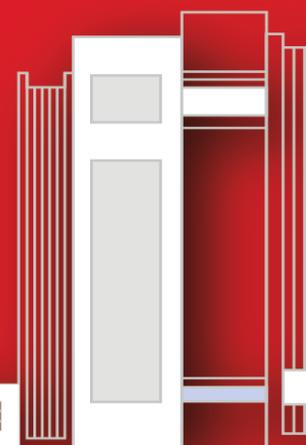


# PLANES INSTITUCIONALES 2025

**Plan de Tratamiento de  
Riesgos de la Seguridad y  
Privacidad de la Información**  
Vigencia 2025



**GOBERNACIÓN**  
Departamento del  
Valle del Cauca





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

P15-T

Versión:2

27/01/2020

Página 2 de 12

## CONTENIDO

1. Objetivo .....	3
1.1. Objetivos Específicos .....	3
2. Alcance .....	4
3. Términos y definiciones .....	4
4. Plan de tratamiento de riesgos de seguridad y privacidad de la información .....	10
4.1. Riesgos de seguridad y privacidad de la información .....	10
4.2. Programación de monitoreo de controles de riesgos de seguridad y privacidad de la información .....	11
5. Marco legal .....	6
6. Requisitos técnicos.....	10
7. Conclusión .....	<b>iError! Marcador no definido.</b>



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

P15-T

Versión:2

27/01/2020

Página 3 de 12

---

## 1. INTRODUCCIÓN

---

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto del proceso, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicionalmente 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 por la Biblioteca Departamental Jorge Garcés Borrero.

---

## 2. OBJETIVO

---

Establecer las actividades orientadas a tratar de manera integral los riesgos de Seguridad y Privacidad de la Información a los cuales la Biblioteca puede estar expuesta; con el fin de alcanzar sus objetivos institucionales y el cumplimiento de su misión y visión y la prestación de los servicios protegiendo y preservando la integridad, confidencialidad y disponibilidad de la información.

### **Objetivos Específicos**

- Gestionar los riesgos de Seguridad y Privacidad de la Información, teniendo en cuenta los activos de información identificados.
- Mantener actualizado el inventario del parque tecnológico identificando su ubicación y propietario.
- Aplicar Manual de administración del riesgo de la Biblioteca Departamental Jorge Garcés Borrero en su versión más reciente.
- Socializar y sensibilizar a los funcionarios y contratistas, los lineamientos establecidos para la gestión de riesgos de Seguridad y Privacidad de la Información.

	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	P15-T
		Versión:2
		27/01/2020
		Página 4 de 12

- ar cumplimiento a los requisitos legales y normativos en materia de riesgos de seguridad y privacidad de la información.

---

### 3. ALCANCE

---

El alcance está del plan de tratamiento de riesgos está dirigido para cada uno de los procesos estratégicos, misionales y de apoyo de la Biblioteca Departamental Jorge Garcés Borrero.

---

### 4. TÉRMINOS Y DEFINICIONES

---

Para los propósitos de este documento, MANUAL DE ADMINISTRACIÓN DEL RIESGO de la BIBLIOTECA DEPARTAMENTAL JORGE GARCÉS BORRERO

**Riesgo:** es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

**Gestión del Riesgo:** En términos generales la gestión del riesgo se refiere a los principios y metodología para la gestión eficaz del riesgo, mientras que gestionar el riesgo se refiere a la aplicación de estos principios y metodología a riesgos particulares.

**Administración del riesgo:** La administración del Riesgo comprende el conjunto de Elementos de Control y sus interrelaciones, para que la institución evalúe e intervenga aquellos eventos, tanto Internos como externos.

**Contexto estratégico:** Son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución. Las situaciones del entorno o externas pueden ser de carácter social, cultural, económico, tecnológico, político y legal, bien sean internacional nacional o regional según sea el caso de análisis.



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

P15-T

Versión:2

27/01/2020

Página 5 de 12

**Identificación de riesgos:** se realiza determinando las causas, con base en los factores internos y/o externos analizados para la entidad, y que pueden afectar el logro de los objetivos. con base en los factores de riesgo internos y externos (contexto estratégico), presentando una descripción de cada uno de estos y finalmente definiendo los posibles efectos (consecuencias).

**Análisis de riesgos:** busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias, este último aspecto puede orientar la clasificación del riesgo, con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar. Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados: Probabilidad e Impacto. Se debe Calificar numéricamente a través de la estimación de su ocurrencia.

