



**EMPRESA DE RENOVACIÓN Y DESARROLLO URBANO DE
BOGOTÁ**

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ENERO 2023

1. Introducción

La Empresa de Renovación y Desarrollo Urbano de Bogotá D.C. en adelante ERU, está comprometida a proteger los activos de información de la entidad (Empleados, información y entorno laboral), orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad, a la continuidad de las operaciones de gobernabilidad, la administración y/o gestión de riesgos, la creación de cultura y conciencia de seguridad en los funcionarios, contratistas, proveedores y personas que hagan uso de los activos de información de ERU.

Por lo anterior, en el presente documento se especifican las actividades relacionadas con el Plan de Implementación del Modelo de Seguridad y Privacidad de la Información en la ERU.

2. Objetivo General

Establecer las actividades que estén contempladas en el Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad de Servicio, en el Mapa de Procesos de la Empresa de Renovación y Desarrollo Urbano de Bogotá.

2.1. Objetivos Específicos del Modelo de Seguridad y Privacidad de la Información MSPI

- a) Establecer los mecanismos necesarios para garantizar la disponibilidad, confidencialidad y privacidad de la información de la Empresa de Renovación y Desarrollo Urbano de Bogotá.
- b) Establecer y actualizar periódicamente políticas, manuales, procedimientos, guías, formatos relacionados con el MSPI.
- c) Gestionar los riesgos y mitigar los incidentes relacionados con la seguridad y privacidad de la información manejada en la Entidad.
- d) Dar cumplimiento a los requisitos establecidos por el Gobierno en materia de Seguridad y Privacidad de la Información.

3. Alcance

Las Políticas de seguridad de la Información cubren los aspectos de privacidad, acceso, autenticación, mantenimiento y divulgación relacionados con cualquier activo de información, que conllevan a disponer guías y controles que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros, que laboren o tengan relación con la ERU, para alcanzar un adecuado nivel de protección en cuanto a confidencialidad, integridad y disponibilidad de la información.

4. Base Legal

Con el objeto de mitigar los riesgos relacionados con la autenticidad, la integridad, la disponibilidad, el no repudio, la confidencialidad y la trazabilidad de la información, se tiene que cualquier incidente que viole el marco normativo legal vigente en Colombia, en materia de políticas de seguridad de la información estará sujeto, entre otras, a lo establecido en las siguientes disposiciones legales: Marco normativo de buenas prácticas para el tratamiento de la información:

- Ley 527 de 1999 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 dictan otras disposiciones.
- Ley 1273 de 2009, Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- 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.
- Ley 1952 de 2019 Por medio de la cual se expide el Código General Disciplinario, se derogan la Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011, relacionadas con el derecho disciplinario.
- Decreto Nacional 1377 de 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto Nacional 103 de 2015 Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto MinTIC 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.
- Recomendaciones y buenas prácticas de los estándares adoptadas por el ICONTEC NTC/ISO 27001 y NTC/ISO 27002.

5. Plan de Implementación del Modelo de Seguridad y Privacidad de la Información MSPI

Gestión	Metas	Tareas	Fecha inicio	Fecha Final
Protección de Datos Personales	Recolectar bases de datos	Solicitar, a las áreas de la Entidad por medio de un memorando, la información correspondiente a las bases de datos personales que manejan actualmente y su respectiva actualización de las bases reportadas en la vigencia anterior.	1-Feb-2023	10-Feb-2023
	Revisión de bases de datos	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos en la SIC.	20-Feb-2023	28-Feb-2023
	Política y Documentos	Revisar y analizar con los grupos de interés el documento actual de política de datos personales, con el fin de evaluar una posible actualización del documento.	Oct-2023	Nov-2023
		Revisar y analizar los formatos, guías,	Sep-2023	Nov-2023

Gestión	Metas	Tareas	Fecha inicio	Fecha Final
		procedimientos existentes de las diferentes áreas relacionados a la recolección de datos personales con el fin de evaluar su actualización, modificación o creación de documentos nuevos.		
	Publicaciones de Información de ante la SIC en el Registro Nacional de Bases de Datos	Solicitud de Información al área de OGS los posibles reclamos presentados por titulares en el periodo correspondiente al segundo semestre 2022	01-Feb-2023	07-Feb-2023
		Publicación en la SIC, reclamos presentados por titulares segundo semestre 2021	07-Feb-2023	11-Feb-2024
		Capacitación de Usuarios Bases de Datos Personales y Registro Nacional de Bases de Datos	01-Mar-2023	18-Mar-2023
Protección de Datos Personales	Publicaciones de Información de ante la SIC en el Registro Nacional de Bases de Datos	Ajustes matriz de información contenida y medidas de seguridad de las BD entregadas.	07-Mar-2022	21-Mar-2022

