de 2023 (estructura organizacional)**: establece la estructura organizacional vigente de la Entidad, la distribución de funciones y los niveles de decisión sobre los cuales se asignan los roles y responsabilidades definidos en esta política. El gobierno y la operación del SGSI se soportan en la Política Integral de Gestión y en los instrumentos que la desarrollan.
- **Gobernanza del SGSI (SGSI-LIN-GOV-001-v02)**: Establece el modelo de gobernanza del SGSI alineado con ISO/IEC 27001:2022: roles de decisión, ciclos de revisión y articulación con TI, datos y continuidad.
- **Controles y gestión del SGSI (SGSI-LIN-GOV-002-v01)**: Lineamiento puente entre esta política y los procedimientos operativos; define la aplicación proporcional de controles, su trazabilidad y los criterios de sostenibilidad.
- **Inventario y clasificación de activos (SGSI-LIN-GOV-003-v02)**: Regula la identificación, clasificación por nivel CIA y gestión del ciclo de vida de los activos de información e infraestructura crítica.
- **Control de acceso (SGSI-LIN-ACC-001)**: Establece criterios para la asignación, modificación, revisión, elevación y revocación de accesos lógicos y privilegios bajo el principio de mínimo privilegio.
- **Uso adecuado de la información y recursos (SGSI-LIN-UAIR-001)**: Define las reglas de uso responsable de la información institucional y los recursos tecnológicos por parte de funcionarios, contratistas y terceros.
- **Gobernanza y uso seguro de IA (SGSI-LIN-IA-001-v1.0)**: Fija criterios y controles mínimos para el uso seguro y trazable de sistemas de inteligencia artificial, incluida IA generativa, en el contexto institucional.

Los anteriores instrumentos se complementan con los lineamientos, procedimientos, formatos y demás documentos que se vayan incorporando al SGSI, los cuales estarán disponibles en el Repositorio SGSI y en la intranet institucional.

7. Definiciones

Activo de información: Recurso que tiene valor para la Entidad (datos, documentos, aplicaciones, infraestructura, servicios en nube y evidencias), cuya protección se gestiona en el SGSI durante todo su ciclo de vida y bajo control documental (código, metadatos, versión, estado, retención) en el repositorio oficial.

Clasificación de la información: Asignación de niveles (p. ej., pública, interna, confidencial, restringida) que determinan controles de acceso, circulación y conservación; se registra en los metadatos de la información documentada.

Confidencialidad / integridad / disponibilidad (CID): Principios que aseguran acceso autorizado a la información, exactitud y completitud de los datos, y su oportunidad para el uso previsto. Su evidencia se conserva en el repositorio del SGSI.

Control: Medida organizacional o técnica para tratar un riesgo (p. ej., autenticación, cifrado, continuidad, gestión de vulnerabilidades) y cuya implementación/eficacia debe evidenciarse y estar referenciada en la SOA.

IA generativa: Modelos que crean contenido nuevo (texto, imagen, audio, código u otros) a partir de instrucciones de entrada

Incidente de seguridad de la información: Evento que compromete o puede comprometer los principios CID, y que debe ser gestionado conforme al flujo operativo (detección–respuesta–lecciones aprendidas), con métricas y escalamiento según niveles definidos.

Información documentada: La información documentada del SGSI se gestionará conforme a la normativa institucional y a ISO/IEC 27001:2022, garantizando integridad, trazabilidad, disponibilidad y actualización.

Proveedor de IA: Tercero que desarrolla, aloja o suministra capacidades o servicios de IA.

Riesgo de seguridad de la información: Posibilidad de que una amenaza explote una vulnerabilidad sobre un activo, afectando los objetivos de seguridad; se gestiona con apreciación y tratamiento documentados y trazados contra la DOA/SOA.

SGSI (Sistema de gestión de seguridad de la información): Conjunto de políticas, procesos, controles y evidencias que permiten preservar confidencialidad, integridad y disponibilidad; opera con ciclo PHVA, medición por indicadores y gobierno documentado.

Sistema de IA: Solución que produce predicciones, recomendaciones o contenido que puede influir en procesos o decisiones

SOA: Declaración de Aplicabilidad (del inglés Statement of Applicability — SOA, o Declaración de Obligaciones de Aplicabilidad): documento formal del SGSI que lista todos los controles de seguridad del Anexo A de ISO/IEC 27001:2022, indicando para cada uno si aplica o no, la justificación de su inclusión o exclusión, y el estado de implementación. Constituye el vínculo principal entre el tratamiento del riesgo y los controles implementados.