**Evaluación del Riesgo:** permite comparar los resultados de la calificación del riesgo, con los criterios definidos para establecer el grado de exposición de la entidad; de esta forma es posible distinguir entre los riesgos aceptables, tolerables, moderados, importantes o inaceptables y fijar las prioridades de las acciones requeridas para su tratamiento. Para facilitar la calificación y evaluación a los riesgos, se debe definir una matriz que contempla un análisis cualitativo, para presentar la magnitud de las consecuencias potenciales (impacto) y la posibilidad de ocurrencia (probabilidad). Las categorías relacionadas con el impacto son: insignificante, menor, moderado, mayor y catastrófico. Las categorías relacionadas con la probabilidad son raro, improbable, posible, probable y casi seguro.

**Valoración de riesgos:** es el producto de confrontar los resultados de la evaluación del riesgo con los controles identificados, esto se hace con el objetivo de establecer prioridades para su manejo y para la fijación de políticas. Para adelantar esta etapa se hace necesario tener claridad sobre los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones.

**Políticas de administración de riesgos:** Las políticas identifican las opciones para tratar y manejar los riesgos basadas en la valoración de los mismos, permiten tomar decisiones adecuadas y fijar los lineamientos, que van a transmitir la posición de la dirección y establecen las guías de acción necesarias a todos los servidores de la entidad.

## 5. MARCO LEGAL

La política de tratamiento de LA BIBLIOTECA DEPARTAMENTAL JORGE GARCÉS BORRERO sobre la información que la institución administra, se desarrolla en cumplimiento:

Decreto 612 de 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las Entidades del Estado.

Decreto 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

Marco Normativo	Descripción
<b>Ley 44 de 1993</b>	Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).
<b>Ley 1273 de 2009</b>	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
<b>Ley 1341 de 2009</b>	Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
<b>Ley 527 de 1999</b>	Por 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 establecen las entidades de certificación y se dictan otras disposiciones
<b>Ley 1266 de 2008</b>	Por la cual se dictan las disposiciones generales del Habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera,



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

P15-T

Versión:2

27/01/2020

Página 7 de 12

Marco Normativo	Descripción
	crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
<b>Ley 594 de 2000</b>	Por medio de la cual se expide la Ley General de Archivos
<b>Ley 1581 de 2012</b>	Por la cual se dictan disposiciones generales para la protección de datos personales.
<b>Ley 1712 de 2014</b>	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.
<b>Ley 1915 de 2018</b>	Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
<b>Ley 1952 de 2019</b>	Por medio de la cual se expide el código general disciplinario.
<b>Decreto 1413 de 2017</b>	En el Capítulo 2 Características de los Servicios Ciudadanos Digitales, Sección 1 Generalidades de los Servicios Ciudadanos Digitales
<b>Ley 1474 de 2011</b>	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
<b>Decreto 2150 de 1995</b>	Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
<b>Decreto 4485 de 2009</b>	Por medio de la cual se adopta la actualización de la Norma Técnica de Calidad en la Gestión Pública.
<b>Decreto 235 de 2010</b>	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
<b>Decreto 2364 de 2012</b>	Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
<b>Decreto 2693 de 2012</b>	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011, y se dictan otras disposiciones.



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

P15-T

Versión:2

27/01/2020

Página 8 de 12

Marco Normativo	Descripción
<b>Decreto 1377 de 2013</b>	Por el cual se reglamenta parcialmente la Ley 1581 de 2012" o Ley de Datos Personales.
<b>Decreto 2573 de 2014</b>	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones
<b>Decreto 2433 de 2015</b>	Por el cual se reglamenta el registro de TIC y se subroga el título 1 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.
<b>Decreto 1078 de 2015</b>	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
<b>Decreto 103 de 2015</b>	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
<b>Decreto 415 de 2016</b>	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las Comunicaciones.
<b>Decreto 728 2016</b>	Actualiza el Decreto 1078 de 2015 con la implementación de zonas de acceso público a Internet inalámbrico
<b>Decreto 728 de 2017</b>	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
<b>Decreto 612 de 2018</b>	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
<b>Decreto 2106 del 2109</b>	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública

Marco Normativo	Descripción
	Cap. II Transformación Digital Para Una Gestión Pública Efectiva
<b>Decreto 620 de 2020</b>	Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"
<b>Resolución 2710 de 2017</b>	Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.
<b>Resolución 3564 de 2015</b>	Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
<b>Resolución 3564 2015</b>	Reglamenta algunos artículos y párrafos del Decreto número 1081 de 2015 (Lineamientos para publicación de la Información para discapacitados)
<b>Norma Técnica Colombiana NTC 5854 de 2012</b>	Accesibilidad a páginas web El objeto de la Norma Técnica Colombiana (NTC) 5854 es establecer los requisitos de accesibilidad que son aplicables a las páginas web, que se presentan agrupados en tres niveles de conformidad: A, AA, y AAA.
<b>CONPES 3292 de 2004</b>	Señala la necesidad de eliminar, racionalizar y estandarizar trámites a partir de asociaciones comunes sectoriales e intersectoriales (cadenas de trámites), enfatizando en el flujo de información entre los eslabones que componen la cadena de procesos administrativos y soportados en desarrollos tecnológicos que permitan mayor eficiencia y transparencia en la prestación de servicios a los ciudadanos.
<b>CONPES 3920 de Big Data, del 17 de abril de 2018</b>	La presente política tiene por objetivo aumentar el aprovechamiento de datos, mediante el desarrollo de las condiciones para que sean gestionados como activos para generar valor social y económico. En lo que se refiere a las actividades de las entidades públicas, esta generación de valor es entendida como la provisión de bienes públicos para brindar respuestas efectivas y útiles frente a las necesidades sociales.
<b>CONPES 3975</b>	Define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los



