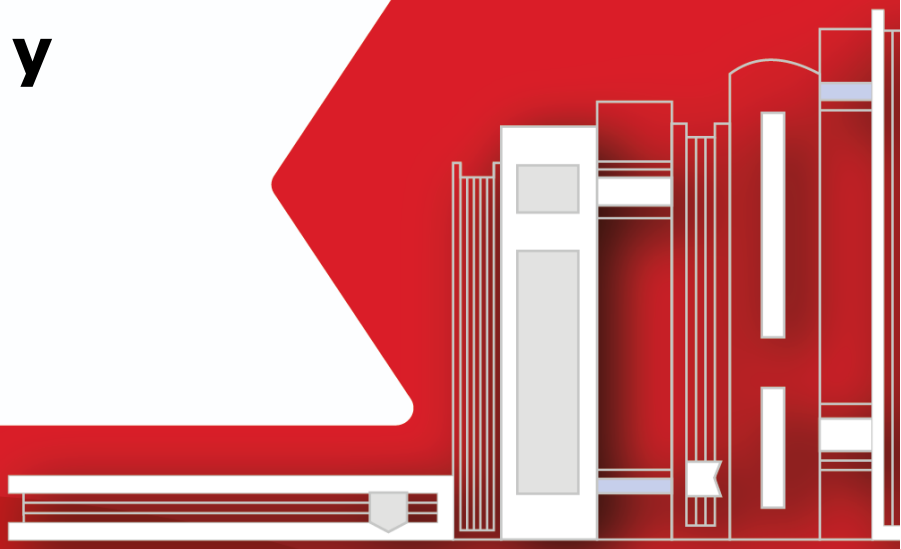
PLANES INSTITUCIONALES 2025

Plan de Seguridad y Privacidad de la Información - PSI

Vigencia 2025



GOBERNACIÓN Departamento del Valle del Cauca

paraíso de todos

Biblioteca DEPARTAMENTAL Jorge Garcés Borrero - Valle del Cauca

CONTENIDO

1. INTRODUCCIÓN

La Biblioteca Departamental del Valle del Cauca Jorge Garcés Borrero como ente descentralizado de la Gobernación del Valle del Cauca, ofrece servicios Bibliotecarios para: promover la ciencia, cultura e innovación tecnológica, por lo cual en el normal desarrollo de sus procesos administrativos y misionales hace uso de las tecnologías de la información.

Dado lo anterior, la biblioteca tiene el deber de cumplir la política de gobierno digital según el decreto No 1008 del 14 de junio del 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

En relación con lo anterior cualquier entidad sin distinción de tamaño y naturaleza, debe de ser consciente de las amenazas que fluctúan y evolucionan a diario que afectan directamente en sobre confidencialidad, integridad y disponibilidad de la información de las entidades del Estado.

En consecuencia, de lo anterior, bajo un contexto multidisciplinario el Proceso de telemática con la oficina de planeación, tiene la tarea de actualizar los riegos informáticos, que puedan afectar el buen ejercicio de las labores de los funcionarios y/o la comunidad académica.

La Biblioteca Departamental del Valle del Cauca Jorge Garcés Borrero en concordancia con MSPI, adoptará y ajustará según necesidades particulares de la entidad basándose en la EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A, justificando las que no aplique, como lo establece el Instrumento Evaluación MSPI, proporcionando un marco metodológico que usa como referencia las buenas prácticas, tales como GTC/ISO 27002:2015, ISO 27005:2009, etc.; recomendaciones de las mejores prácticas en la gestión de

la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

Bajo esta perspectiva, con el fin de lograr una correcta implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información, instituye el Plan Estratégico de Seguridad y Privacidad de la Información, documento en el cual establecen los aspectos a tener en cuenta para el establecimiento de un sistema que cumple con los mejores estándares a nivel nacional e internacional. Para lo anterior, se realiza un análisis de la situación actual y deseada, así mismo se plantean las herramientas y diferentes aspectos como proyectos y actividades que se requieren llevar a cabo por parte de la Biblioteca JGB, para lograr un nivel adecuado para la protección de la confidencialidad, integridad y disponibilidad de su información, principios fundamentales que constituyen el pilar de la protección de los activos de la información.

En resumen, el plan estratégico de seguridad de la información es fundamental para proteger los activos de información de la Biblioteca, garantizar el cumplimiento normativo, mitigar riesgos, y mantener la confianza y la continuidad del negocio.

2. OBJETIVOS

Objetivo General

Adoptar e implementar los lineamientos del Modelo de Seguridad y Privacidad de la Información MSPI y la Estrategia de seguridad digital conforme a lo establecido por MinTic con el objetivo de implementar un sistema de Getión de Seguridad de la información que permita fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Biblioteca Departamental del Valle del Cauca Jorge Garcés Borrero y el tratamiento de sus riesgos.