Tratamiento del riesgo: Decisiones de **mitigar, transferir, aceptar o evitar**; su justificación, responsables, plazos y evidencias se registran y publican en el repositorio del SGSI.

8. Alineación Estratégica

La presente política se encuentra alineada con el Plan Estratégico 2024-2027 de RenoBo y aporta al logro de sus tres pilares estratégicos: **Retorno social y sostenibilidad**, **Crecimiento financiero** y **Excelencia operacional**.

En particular, esta política contribuye al **Retorno social y sostenibilidad** al proteger la información que soporta la prestación de servicios confiables, transparentes y orientados al ciudadano; al **Crecimiento financiero**, al fortalecer la gestión de riesgos, la continuidad y la protección de los activos de información que respaldan la operación y la toma de decisiones; y a la **Excelencia operacional**, al establecer lineamientos para una gestión segura, trazable y eficiente de la información en los procesos misionales y de apoyo.

La política es de obligatorio cumplimiento para funcionarios, contratistas y terceros.

9. Desarrollo de la política

9.1 Principios de la política

- **Legalidad y transparencia**: La gestión de seguridad y privacidad se fundamenta en la observancia de la normatividad vigente, la trazabilidad de las decisiones y la disponibilidad de evidencias verificables en el repositorio oficial del SGSI, conforme a la Estructura documental SGSI (codificación, metadatos, control de cambios y publicación exclusiva).

- **Responsabilidad y rendición de cuentas**: Cada activo, control y evidencia tiene responsables definidos y segregación mínima efectiva: quien redacta no aprueba, y quien ejecuta el control no valida su cierre, preservando independencia básica para auditoría y control interno.

- **Información documentada controlada**: La información documentada del SGSI se gestionará conforme a la normativa institucional y a ISO/IEC 27001:2022, asegurando integridad, disponibilidad, actualización y trazabilidad.

- **Relación con terceros y servicios en la nube**: Los proveedores y plataformas en nube deberán cumplir los requisitos contractuales y de seguridad definidos por la Entidad.

- **Accesibilidad y servicio al ciudadano:** Los portales y servicios digitales deberán observar los lineamientos de accesibilidad y seguridad establecidos, con verificación y registro de cumplimiento y corrección, mitigación o tratamiento documentadas para auditoría y seguimiento interno.

- **Sostenibilidad digital y articulación con el entorno:** La gestión de la seguridad de la información incorporará, como criterio transversal, el uso responsable de los recursos tecnológicos y la consideración de factores del entorno que puedan afectar la disponibilidad, integridad o continuidad de los activos de información. Este principio se desarrollará bajo el enfoque de gestión del riesgo del SGSI y en articulación con los procesos institucionales competentes, sin superponer responsabilidades propias de la gestión ambiental, de seguridad y salud en el trabajo o de otros sistemas de gestión.

9.2 Gobierno del SGSI

La información documentada del **SGSI** se administrará conforme a la normativa institucional de gestión documental y a ISO/IEC 27001:2022, garantizando **identificación, control de cambios, versiones y disponibilidad.** La publicación de documentos oficiales se realizará por los canales autorizados por la Entidad.

9.3 Seguimiento, medición y mejora continua

La Entidad medirá y hará seguimiento al desempeño del SGSI mediante indicadores, revisiones periódicas y acciones correctivas documentadas, conforme al ciclo PHVA. Los lineamientos aplicables se desarrollan en los instrumentos del SGSI.

9.4 Roles y responsabilidades

La Entidad define roles y responsabilidades claras para la gestión de la seguridad y privacidad de la información, incluyendo la protección de datos personales, asegurando coordinación, trazabilidad y rendición de cuentas en el marco del Sistema de Gestión de Seguridad de la Información (SGSI).

La asignación de responsabilidades se realiza conforme a la estructura organizacional vigente y bajo los principios de legalidad, proporcionalidad y segregación mínima efectiva, garantizando la auditabilidad y defendibilidad del SGSI.

Las responsabilidades se establecen así:

Comité Institucional de Gestión y Desempeño

- Aprobar la orientación general del SGSI.
- Asegurar patrocinio, prioridad institucional y disponibilidad de recursos.
- Conocer y decidir sobre asuntos estratégicos, excepciones de alto impacto y riesgos residuales que requieran escalamiento.

