

EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA DE CALI – EDRU EICE
RESOLUCIÓN No. 10.15. 024-2024
(31 de Enero de 2024)

POR MEDIO DE LA CUAL SE ADOPTA EL PLAN DE TRATAMIENTO DE RIESGOS Y EL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024 EN LA EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA EDRU EICE.

La Gerente de la Empresa de Desarrollo y Renovación Urbana E.I.C.E., cargo para el cual fue nombrada mediante el Decreto 4112.010.20.0023 de enero 11 de 2024, con Acta de Posesión N°. 117 de enero 11 de 2024, en uso de sus facultades legales y estatutarias establecidas en el Decreto Municipal No. 084 bis del 04 de marzo de 2002, en la Resolución de Junta Directiva No. 01 del 02 de diciembre de 2002, y en especial las disposiciones conferidas por el Decreto 943 de 2014 y,

CONSIDERANDO

1. Que conforme al principio de "masificación del gobierno en línea" hoy gobierno digital, consagrado en el numeral 80 del artículo 20 de la Ley 1341 de 2009, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones.
2. Que de acuerdo con el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015 (DUR-TIC), por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, la política de gobierno digital será definida por MinTIC y se desarrollará a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC.
3. Que según el numeral 2, del artículo anteriormente citado, los habilitadores transversales de la política de gobierno digital, son los elementos fundamentales de seguridad y privacidad de la información, arquitectura y servicios ciudadanos digitales, que permiten el desarrollo de los componentes y el logro de los propósitos de dicha política.
4. Que el parágrafo del artículo 16 del Decreto 2106 de 2019, por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública, señala que las autoridades deberán disponer de una estrategia de seguridad digital, para la gestión documental electrónica y preservación de la información, siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.
5. Que el Plan de Tratamiento de Riesgos y el plan de Seguridad y Privacidad de la Información contribuye a que se garantice la confidencialidad, integridad y disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo asociado al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, lo que permite establecer entornos de confianza digital entre las partes interesadas y que hacen uso de la tecnología para el intercambio de información.

EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA DE CALI – EDRU EICE
RESOLUCIÓN No. 10.15. 024-2024
(31 de Enero de 2024)

POR MEDIO DE LA CUAL SE ADOPTA EL PLAN DE TRATAMIENTO DE RIESGOS Y EL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024 EN LA EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA EDRU EICE.

6. Que por lo anterior se hace necesario que EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA EICE - EDRU EICE adopte el Modelo de Seguridad y Privacidad de la información dado por el Ministerio de Tecnologías de la Información y las comunicaciones a través del Estrategia de Gobierno en Línea hoy Gobierno Digital.

En mérito de las anteriores consideraciones, se:

RESUELVE

Artículo 1. ADOPCIÓN se adopta el Plan de Tratamiento de Riesgos y el plan de Seguridad y Privacidad de la Información, en la EMPRESA DE DESARROLLO Y RENOVACIÓN URBANA EICE - EDRU EICE, el cual se anexa y hace parte integral de este Acto Administrativo, que se actualizó en enero de 2024, en el cual se incorpora las acciones y actividades que se llevaran a cabo para el presente año.

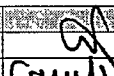
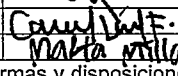
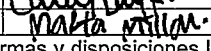
Artículo Segundo: CUMPLIMIENTO. El Comité Institucional de Gestión y Desempeño, será la instancia coordinadora y de seguimiento de todas las acciones que se propongan dentro de los procesos de formulación, concertación, implementación, evaluación y seguimiento al Plan de Tratamiento de Riesgos y el plan de Seguridad y Privacidad de la Información y se encargarán de verificar su cumplimiento, de acuerdo a las temáticas definidas en su contenido.