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

P15-T

Versión:2

27/01/2020

Página 10 de 12

Marco Normativo	Descripción
	lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema.
<b>Circular 02 de 2019</b>	Con el propósito de avanzar en la transformación digital del Estado e impactar positivamente la calidad de vida de los ciudadanos generando valor público en cada una de las interacciones digitales entre ciudadano y Estado y mejorar la provisión de servicios digitales de confianza y calidad.
<b>Directiva 02 2019</b>	Moderniza el sector de las TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones

## 6. SITUACIÓN ACTUAL

### Plan de tratamiento de riesgos de seguridad y privacidad de la información

En concordancia con el Modelo de seguridad y Privacidad de la información, busca mitigar los riesgos y sus consecuencias que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

De esta forma se pueden convertir los riesgos en oportunidad de mejoras, acorde con el manual de administración de riesgos de la Biblioteca Departamental Jorge Garcés Borrero M03-PMC-01-16.

### Riesgos de seguridad y privacidad de la información

Se realizaron acciones establecidas para mitigar algunos de los riesgos, y que a su vez parte de estas acciones se ve reflejado, en principio la implementación ya actualizada de Firewall UTM como seguridad perimetral mediante monitoreo registrado en el Software de Mesa de Ayuda.



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

P15-T

Versión:2

27/01/2020

Página 11 de 12

La acción de mejora encaminada a mejorar y actualizar la seguridad perimetral, por lo que se propuso y se ejecutó la compra e implementación del conjunto de Firewall y solución antimalware con soporte comercial que se administran de forma local y en la nube, lo que garantiza la administración y seguridad al interior de la entidad en su red y en el parque informático.

### Programación de monitoreo de controles de riesgos de seguridad y privacidad de la información

Se debe continuar identificando nuevos riesgos, donde se establecerán acciones a seguir partiendo de lo cual se determinarán los controles para ser monitoreados periódicamente, siguiendo el lineamiento establecido por el manual de la gestión del riesgo, partiendo de lo cual se establecerá la frecuencia de monitoreo.

## 7. MAPA DE RUTA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos identificados en la entidad, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016):

ITEM	ACTIVIDAD	TAREAS
1	Sensibilización	Socialización de lineamientos y herramientas para la Gestión de Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital.
2	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y	Contexto, identificación, análisis y evaluación de riesgos. Realimentación, revisión y verificación de los riesgos identificados. (Ajustes).



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

P15-T

Versión:2

27/01/2020

Página 12 de 12

ITEM	ACTIVIDAD	TAREAS
	Continuidad de la Operación.	
3	Aceptación de Riesgos Identificados	Aceptación, aprobación y definición de planes de tratamiento.
4	Divulgación	Publicación de mapas de riesgos de procesos.
5	Seguimiento fase de tratamiento	Seguimiento a la implementación de controles y planes de tratamiento de riesgos identificados.
6	Mejoramiento	Identificación de oportunidades de mejora acorde al seguimiento de la ejecución de los controles y de los planes de tratamiento. Revisión y/o actualización de lineamientos de Riesgos de Seguridad y privacidad de la información de acuerdo con las observaciones identificadas.
7	Monitoreo y Revisión	Medición, presentación y reporte de indicadores.

## 8. MEDICIÓN Y SEGUIMIENTO

Para verificación del cumplimiento del plan se realizará a través del número de actividades ejecutadas sobre las programadas en la tabla

*Cumplimiento del Plan de TRSPI 2025 = Actividades Ejecutadas / Actividades Planeadas × 100%*

De igual forma, la eficacia de las acciones definidas se observará a través del informe de segunda línea de defensa o informe final de gestión del riesgo.

*Elaboró: Catherine Aristizabal Montúfar – Profesional Universitario – Planeación y Mejoramiento Continuo*

*Aprobó: Comité Institucional de Gestión y Desempeño ACTA No.01-2025 del 24 de enero del 2025*

*Adoptado mediante resolución N° 231.23.01.045 del 30 de enero de 2025*