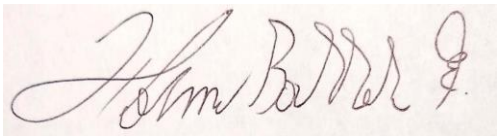
EMPRESA DE RENOVACIÓN Y DESARROLLO URBANO DE BOGOTÁ

PLAN TRATAMIENTO DE RIESGOS SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ENERO 2022

CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1	27/01/2022	Documento Original

ELABORADO POR:	REVISADO Y APROBADO POR:
	
Holman Barrera Espitia	María Cecilia Gaitán Rozo
Gestor Junior 3	Subgerente de Gestión Corporativa

1. Introducción

La Empresa de Renovación y Desarrollo Urbano de Bogotá D.C. en adelante ERU, mediante la definición del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, busca mitigar los riesgos presentes en el manejo de la seguridad y privacidad de la información tales como perdida de la confidencialidad, integridad y disponibilidad de los activos, evitando situaciones que impidan el logro de los objetivos de la Entidad.

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, se basa en el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC para el Desarrollo Digital y ciudadanos.

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

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.

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

a) Identificar, gestionar, tratar, manejar, hacer seguimiento y evaluar los riesgos de Seguridad y Privacidad de la Información, que se puedan presentar en la empresa articulándola con las demás políticas y planes existentes para contribuir al desempeño y asegurar razonablemente el logro de los propósitos y metas institucionales.

b) Dar cumplimiento a los requisitos establecidos por el Gobierno en materia de Seguridad y Privacidad de la Información.

2. Alcance

Esta política contempla la administración de los riesgos de Seguridad y Privacidad de la Información, la cual aplica para las operaciones de todos los procesos de la Empresa. Con el fin de realizar una eficiente gestión de riesgos, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos.

Junto con Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016) y la guía para la Administración del Riesgo y el Diseño de Controles para las Entidades Públicas DAFP 2020, se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en la ERU.

3. 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.

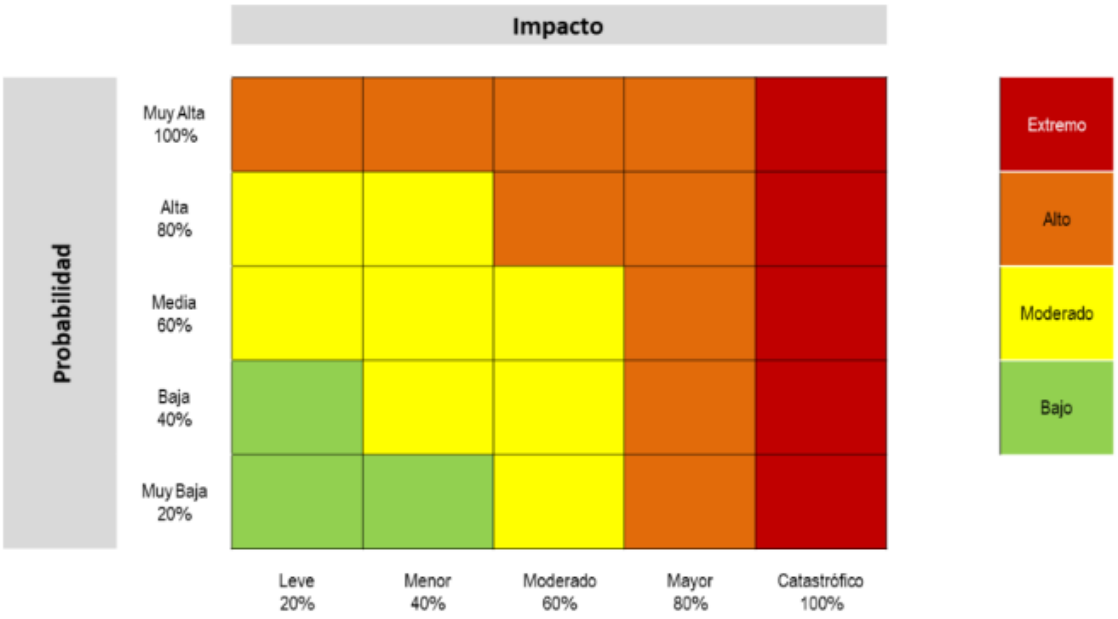
• Recomendaciones y buenas prácticas de los estándares adoptadas por el ICONTEC NTC/ISO 27001 y NTC/ISO 27002.

4. Política de Administración de Riesgos

El tratamiento de riesgos es la respuesta establecida por el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos.

El tratamiento o respuesta dada al riesgo, depende del nivel de aceptación del riesgo de acuerdo a lo establecido en la política de administración de riesgos (GI-05 versión 3).

De acuerdo con lo establecido en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP del 2020, se definen 4 zonas de severidad en la matriz de calor, a través de la combinación entre la probabilidad y el impacto:



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

De acuerdo con lo anterior, el nivel de riesgo que la empresa puede aceptar, que podría permitir el logro de los objetivos institucionales se describe a continuación.

- Para los riesgos que se encuentren en zona de riesgo baja, la Empresa está dispuesta a aceptar el riesgo, conociendo los efectos de su posible materialización y para los cuales no se requiere la definición y valoración de controles, sin embargo, se deben monitorear conforme a la periodicidad establecida.

- Para los riesgos calificados de zona modera a extrema, se deben establecer los controles que los mitiguen o reduzcan y se deben monitorear conforme a la periodicidad establecida.

- Los riesgos asociados a posibles actos de corrupción no admiten aceptación del riesgo y se deben definir los lineamientos para su tratamiento. De igual manera, se deben monitorear conforme a la periodicidad establecida.

- Cuando sea muy difícil para la empresa reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, éste puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización. Estos mecanismos de transferencia de riesgos deberán estar formalizados a través de un acuerdo contractual.

- Los líderes de proceso ante la materialización de los riesgos que impliquen la interrupción de las operaciones deben implementar los planes de contingencia y/o continuidad correspondiente.

- Para mitigar/tratar los riesgos de seguridad de la información se deben emplear como los controles del anexo A de la ISO/IEC 27001:2013 que apliquen.

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. Las 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.

5. Metodología

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar con el objetivo de mitigar los riesgos de Seguridad y Privacidad de la Información sobre los activos de la entidad, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información.

Gestión	Metas	Tareas	Fecha inicio	Fecha Final
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-2022	Dic-2022
	Sensibilización	Socializar guía o herramienta gestión de riesgos de Seguridad y Privacidad de la Información.	Abril-2022	Dic-2022
	Identificar Riesgos de Seguridad y Privacidad de la Información	Identificación, análisis y evaluación de riesgos de seguridad de la información.	Abril-2022	Dic-2022
		Revisión y verificación de los riesgos identificados (Ajustes)	Abril-2022	Dic-2022
	Aceptación Riesgos Identificados	Aceptación, aprobación de riesgos identificados y efectuar planes de tratamiento	Abril-2022	Dic-2022
	Seguimiento Fase de Valoración y Tratamiento	Seguimiento estado planes de tratamiento de riesgos identificados.	Abri-2022	Dic-2022

5.1. Desarrollo Metodológico

- **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 define el nivel de severidad del riesgo de seguridad de la información identificado en la metodología para la administración del riesgo contemplada en la “Actualización de la Política de administración de riesgos, de acuerdo con los nuevos lineamientos establecidos 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 2020” del 07-Oct-2021, en la cual se establecen los siguientes pasos:

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

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

En esta etapa se tratan los riesgos de seguridad y privacidad de la información empleando los controles establecidos en la norma ISO 27001:2013.