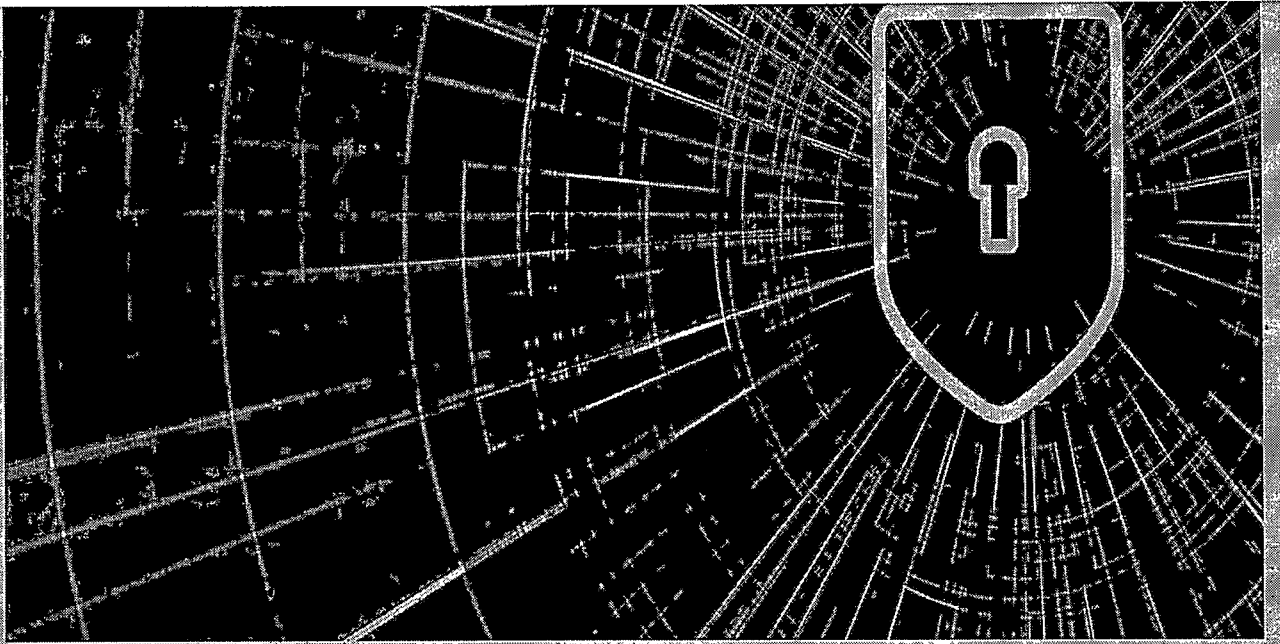
Artículo Tercero: DIVULGACIÓN Y SOCIALIZACIÓN. Plan de Tratamiento de Riesgos y el plan de Seguridad y Privacidad de la Información, deberá ser publicado en la página web de la EDRU EICE, y deberá ser socializado a todos los funcionarios de la entidad, a través de las capacitaciones, inducciones y re inducciones que se programen.

Artículo Cuarto: VIGENCIA. La presente Resolución rige a partir de su expedición. Se expide en Santiago de Cali a los Treinta y un (31) días del mes de enero de 2024.

COMUNIQUESE Y CUMPLASE


RAQUEL GARAVITO CHAPAVAL
Gerente EDRU EICE

	Nombre	Cargo / Actividad	Firma
Revisó	Carlos Andrés Argoty Botero	Jefe Oficina de Planeación EDRU E.I.C.E.	
Revisó	Carolina Soto Flórez	Jefe Oficina Asesora Jurídica EDRU E.I.C.E.	
Aprobó	Martha Alexandra Millán Córdoba	Secretaría General EDRU E.I.C.E.	
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para firma.			




PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Empresa de Desarrollo y Renovación
Urbana EDRU E.I.C.E

Proceso Gestión de TIC


Versión 1:2024



	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: DOC-GTI-02
		Versión: 01
	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Fecha Emisión: 30/01/2024

CONTENIDO

1	INTRODUCCIÓN	3
2	OBJETIVO	4
3	ALCANCE	4
4	OBJETIVOS ESPECIFICOS	5
5	TERMINOS Y DEFINICIONES	6
6	VISION GENERAL DEL PROCESO DE GESTION DE RIESGO EN LA SEGURIDAD DE LA INFORMACION	9
6.1	ESTABLECIMIENTO DEL CONTEXTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	10
6.1.1	Criterios de evaluación del riesgo de seguridad de la información:	10
6.1.2	Criterios de Impacto	11
6.1.3	Criterios de Aceptación	11
6.2	VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	12
6.2.1	Identificación del riesgo	12
6.2.2	Estimación del riesgo	14
6.2.3	Determinación del riesgo inherente y residual	17
6.2.4	Evaluación de los riesgos	18
6.3	TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	18
6.4	MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	20

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: DOC-GTI-02
		Versión: 01
	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Fecha Emisión: 30/01/2024

1 INTRODUCCIÓN


Hoy día, las empresas inmersas en la denominada revolución digital, reconocen el protagonismo de la información en sus procesos productivos, por tanto la importancia de tener su información adecuadamente identificada y protegida, como también la proporcionada por sus partes interesadas, enmarcada bajo las relaciones de cumplimiento, comerciales y contractuales como los son acuerdos de confidencialidad y demás compromisos, que obligan a dar un tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia.

La Seguridad de la Información en las empresas tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio.

La Empresa de Desarrollo y Renovación Urbana EDRU E.I.C.E decide entonces vincular el modelo de administración de los riesgos de seguridad de la información y las actividades de valoración de mismos riesgos en cumplimiento de la política de seguridad de la información, y como medio o herramienta para el logro de los objetivos de mantener la información de la Entidad confidencial, íntegra y disponible, a través de su ciclo de vida desde su captura, almacenamiento, explotación, hasta su eliminación.

Los principios de protección de la información se enmarcan en:

- **Confidencialidad:** Propiedad que la información sea concedida únicamente a quien esté autorizado.
- **Integridad:** Propiedad que la información se mantenga exacta y completa.
- **Disponibilidad:** propiedad que la información sea accesible y utilizable en el momento que se requiera.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: DOC-GTI-02
		Versión: 01
	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Fecha Emisión: 30/01/2024


2 OBJETIVO

Brindar a la Empresa de Desarrollo y Renovación Urbana EDRU E.I.C.E una herramienta con enfoque sistemático que proporcione las pautas necesarias para desarrollar y fortalecer una adecuada gestión de los riesgos de seguridad de la información, a través de métodos que faciliten la determinación del contexto estratégico, la identificación de riesgo y oportunidades, el análisis, la valoración y expedición de políticas así como el seguimiento y monitoreo permanente enfocado a su cumplimiento y mejoramiento continuo.

3 ALCANCE

La gestión de riesgos de seguridad de la información y su tratamiento, podrá ser aplicada sobre cualquier proceso de la EDRU, a cualquier sistema de información o aspecto particular de control de la entidad, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información, análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.


X

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: DOC-GTI-02
	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Versión: 01
		Fecha Emisión: 30/01/2024

4 OBJETIVOS ESPECIFICOS

En beneficio del apoyo y cumplimiento de los propósitos de la política estratégica de seguridad de la información en la Empresa de Desarrollo y Renovación Urbana EDRU E.I.C.E, se declaran los siguientes objetivos específicos:

- Brindar lineamientos y principios que propendan por la unificación de criterios para la administración de los riesgos de seguridad de la información.
- Fortalecer el sistema de gestión de riesgos de la Entidad incorporando controles y medidas de seguridad de la información que estén acordes al entorno operativo de la Entidad.
- Proteger el valor de los activos de información mediante el control de implementación de acciones de mitigación frente al riesgo y potencializar las oportunidades asociadas
- Generar una cultura y apropiación de trabajo enfocada a la identificación de los riesgos de seguridad de la información, y su mitigación.
- Reducir toda posibilidad de que una brecha o evento produzca determinado impacto bien en la información o cualquier otro activo de información asociado, a través de la gestión adecuada de los riesgos de la seguridad de la información.
- Lograr y mantener a través de la implementación de medidas de control el nivel de probabilidad e impacto residual de los riesgos a el nivel aceptable por parte de la Alta Gerencia.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: DOC-GTI-02
		Versión: 01
	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Fecha Emisión: 30/01/2024

5 TERMINOS Y DEFINICIONES

A continuación, se listan algunos términos y definiciones de términos que se utilizarán durante el desarrollo de la gestión de riesgos de seguridad de la información, en beneficio de unificar criterios dentro de la Empresa de Desarrollo y Renovación Urbana EDRU E.I.C.E.

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evalúa.

Control: Medida que modifica el riesgo.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.


Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

X



607

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: DOC-GTI-02
	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Versión: 01
Fecha Emisión: 30/01/2024		

Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.


Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorías de los sistemas integrados de gestión.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

 <p>EDRU Empresa de Desarrollo y Renovación Urbana</p>	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: DOC-GTI-02
	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Versión: 01
		Fecha Emisión: 30/01/2024

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Riesgo en la seguridad de la información. Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo. Aceptación de la pérdida o ganancia proveniente de un riesgo particular

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.

Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

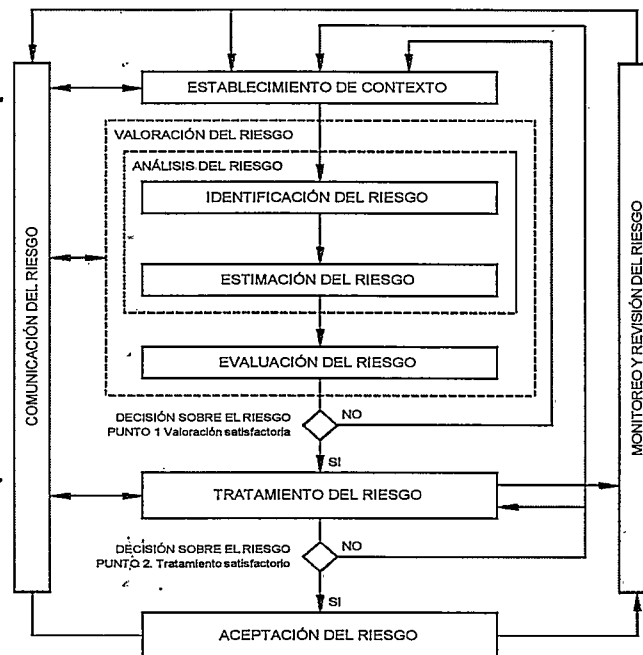
SGSI: Sistema de Gestión de Seguridad de la Información.

X


8
9

6 VISION GENERAL DEL PROCESO DE GESTION DE RIESGO EN LA SEGURIDAD DE LA INFORMACION

A continuación, se presenta el modelo de gestión de riesgos de seguridad de la información diseñado basado tanto en la norma ISO/IEC 31000 como en la ISO 27005 aprobado por la Empresa de Desarrollo y Renovación Urbana EDRU E.I.C.E para la adecuada administración de riesgos, en la seguridad de la información; los elementos que lo componen son:



La gestión de riesgos de seguridad de la información deberá ser iterativa para las actividades de valoración de riesgos y/o tratamiento de estos.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: DOC-GTI-02
		Versión: 01
	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Fecha Emisión: 30/01/2024

6.1 ESTABLECIMIENTO DEL CONTEXTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN


El contexto de gestión de riesgos de seguridad de la información define los criterios básicos que serán necesarios para enfocar el ejercicio por parte de la EDRU y obtener los resultados esperados, basándose en, la identificación de las fuentes que pueden dar origen a los riesgos y oportunidades en los procesos de la EDRU, en el análisis de las debilidades y amenazas asociadas, en la valoración de los riesgos en términos de sus consecuencias para la Entidad y en la probabilidad de su ocurrencia, al igual que en la construcción de acciones de mitigación en beneficio de lograr y mantener niveles de riesgos aceptables para la Entidad.