Dirección Administrativa y de TICs

- Liderar la implementación, operación, mantenimiento y mejora continua del SGSI.
- Coordinar la identificación de riesgos, la definición de controles y la articulación técnica con las demás dependencias.
- Implementar y operar los controles técnicos de seguridad.
- Generar, custodiar y conservar la evidencia técnica correspondiente.
- Apoyar la gestión de incidentes de seguridad de la información y la continuidad tecnológica.

Oficina Jurídica

- Acompañar y conceptuar sobre los aspectos legales, regulatorios y contractuales asociados al SGSI.

- Apoyar la gestión de incidentes que involucren datos personales o eventuales obligaciones de reporte.
- Verificar la coherencia jurídica de los instrumentos del SGSI.

Oficina Asesora de Relacionamiento y Comunicaciones

- Ejercer la vocería externa autorizada en caso de incidentes de seguridad, cuando corresponda.
- Coordinar los mensajes institucionales con las dependencias competentes en tecnología y asuntos jurídicos.

Líderes, dueños o responsables de proceso

- Identificar y gestionar los riesgos de seguridad de la información en sus procesos.
- Ejecutar o promover las acciones de tratamiento que les sean asignadas.
- Garantizar el uso autorizado, proporcional y trazable de la información bajo su responsabilidad.

Oficina de Control Interno

- Evaluar la conformidad del SGSI y la calidad de las evidencias.
- Formular recomendaciones y realizar seguimiento independiente.
- Mantener independencia frente a la operación de los controles.

Dirección de Contratación

- Incorporar en los instrumentos contractuales los requisitos de seguridad y privacidad de la información definidos por el SGSI.
- Verificar la inclusión de cláusulas de confidencialidad, tratamiento de datos personales y manejo seguro de la información.
- Articular con las dependencias competentes la definición y trazabilidad de requisitos aplicables a proveedores y terceros.

Funcionarios, contratistas y terceros

- Cumplir esta política y los lineamientos del SGSI.
- Proteger la información conforme a su rol y al principio de mínimo privilegio.
- Reportar oportunamente incidentes, debilidades o posibles compromisos de seguridad de la información.

Las responsabilidades operativas detalladas se desarrollan en los lineamientos, procedimientos e instrumentos del SGSI que complementan esta política.

Para efectos de aplicación de la presente política, las referencias funcionales deberán entenderse conforme a la estructura organizacional vigente de la Entidad. A la fecha de aprobación, dichas funciones recaen, según corresponda, en la **Dirección Administrativa y de TICs**, la **Oficina Jurídica**, la **Oficina Asesora de Relacionamiento y Comunicaciones**, la **Oficina de Control Interno** y la **Dirección de Contratación**.

9.5 Declaración de aplicabilidad

La Entidad mantendrá una Declaración de Aplicabilidad (DOA/SOA) vigente que consolide los controles de seguridad aplicables, su estado de implementación y la justificación de inclusión o exclusión, tomando como referente ISO/IEC 27001:2022 e ISO/IEC 27002:2022. La DOA/SOA será trazable con la **matriz de riesgos de seguridad y privacidad de la información del SGSI** y con el **plan de tratamiento de riesgos**, y se articulará con el mapa de riesgos institucional cuando aplique. La DOA/SOA se revisará con la periodicidad definida institucionalmente y cuando ocurran cambios materiales en riesgos, controles, servicios o requisitos aplicables, conservando evidencia conforme al control documental institucional.

9.6 Vocería ante incidentes

La Oficina Asesora de Relacionamiento y Comunicaciones es la vocería oficial para comunicaciones externas de incidentes; actúa con apoyo de la Oficina Jurídica y la Dirección Administrativa y de TICs, siguiendo tiempos definidos y asegurando coherencia con las obligaciones regulatorias.

9.7 Compromisos institucionales

Los siguientes compromisos institucionales desarrollan las obligaciones de la Entidad para implementar, operar y mejorar continuamente el SGSI. Cada compromiso deberá ejecutarse por el responsable correspondiente, conforme a la estructura organizacional vigente, y en la oportunidad que aplique según su naturaleza, dejando evidencia documentada de su cumplimiento en el Repositorio SGSI.

9.7.1 Dirección y gobernanza

- La Dirección Administrativa y de TICs garantizará el liderazgo, patrocinio y recursos necesarios para mantener un Sistema de Gestión de Seguridad de la Información (SGSI) eficaz, medible y trazable, conforme a los lineamientos institucionales y a los estándares internacionales aplicables.
- La Dirección Administrativa y de TICs lidera la gobernanza del SGSI y asegura la articulación de roles y responsabilidades en toda la Entidad.