Gestión	Metas	Tareas	Fecha inicio	Fecha Final
		Registrar o actualizar las BD personales teniendo en cuenta la información suministrada por las áreas ante el RNBD	12-Mar-2023	30-Mar-2023
		Solicitud de Información al área de OGS los posibles reclamos presentados por titulares en el periodo correspondiente al Primer semestre 2023	01-Ago-2022	04-Ago-2022
		Publicación en la SIC, reclamos presentados por titulares primer semestre 2022	08-Ago-2022	15-Ago-2022
Vulnerabilidades	Control de Acceso VPN	Actualizar cliente VPN de los usuarios con el fin de garantizar la seguridad de acceso a los servicios de TI, que ofrece la entidad.	Ene-2023	Dic-2023
	Identificar vulnerabilidades técnicas y administrativas.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Jul-2023	Dic-2023
	Consola Antivirus	Monitorear y Actualizar las	Ene-2023	Dic-2023

Gestión	Metas	Tareas	Fecha inicio	Fecha Final
		licencias y bases de datos de antivirus con el fin de tener actualizado los equipos de cómputo de la Entidad		
Gobierno Digital	Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad.	Actualización del nivel de madurez: descargar la herramienta de Mintic y diligenciar para conocer estado actual del MSPI	Abr-2022	May-2022
	Normas Seguridad y Privacidad de la Información.	Revisar y alinear si es necesario la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.	May-2023	Nov-2023
	Socializar Modelo de Seguridad y Privacidad de la Información	Realizar capacitación referente al Modelo de Seguridad y Privacidad de la Información y Charlas relacionadas con seguridad de la información y seguridad digital.	Ago-2023	Dic-2023
Implementación	Indicadores de Gestión del MSPI	Formular, Implementar y Actualizar los indicadores del	Jul-2023	Nov-2023

Gestión	Metas	Tareas	Fecha inicio	Fecha Final
		SGSI de ser necesario		
		Reportes de Indicadores	Ene-2023	Dic-2023
Revisión Controles Norma ISO 27001:2013	Monitoreo de Controles Norma ISO 27001:2013	Actualizar y Monitorear Herramienta para validar el cumplimiento de los controles de la norma ISO 27001:2013, que aplican en la Entidad	May-2022	Nov-2022
Evaluación y Desempeño	Auditorías Internas y Externas	Participar en las auditorias programadas a los diferentes procesos de la Entidad.	Plan Auditorias OCI	Plan Auditorias OCI
Planeación	Revisar Política de Seguridad y Privacidad de la Información	Verificar la Política de seguridad de la información, con el fin de realizar actualizaciones en el caso de ser requeridas, y socializar los cambios que se puedan generar.	Jun-2023	Nov-2023
	Manual con las políticas de seguridad y privacidad de la información	Validar, verificar y Actualizar el Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas y socializadas al interior de la Entidad.	Jul-2023	Nov-2023

Gestión	Metas	Tareas	Fecha inicio	Fecha Final
	Procedimientos de seguridad de la información	Validar procedimientos existentes para su actualización de ser necesario y desarrollar o creación de nuevos procedimientos .	Jul-2023	Nov-2023
	Roles y responsabilidades de seguridad y privacidad de la información.	Actualizar manual e Incluir los Roles y Responsabilidades de diferentes dependencias y actividades relacionadas con Gobierno Digital.	Jul-2023	Nov-2023
Activos de Información	Definir lineamientos para el levantamiento de activos de información	Actualización de Guía o instrumento para el levantamiento de activos de información.	Abr-2023	Jul-2023
	Levantamiento Activos de Información	Socializar guía o instrumento de activo de información	Jul-2023	Ago-2023
		Validar Activos de Información publicados en vigencias anteriores	Ago-2023	Oct-2023
		Identificar nuevos activos de información en cada dependencia	Ago-2023	Nov-2023
		Socializar con las dependencias las actualizaciones y modificaciones de los posibles	Ago-2023	Nov-2023

Gestión	Metas	Tareas	Fecha inicio	Fecha Final
		cambios físicos de ubicación de los activos de información.		
	Publicación	Validar y aceptar los activos de información para su publicación por cada líder de proceso y Gestión Documental	Sep-2023	Nov-2023
		Publicación del registro de activos de información página web de la Entidad Ley 1712	Nov-2023	Ene-2024
Gestión de Riesgos	Actualizar política gestión del riesgo	Verificar la Política de gestión el riesgo, con el fin de realizar actualizaciones en el caso de ser requeridas, y socializar los cambios que se puedan generar.	Abril-2023	Dic-2023
	Sensibilización	Socializar guía o herramienta gestión de riesgos de Seguridad y Privacidad de la Información.	Abril-2023	Dic-2023
	Identificar Riesgos de Seguridad y Privacidad de la Información	Identificación, análisis y evaluación de riesgos de seguridad de la información.	Abril-2023	Dic-2023
		Revisión y verificación de los riesgos identificados (Ajustes)	Abril-2023	Dic-2023

Gestión	Metas	Tareas	Fecha inicio	Fecha Final
	Aceptación Riesgos Identificados	Aceptación, aprobación de riesgos identificados y efectuar planes de tratamiento	Abril-2023	Dic-2023
	Seguimiento Fase de Valoración y Tratamiento	Seguimiento estado planes de tratamiento de riesgos identificados.	Abri-2023	Dic-2023
Gestión de Incidentes de Seguridad de la Información	Boletines informativos CSIRT	Socializar boletines informativos de seguridad	Feb-2023	Dic-2023