Como criterios para la gestión de riesgos de seguridad de la información se establecen:

6.1.1 Criterios de evaluación del riesgo de seguridad de la información:

La evaluación de los riesgos de seguridad de la información se enfocará en:

- El valor estratégico del proceso de información en la EDRU.
- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales.
- La importancia de la disponibilidad, integridad y confidencialidad para las operaciones de la EDRU.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y reputación de la EDRU.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: DOC-GTI-02
		Versión: 01
	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Fecha Emisión: 30/01/2024

6.1.2 Criterios de Impacto

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para la EDRU, causados por un evento de seguridad de la información, considerando aspectos tales como:


- Nivel de clasificación de los activos de información impactados.
- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad).
- Operaciones deterioradas (afectación a partes internas o terceras partes).
- Pérdida del negocio y del valor financiero.
- Alteración de planes o fechas límites.
- Daños en la reputación.
- Incumplimiento de los requisitos legales, reglamentarios o contractuales.

Los niveles de clasificación de los impactos establecidos por la EDRU se podrán tomar del documento Mapas de Calor, elaborados con cada una de las áreas, que para este plan se contemplan en los procesos de *Gestión Estratégica* y *Gestión de Planeación*.

6.1.3 Criterios de Aceptación

Los criterios de aceptación dependerán con frecuencia de las políticas, metas, objetivos de la EDRU y de las partes interesadas, por tanto, las escalas de aceptación de riesgos de seguridad de información se podrán tomar del documento.

x

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: DOC-GTI-02
		Versión: 01
	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Fecha Emisión: 30/01/2024

6.2 VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Los riesgos se deberán identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes para la EDRU, esta fase consta de las siguientes etapas:

La valoración del Riesgo de seguridad de la información consta de las siguientes actividades:

- Análisis del riesgo
 - a) Identificación de los riesgos
 - b) Estimación del riesgo
- Evaluación del riesgo


6.2.1 Identificación del riesgo

Para la evaluación de riesgos de seguridad de la información en primer lugar se deberán identificar los activos de información por proceso en evaluación.

Los **activos de información** se clasifican en dos tipos:

a) **Primarios:**

- a. **Procesos o subprocesos y actividades del Negocio:** procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.
- b. **Información:** información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información


	<p style="text-align: center;">PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</p>	Código: DOC-GTI-02
		Versión: 01
	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Fecha Emisión: 30/01/2024

- c. estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.
- d. Actividades y procesos de negocio: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual.

b) De Soporte

- a. **Hardware:** Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).
- b. **Software:** Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.).
- c. **Redes:** Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)
- d. **Personal:** Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)
- e. **Sitio:** Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización Sede principal (Edificio Fuente Versailles y Centro de Inclusión Social y Oportunidades Barrio San Pascual)
- f. **Estructura organizativa:** responsables, áreas, contratistas.

Después de tener una relación con todos los activos se han de conocer las **amenazas** que pueden causar daños en la información, los procesos y los soportes. La identificación

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código:
		DOC-GTI-02
	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Versión:
01		
		Fecha Emisión:
		30/01/2024

de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios y expertos.

Posterior a la identificación del listado de activos, sus amenazas y las medidas que ya se han tomado, a continuación, se revisarán las **vulnerabilidades** que podrían aprovechar las amenazas y causar daños a los activos de información de la EDRU. Existen distintos métodos para analizar amenazas, por ejemplo:

- Entrevistas con líderes de procesos y usuarios
- Inspección física
- Uso de las herramientas para el escaneo automatizado

Para cada una de las **amenazas** analizaremos las **vulnerabilidades** (debilidades) que podrían ser explotadas.