9.7.2 Gestión del riesgo y mejora continua

- La Dirección Administrativa y de TICs identificará, analizará, tratará y monitoreará los riesgos de seguridad mediante procesos documentados, con revisiones periódicas y acciones de mejora conforme al ciclo PHVA.

9.7.3 Cumplimiento normativo y privacidad

- La Dirección Administrativa y de TICs, con apoyo de la Oficina Jurídica, cumplirá los lineamientos aplicables y protegerá la información personal bajo principios de necesidad y minimización, con controles de acceso basados en roles.

9.7.4 Alineación organizacional y responsabilidades

- El Comité Institucional de Gestión y Desempeño asignará responsabilidades según la estructura organizacional vigente, preservando segregación mínima efectiva (quien elabora no aprueba; quien ejecuta no valida el cierre) y respetando las funciones institucionales establecidas.

9.8 Directrices obligatorias de seguridad

Las siguientes directrices son **obligatorias** para la gestión de la seguridad y privacidad de la información en la Entidad.

9.8.1 Gestión del riesgo y controles

- La Dirección Administrativa y de TICs, en articulación con los líderes de proceso, deberá identificar, analizar y tratar los riesgos de seguridad de la información.
- Los controles aplicables **deberán** estar documentados en la **Declaración de Aplicabilidad (SOA).**
- Los cambios en el riesgo o en los controles **deberán** reflejarse en la versión vigente del SOA.

9.8.2 Información documentada

- La información documentada del SGSI se gestionará bajo prácticas de control documental que aseguren integridad, disponibilidad, actualización y trazabilidad.

9.8.3 Gestión de incidentes

La Dirección Administrativa y de TICs, con apoyo de las áreas correspondientes, establecerá y mantendrá un proceso institucional para la **gestión de incidentes de seguridad de la información**, incluyendo aquellos que involucren **datos personales**, con el fin de garantizar una respuesta oportuna, coordinada, trazable y conforme a la normatividad aplicable.

Todo evento que comprometa o pueda comprometer la **confidencialidad, integridad o disponibilidad** de la información deberá ser tratado como incidente de seguridad y gestionado de acuerdo con los lineamientos del SGSI.

Las directrices obligatorias son:

- Los incidentes de seguridad **deberán** ser identificados, registrados, analizados, atendidos y cerrados de manera documentada.
- Todo incidente **deberá** contar con evidencia verificable de su gestión y conclusión, conservada en el repositorio oficial del SGSI.
- Todo evento que comprometa o pueda comprometer la confidencialidad, integridad o disponibilidad de la información institucional, incluidas las bases de datos personales bajo responsabilidad de la Entidad, deberá ser tratado como incidente de seguridad y gestionado de acuerdo con los lineamientos del SGSI.
- La vocería externa ante incidentes corresponderá exclusivamente a la Oficina Asesora de Relacionamiento y Comunicaciones, en coordinación con la Dirección Administrativa y de TICs y la Oficina Jurídica.
- Los incidentes relevantes **deberán** ser considerados como insumo para la gestión del riesgo, la mejora continua del SGSI y, cuando aplique, la notificación a autoridades competentes.

Los procedimientos, roles operativos, niveles de severidad, tiempos de respuesta y mecanismos de escalamiento se encuentran definidos en los lineamientos y procedimientos del SGSI, los cuales desarrollan técnicamente esta sección.

9.8.4 Control de acceso

- Los accesos a sistemas y activos críticos deberán otorgarse según el principio de mínimo privilegio (cada usuario, proceso o sistema recibe únicamente los permisos estrictamente necesarios para cumplir su función, sin accesos adicionales no autorizados), con revisión y ajuste periódico conforme a los cambios de rol, función o vinculación.

9.8.5 Cifrado y protección de la información

- La información sensible **deberá** cifrarse en tránsito y en reposo en las plataformas que lo soporten.
- Los servicios que no permitan cifrado deberán documentar controles compensatorios.

9.8.6 Proveedores y servicios en la nube

- Los proveedores críticos y plataformas en nube **deberán** cumplir los acuerdos de servicio y los requisitos de seguridad establecidos.

9.8.7 Accesibilidad y servicios digitales

- Los portales y servicios digitales **deberán** ajustarse a los criterios de accesibilidad según lineamientos vigentes.
- Las correcciones derivadas de las evaluaciones **deberán** registrarse con evidencia de corrección, mitigación o tratamiento.