Finalmente se identificarán las **consecuencias**, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información.


6.2.2 Estimación del riesgo

La estimación del riesgo busca establecer la *probabilidad* de ocurrencia de los riesgos y el *impacto* de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos. El objetivo de esta etapa es el de establecer una valoración y priorización de los riesgos.

Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

- **Probabilidad:** La posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse.
- **Impacto:** Hace referencia a las consecuencias que puede ocasionar a la EDRU la materialización del riesgo; se refiere a la magnitud de sus efectos.

Se sugiere realizar este análisis con todas o las personas que más conozcan del proceso, y que por sus conocimientos o experiencia puedan determinar el impacto y la probabilidad del riesgo de acuerdo con los rangos señalados en las tablas que se muestran más adelante.

 EDRU Empresa de Desarrollo y Renovación Urbana	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: DOC-GTI-02
		Versión: 01
	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Fecha Emisión: 30/01/2024

Como criterios para la estimación del riesgo desde el enfoque de impacto y consecuencias se podrán tener en cuenta: pérdidas financieras, costes de reparación o sustitución, interrupción del servicio, disminución del rendimiento, infracciones legales, pérdida de ventaja competitiva, daños personales, entre otros.

Además de medir las posibles consecuencias se deberán analizar o estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información o la operación del negocio.

Formulario para el registro de la estimación de los riesgos de seguridad de la información:

Para realizar el análisis de riesgo de un proceso, se utilizará el *Mapa de riesgos institucionales y por proceso* que adaptó oficina asesora de control interno de la EMRU en el cual personas del equipo deberán calificar el impacto y la probabilidad de cada uno de los riesgos identificados de acuerdo con los niveles para la estimación de los riesgos.

PROBABILIDAD			
Concepto	Valor	Descripción	Frecuencia
Rara vez	1	El evento puede ocurrir sólo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años
Improbable	2	Es muy poco factible que el evento se presente.	Al menos de 1 vez en los últimos 5 años.
Posible	3	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
Probable	4	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en el último año.
Casi Seguro	5	Se espera que ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