9.8.8 Uso responsable de la información

El uso responsable de la información institucional es de obligatorio cumplimiento para todos los funcionarios, contratistas y terceros de la Entidad, en cualquier nivel o modalidad de acceso, conforme a esta política, a los lineamientos del SGSI y a la normatividad aplicable.

El uso de la información institucional estará sujeto, como mínimo, a las siguientes directrices obligatorias:

- La información **solo deberá** ser utilizada para las finalidades explícitamente autorizadas y relacionadas con las funciones, procesos o actividades institucionales.
- El acceso, uso, reproducción, transmisión, almacenamiento y eliminación de la información **deberá** realizarse conforme a su nivel de clasificación y a los controles definidos por el SGSI.
- La información que contenga **datos personales o datos sensibles deberá** tratarse bajo los principios de legalidad, finalidad, minimización y confidencialidad, y únicamente por personal autorizado.
- Se **prohíbe** el uso de la información institucional para fines personales, no autorizados, distintos a los establecidos o contrarios a la ley.
- Queda **prohibida** la divulgación, cesión, copia o reutilización de información institucional sin autorización expresa y documentada.
- Toda persona que tenga conocimiento de un uso indebido, pérdida o posible compromiso de la información deberá reportarlo de manera inmediata a través de los canales definidos para la gestión de incidentes, conforme al Procedimiento de Gestión de Incidentes de Seguridad de la Información del SGSI, disponible en el Repositorio SGSI y en la intranet institucional.

El incumplimiento de estas directrices podrá dar lugar a **acciones disciplinarias, contractuales o legales**, según corresponda, sin perjuicio de las responsabilidades civiles, penales o administrativas a que haya lugar.

9.8.9 Seguridad de recursos humanos

La Entidad garantizará que el personal cumpla las responsabilidades asociadas a la seguridad de la información durante el ciclo de vida laboral y contractual.

Directrices

- Toda vinculación incluirá verificaciones previas conforme a la normatividad aplicable.
- Todo funcionario, contratista o tercero suscribirá acuerdos de confidencialidad antes de recibir accesos.
- La Entidad mantendrá programas de inducción y formación periódica en seguridad y privacidad.
- Los accesos se asignarán, ajustarán y revocarán según el rol, bajo mínimo privilegio.
- Ante el retiro del personal, los accesos a los activos de información deberán revocarse de manera oportuna y se deberán recuperar los activos asignados, conservando la evidencia correspondiente.

9.8.10 Seguridad física y del entorno

La Entidad protegerá sus instalaciones, áreas críticas, recursos tecnológicos y activos de información frente a accesos no autorizados, daños, interferencias y factores del entorno que puedan afectar la confidencialidad, integridad, disponibilidad o continuidad de la información, independientemente de que opere en instalaciones propias, compartidas o arrendadas. Esta política establece lineamientos de seguridad de la información aplicables a la seguridad física y del entorno, bajo un enfoque de gestión del riesgo del SGSI.

En este contexto, el SGSI identificará y articulará los riesgos físicos y del entorno que puedan impactar los activos de información, incluyendo aquellos asociados a incendios, inundaciones, fallas eléctricas, condiciones locativas, afectaciones ambientales u otros eventos con potencial de interrupción o daño. La implementación de controles físicos, locativos, ambientales u ocupacionales especializados se realizará en coordinación con los procesos institucionales competentes, evitando superposición de funciones y manteniendo dentro del SGSI la responsabilidad sobre la identificación, análisis, tratamiento y seguimiento del riesgo de seguridad de la información.

Cuando la Entidad opere en inmuebles arrendados o administrados por terceros, deberá asegurar que existan condiciones mínimas de protección física y del entorno acordes con los riesgos identificados, así como mecanismos de coordinación con el arrendador, administrador o proveedor correspondiente, cuando ello resulte aplicable.

Directrices

- Los accesos físicos a las instalaciones deberán controlarse mediante mecanismos de identificación, autenticación, autorización y registro, aplicados directamente por la Entidad o en coordinación con terceros responsables del inmueble.
- Las áreas restringidas o críticas, tales como cuartos técnicos, archivos, espacios con infraestructura tecnológica, centros de cableado, servidores o dependencias con tratamiento de información sensible, deberán contar con controles de acceso diferenciados, autorización previa y, cuando aplique, supervisión durante la permanencia.
- Toda visita a las instalaciones deberá registrarse y gestionarse conforme a los controles definidos por la Entidad, incluyendo acompañamiento cuando el nivel de riesgo o la naturaleza del área visitada así lo requiera.
- Las instalaciones y áreas críticas deberán contar con medidas de protección física acordes con los riesgos identificados, tales como cerraduras, controles de acceso, señalización, cámaras, protección contra incendios, respaldo eléctrico u otras medidas razonables y proporcionales a la capacidad institucional y a las condiciones de operación.
- Cuando la operación se desarrolle en sedes arrendadas, compartidas o bajo administración de terceros, deberán definirse y articularse las condiciones mínimas de seguridad física y del entorno requeridas para proteger los activos de información y soportar la continuidad de la operación.