Adaptado para la EDRU de la Guía de Riesgos DAFP, 2013



**PLAN DE TRATAMIENTO DE
RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA
INFORMACIÓN**

Código:
DOC-GTI-02


Versión:
01

Fecha Emisión:
30/01/2024

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

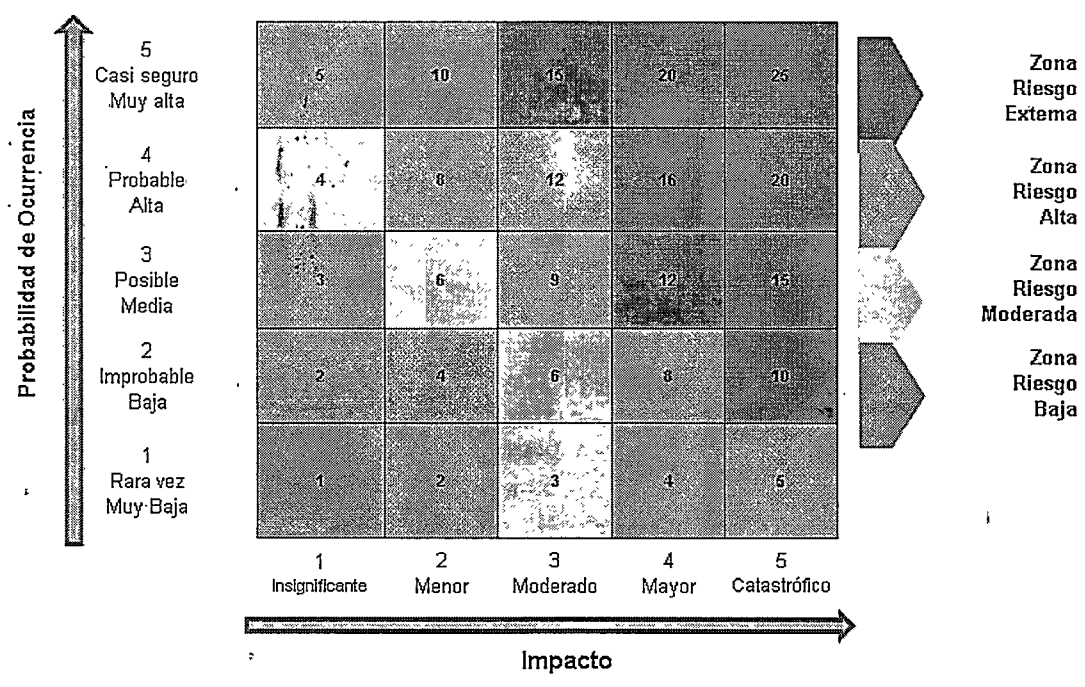
IMPACTO		
Concepto	Valor	Descripción
Insignificante	1	La materialización del riesgo puede ser controlado por los participantes del proceso, y no afecta los objetivos del proceso.
Menor	6	La materialización del riesgo ocasiona pequeñas demoras en el cumplimiento de las actividades del proceso, y no afecta significativamente el cumplimiento de los objetivos de la EDRU. Tiene un impacto bajo en los procesos de otras áreas de la EDRU.
Moderado	7	La materialización del riesgo demora el cumplimiento de los objetivos del proceso , y tiene un impacto moderado en los procesos de otras áreas de la EDRU. Puede además causar un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma normal.
Mayor	11	La materialización del riesgo retrasa el cumplimiento de los objetivos de la EDRU y tiene un impacto significativo en la imagen pública de la EDRU. Puede además generar impactos en: la industria, sectores económicos, el cumplimiento de acuerdos y obligaciones legales y las finanzas públicas; entre otras.
Catastrófico	13	La materialización del riesgo imposibilita el cumplimiento de los objetivos de la EDRU , tiene un impacto catastrófico en la imagen pública de la EDRU. Puede además generar impactos en: sectores económicos, los mercados; la industria, el cumplimiento de acuerdos y obligaciones legales; multas y las finanzas públicas; entre otras.

Adaptado para la EDRU de la Guía de Riesgos DAFP, 2013


	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: DOC-GTI-02
		Versión: 01
	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Fecha Emisión: 30/01/2024.

6.2.3 Determinación del riesgo inherente y residual

El análisis del riesgo determinado por su probabilidad e impacto permite tener una primera evaluación del riesgo inherente (escenario sin controles) y ver el grado de exposición al riesgo que tiene la entidad. La exposición al riesgo es la ponderación de la probabilidad e impacto, y se puede ver gráficamente en la matriz de riesgo, instrumento que muestra las zonas de riesgos y que facilita el análisis gráfico. Permite analizar de manera global los riesgos que deben priorizarse según la zona en que quedan ubicados los mismos (zona de riesgo bajo, moderado, alto o extremo) facilitando la organización de prioridades para la decisión del tratamiento e implementación de planes de acción.



Esquema general de Matriz de Riesgo Institucional y Zonas de Riesgo Institucional para la EDRU.

	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: DOC-GTI-02
		Versión: 01
	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Fecha Emisión: 30/01/2024

6.2.4 Evaluación de los riesgos

Una vez se valoran los impactos, la probabilidad y las consecuencias de los escenarios de incidentes sobre los activos de información, se obtendrán los niveles de riesgo, para los cuales se deberán comparar frente a los criterios básicos del contexto, para una adecuada y pertinente toma de decisiones basada en riesgos de seguridad de la información y en beneficio de reducir su impacto a la EDRU!


6.3 TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Como resultado de la etapa de evaluación del riesgo tendremos una lista ordenada de riesgos o una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos.