- Deberán identificarse y gestionarse los factores del entorno que puedan afectar los activos de información, incluidos incendios, inundaciones, fallas eléctricas, humedad, temperatura, polvo, deficiencias locativas y demás eventos que puedan comprometer la disponibilidad, integridad o continuidad de la información o de los servicios que la soportan.
- El SGSI deberá incorporar los riesgos de seguridad de la información del entorno físico identificados en el análisis y tratamiento correspondiente, articulando su gestión con los procesos competentes cuando la implementación de controles especializados corresponda a materias de infraestructura, mantenimiento, gestión ambiental, seguridad y salud en el trabajo, servicios generales o administración locativa.
- Los activos de información ubicados en áreas físicas deberán organizarse, resguardarse y operarse de manera que se reduzca la exposición a daño, pérdida, manipulación no autorizada o interrupción del servicio.
- Los incidentes de seguridad física y del entorno que afecten o puedan afectar activos de información deberán ser reportados, documentados, analizados y registrados como evidencia del SGSI, con el fin de soportar la respuesta institucional, la mejora continua y la definición de acciones correctivas o preventivas.
- La ejecución de controles físicos especializados por parte de procesos institucionales competentes no excluye la obligación del SGSI de mantener la trazabilidad del riesgo, la articulación interproceso y el seguimiento a la eficacia de las medidas adoptadas.

9.8.11 Sede electrónica

La sede electrónica y los canales digitales oficiales de la Entidad deberán operar bajo criterios de seguridad de la información, privacidad, accesibilidad, interoperabilidad, disponibilidad y gestión documental, garantizando la protección de los activos de información y la prestación confiable de servicios, consultas, trámites y mecanismos de interacción institucional.

La Entidad deberá asegurar que los canales habilitados para consulta, interacción, recepción o intercambio de información institucional cuenten con controles razonables de seguridad, trazabilidad, integridad y disponibilidad, conforme a los lineamientos del Sistema de Gestión de Seguridad de la Información (SGSI) y a las disposiciones institucionales de gestión documental aplicables.

La recepción, radicación, consulta, seguimiento e intercambio de información se realizará mediante los canales oficiales definidos y divulgados por la Entidad, de conformidad con los lineamientos institucionales, las disposiciones de gestión documental y los controles establecidos por el Sistema de Gestión de Seguridad de la Información (SGSI), garantizando la trazabilidad, integridad, disponibilidad y el tratamiento adecuado de la información.

La administración, operación, soporte y actualización de los componentes de la sede electrónica se realizará por las dependencias competentes conforme a la estructura organizacional vigente, en articulación entre la **Dirección Administrativa y de TICs**, la **Oficina Asesora de Relacionamiento y Comunicaciones** y las demás dependencias que resulten aplicables, sin afectar la responsabilidad institucional sobre la administración, publicación, custodia, conservación y trazabilidad de la información gestionada por medios digitales.

Directrices

- Los canales digitales oficiales deberán estar formalmente definidos, autorizados y divulgados por la Entidad, indicando su propósito, alcance, condiciones de uso y restricciones aplicables.
- Los servicios, portales y componentes de la sede electrónica deberán implementar medidas de seguridad acordes con la naturaleza de la información tratada, incluyendo mecanismos de protección de la información en tránsito, cuando aplique.
- Los activos digitales de la Entidad deberán observar los lineamientos de accesibilidad vigentes y los criterios institucionales aplicables a servicios digitales.
- Los expedientes electrónicos, registros de interacción y demás evidencias documentales gestionadas mediante la sede electrónica deberán garantizar integridad, autenticidad, disponibilidad, confidencialidad y trazabilidad, en concordancia con la normativa de gestión documental y los lineamientos del SGSI.
- Las soluciones que soporten la sede electrónica deberán incorporar principios de seguridad y privacidad desde el diseño, así como mecanismos de registro y trazabilidad que permitan verificar su operación, administración y uso.
- Cuando no exista ventanilla virtual para la radicación de determinadas comunicaciones oficiales de entrada, la Entidad deberá habilitar un canal institucional alterno, controlado y divulgado, respaldado por procedimientos que definan recepción, radicación, seguimiento, conservación de evidencias y responsabilidades asociadas.
- Cuando la sede electrónica ofrezca funcionalidades de consulta o seguimiento limitadas, la Entidad deberá comunicar de forma clara el alcance del servicio habilitado y las condiciones de acceso a la información disponible, con el fin de asegurar transparencia y reducir interpretaciones erróneas.
- La administración de contenidos, opciones visibles y componentes funcionales de la sede electrónica deberá realizarse por los roles o dependencias competentes, con articulación entre comunicaciones, tecnología, gestión documental y las demás funciones que correspondan, sin afectar la responsabilidad institucional sobre la información publicada o tramitada.
- Cuando participen terceros en la operación, soporte, intermediación o procesamiento asociado a los canales digitales, deberán existir condiciones definidas de seguridad, trazabilidad, responsabilidad y control, sin trasladar a terceros la responsabilidad institucional sobre la protección de la información
- Los incidentes, indisponibilidades, errores de integridad, fallas de trazabilidad o debilidades de seguridad que afecten la sede electrónica o sus canales asociados deberán ser reportados, gestionados y documentados conforme a los lineamientos de gestión de incidentes del SGSI.

9.8.12 Uso del correo institucional, Internet y recursos tecnológicos

El uso de recursos tecnológicos se realizará bajo criterios de legalidad, seguridad y responsabilidad.

Directrices

- El correo institucional se usará exclusivamente para fines oficiales; se prohíben cadenas y correos no autorizados.
- La información clasificada transmitida por correo institucional deberá protegerse mediante mecanismos de seguridad acordes con su nivel de clasificación, privilegiando el cifrado en tránsito y, cuando el riesgo lo requiera, el uso de controles adicionales conforme a los lineamientos del SGSI.
- La navegación estará sujeta a categorías autorizadas y controles de filtrado.
- Solo se permitirá software autorizado y licenciado.
- Cualquier incidente (phishing, malware, fuga) deberá reportarse al canal institucional definido para gestión de incidentes.

9.8.13 Firma de documentos

Las actuaciones documentales de la Entidad emplearán, según aplique, firma autógrafa mecánica, firma digital o firma electrónica, de conformidad con la normatividad vigente y los lineamientos institucionales.

Para los documentos que, por su naturaleza, nivel de riesgo o rol del firmante, requieran firma electrónica o digital reforzada, se garantizarán, según corresponda:

- Control de acceso al aplicativo de firma.
- Autenticación reforzada.
- Sello con identificador único.
- Estampado de fecha y hora legal colombiana.
- Estado del trámite.
- Trazabilidad.

9.8.14 Gobernanza y seguridad de sistemas de inteligencia artificial

La presente política establece el marco general de gobernanza de RenoBo en cuanto al uso seguro, responsable y trazable de sistemas de inteligencia artificial (IA), incluida la IA generativa, independientemente de que sean propios o de terceros, ya sea que operen en la nube o en instalaciones de la RenoBo y en cualquier etapa de su ciclo de vida. En este marco, los funcionarios, contratistas, proveedores y demás terceros que, en el desarrollo de sus funciones o actividades, diseñen, adquieran, integren, operen o utilicen capacidades de IA, deberán adoptar las responsabilidades y controles que les correspondan conforme a los lineamientos e instrumentos institucionales aplicables.

Se aplicarán principios de **finalidad**, **proporcionalidad**, **seguridad desde el diseño**, **supervisión humana** y **trazabilidad**.

Los detalles operativos serán definidos en los lineamientos e instrumentos del SGSI que desarrollen esta política, en materia de requisitos técnicos, operativos y contractuales para sistemas de inteligencia artificial.

10. Evaluación de la política

Revisión periódica: La presente política será revisada al menos una vez al año Las revisiones permitirán identificar la necesidad de actualización conforme a los criterios establecidos a continuación.

- La normatividad en materia de seguridad, privacidad o accesibilidad cambie o imponga nuevos requisitos.
- Se modifiquen los controles o el nivel de riesgo institucional reflejado en la **Declaración de Aplicabilidad (SOA)**.
- Se presenten hallazgos de auditoría que exijan ajustes formales.