De acuerdo con el nivel evaluación de los riesgos, se deberá seleccionar la opción de tratamiento adecuada por cada uno de los riesgos identificados; el costo/beneficio del tratamiento deberá ser un factor de decisión relevante para la decisión.

COSTO - BENEFICIO	OPCIÓN DE TRATAMIENTO
El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios	Evitar el riesgo, su propósito es no proceder con la actividad o la acción que da origen al riesgo (ejemplo, dejando de realizar una actividad, tomar otra alternativa, etc.)
El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo	Transferir o compartir el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el servicio).
El costo y el tiempo del tratamiento es adecuado a los beneficios	Reducir o Mitigar el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto
La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.	Retener o aceptar el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa



	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: DOC-GTI-02
		Versión: 01
	GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	Fecha Emisión: 30/01/2024

El resultado de esta fase se concreta en un plan de tratamiento de riesgos, es decir, la selección y justificación de una o varias opciones para cada riesgo identificado, que permitan establecer la relación de riesgos residuales, es decir, aquellos que aún siguen existiendo a pesar de las medidas tomadas.

Nota: Será conveniente que para la selección de los controles se consideren posibles restricciones o limitantes que impidan su elección tales como: restricciones de tiempo, financieras, técnicas, operativas, culturales, éticas, ambientales, legales, uso, de personal o las restricciones para la integración de controles nuevos y existentes.

6.4 MONITOREO Y SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Periódicamente se revisará el valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración iterativa de los riesgos de seguridad de la información.

Los riesgos son dinámicos como la misma Entidad (EDRU) por tanto podrán cambiar de forma o manera radical sin previo aviso. Por ello es necesaria una supervisión continua que detecte: (1) nuevos activos o modificaciones en el valor de los activos, (2) nuevas amenazas • (3) cambios o aparición de nuevas vulnerabilidades • (4) aumento de las consecuencias o impactos, (5) incidentes de seguridad de la información.

Con el propósito de conocer los estados de cumplimiento de los objetivos de la gestión de los riesgos de seguridad de la información, se deberán definir esquemas de seguimiento y medición al sistema de gestión de riesgos de la seguridad de la información que permitan contextualizar una toma de decisiones de manera oportuna.



**PLAN DE TRATAMIENTO DE
RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA
INFORMACIÓN**

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

Código:
DÓC-GTI-02

Versión:
01

Fecha Emisión:
30/01/2024

Descripción del Riesgo	Criterios para la Evaluación del Control No. 1 (Copiar y pegar el control)	Evaluación		Puntaje	Justificación de la respuesta
		SI	No		
Pérdida de información sensible, asociada al proceso.	¿El control previene la materialización del riesgo (afecta probabilidad)?	X			El control establecido permite minimizar la ocurrencia del riesgo, con el desarrollo de aplicativos que permiten contar con la información sensible para el proceso, en línea, como lo son procesos de contratación, bases de datos.
	¿El control permite enfrentar la situación en caso de materialización (afecta impacto)?	X			
	¿Existen manuales, instructivos o procedimientos para el manejo del control?	20	0	0	
	¿El control es totalmente automático? (Sistemas o Software que permiten incluir contraseñas de acceso, o con controles de seguimiento a aprobaciones o ejecuciones que se realizan a través de éste, generación de reportes o indicadores, sistemas de seguridad con scanner, sistemas de grabación, entre otros). Nota: si el control es automático en la siguiente pregunta dejar cero.	25	0	25	
	¿El control es manual? Políticas de operación aplicables, autorizaciones a través de firmas o confirmaciones vía correo electrónico, archivos físicos, consecutivos, listas de chequeo, controles de seguridad con personal especializado, entre otros).	20	0	0	
	¿Se cuenta con evidencias de la ejecución y seguimiento del control?	20	0	0	
	El control es efectivo (sirve o cumple su función?)	35	0	0	
Total				25	