Aprobación y publicación: Toda actualización de esta política deberá contar con aprobación de del Comité Institucional de Gestión y Desempeño, y será publicada únicamente en el Repositorio SGSI como versión oficial vigente y en la intranet, en cumplimiento del control 5.3 de ISO/IEC 27002:2022 (Roles y responsabilidades de seguridad de la información) y del Modelo de gobierno documental institucional.

La presente política será institucionalizada mediante el mecanismo formal de adopción que defina la Entidad, conforme a su marco de gobierno y control documental. La adopción formal es el acto mediante el cual este instrumento adquiere carácter obligatorio y vinculante para los destinatarios definidos en su alcance.

Vigencia: Esta política entra en vigencia a partir de su fecha de aprobación y permanecerá vigente hasta la publicación de una versión que la modifique o reemplace, manteniéndose el historial de versiones conforme a los lineamientos de la Estructura documental del SGSI.

Política general de seguridad y privacidad de la información

CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1	22/06/2026	Versión inicial del documento. Versión aprobada en el marco del Comité Institucional de Gestión y Desempeño en sesión del 30 de abril de 2026.

REGISTRO DE FIRMAS ELECTRONICAS

PL-16_Pol_Segur_Privac_Infor_V1

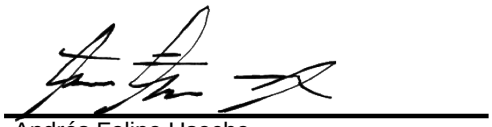
EMPRESA DE RENOVACIÓN Y DESARROLLO URBANO DE BOGOTÁ
gestionado por: azsign.com.co

Id Acuerdo: 20260618-105218-4e88a1-60804511
Estado: Finalizado

Creación: 2026-06-18 10:52:18
Finalización: 2026-06-18 19:34:25

Escanee el código para verificación

Aprobación: Dirección Administrativa y de TICs

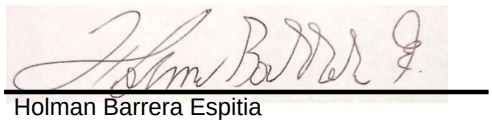


Andrés Felipe Useche
1022402202
ausechel@renobo.com.co
Jefe Oficina Asesora de Planeación
Oficina Asesora de Planeación

Revisión: Dirección Administrativa y de TICs

Fernando Ospina Marín
19432078
fospinam@renobo.com.co
Contratista
RENOBO

Elaboración: Dirección Administrativa y de TICs



Holman Barrera Espitia
79661051
holman@renobo.com.co

Revisión: Oficina Asesora de Planeación

Esperanza Peña Quintero
52166269
epenaq@renobo.com.co
Contratista
Empresa de Renovación y Desarrollo Urbano de Bogotá

REGISTRO DE FIRMAS ELECTRONICAS

PL-16_Pol_Segur_Privac_Infor_V1

EMPRESA DE RENOVACIÓN Y DESARROLLO URBANO DE BOGOTÁ
gestionado por: azsign.com.co

Id Acuerdo: 20260618-105218-4e88a1-60804511
Creación: 2026-06-18 10:52:18
Estado: Finalizado
Finalización: 2026-06-18 19:34:25

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Revisión	Esperanza Peña Quintero epenaq@renobo.com.co Contratista Empresa de Renovación y Desarrollo Urbano de Bogot	Aprobado	Env.: 2026-06-18 10:52:20 Lec.: 2026-06-18 10:52:36 Res.: 2026-06-18 10:52:48 IP Res.: 181.51.197.222 Canal: Email
Elaboración	Holman Barrera Espitia holman@renobo.com.co	Aprobado	Env.: 2026-06-18 10:52:48 Lec.: 2026-06-18 11:23:57 Res.: 2026-06-18 11:24:20 IP Res.: 181.51.197.222 Canal: Email
Revisión	Fernando Ospina Marín fospinam@renobo.com.co Contratista RENOBO	Aprobado	Env.: 2026-06-18 11:24:20 Lec.: 2026-06-18 11:27:52 Res.: 2026-06-18 11:27:59 IP Res.: 186.82.99.51 Canal: Email
Aprobación	Andrés Felipe Useche ausechel@renobo.com.co Jefe Oficina Asesora de Planeación Oficina Asesora de Planeación	Aprobado	Env.: 2026-06-18 11:27:59 Lec.: 2026-06-18 19:34:05 Res.: 2026-06-18 19:34:25 IP Res.: 186.154.13.247 Canal: Email