Objetivos Específicos

- Definir y comunicar la Estrategia de seguridad de la información y seguridad digital.
- Definir y establecer las necesidades para la implementación del Sistema de Gestión de Seguridad de la Información y seguridad digital.
- Cambiar el estado de conocimiento sobre el nivel de madurez en la gestión de la seguridad de la información, mediante análisis organizacional basado en el numeral 4 de la NTC ISO27001:2022 con un enfoque de mejora de la seguridad de la información dado que son aplicables a todas las organizaciones, sin distinción.
- Definir y/o actualizar controles para mitigar los riesgos de seguridad de la información.

3. ALCANCE

Teniendo en cuenta la naturaleza de los servicios Bibliotecarios para promover la ciencia, cultura e innovación tecnológica que ofrece la Biblioteca Departamental del Valle del Cauca Jorge Garcés Borrero, el alcance de este plan de seguridad de la información Asegurar los recursos de TI, garantizando la continuidad de la prestación de los servicios de los procesos: estratégicos, misionales, de apoyo y de control", conforme con su misión y visión aplicables a todos los requisitos de la NTC/ISO 27001 y todos los controles del Anexo A, sin excepción alguna.

de la NTC/ISO 27001 y los controles del Anexo A, acorde a la naturaleza jurídica, misión y visión con un enfoque de mejora de la seguridad de la información.

4. DEFINICIONES

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.

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. REFERENCIAS DOCUMENTALES

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.
- NTC-ISO/IEC 27001
- ISO 22301

6. MARCO NORMATIVO

Marco Normativo	Descripción
Ley 44 de 1993	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).
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 1341 de 2009	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.

Marco Normativo	Descripción
Ley 527 de 1999	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
Ley 1266 de 2008	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, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 594 de 2000	Por medio de la cual se expide la Ley General de Archivos
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 1915 de 2018	Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
Ley 1952 de 2019	Por medio de la cual se expide el código general disciplinario.
Decreto 1413 de 2017	En el Capítulo 2 Características de los Servicios Ciudadanos Digitales, Sección 1 Generalidades de los Servicios Ciudadanos Digitales
Ley 1474 de 2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de

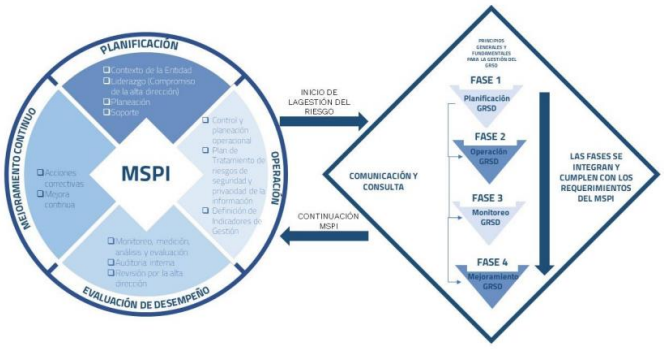
Marco Normativo	Descripción
	actos de corrupción y la efectividad del control de la gestión pública.
Decreto 2150 de 1995	Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
Decreto 4485 de 2009	Por medio de la cual se adopta la actualización de la Norma Técnica de Calidad en la Gestión Pública.
Decreto 235 de 2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
Decreto 2364 de 2012	Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
Decreto 2693 de 2012	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.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012" o Ley de Datos Personales.
Decreto 2573 de 2014	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
Decreto 2433 de 2015	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.

Marco Normativo	Descripción
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 415 de 2016	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.
Decreto 728 2016	Actualiza el Decreto 1078 de 2015 con la implementación de zonas de acceso público a Internet inalámbrico
Decreto 728 de 2017	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.
Decreto 612 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 2106 del 2109	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública Cap. II Transformación Digital Para Una Gestión Pública Efectiva

Marco Normativo	Descripción
Decreto 620 de 2020	Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"
Resolución 2710 de 2017	Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.
Resolución 3564 de 2015	Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
Resolución 3564 2015	Reglamenta algunos artículos y parágrafos del Decreto número 1081 de 2015 (Lineamientos para publicación de la Información para discapacitados)
Norma Técnica Colombiana NTC 5854 de 2012	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.
CONPES 3292 de 2004	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.
CONPES 3920 de Big Data, del 17 de abril de 2018	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

Marco Normativo	Descripción
	para brindar respuestas efectivas y útiles frente a las necesidades sociales.
CONPES 3975	Define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los 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.
Circular 02 de 2019	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.
Directiva 02 2019	Moderniza el sector de las TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones

7. METODOLOGÍA IMPLEMENTACIÓN MODELO DE SEGURIDAD



FUENTE: MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES.

Ciclo Operación

Garantizar la seguridad y la privacidad de la información, por lo cual el modelo de seguridad y privacidad de la información contempla un ciclo de operación que contempla cinco (5) fases que a su vez el modelo puede operar en el ciclo PHVA basado en la ISO 27001, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

Figura 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

Fuente: Manual de estrategia de gobierno en línea

Fase Diagnostico: Permitirá a la Biblioteca Departamental JGB identificar el estado su estado actual con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Fase Planificación (Planear): La Biblioteca Departamental JGB establecerá los objetivos, procesos y procedimientos de seguridad, teniendo en cuenta los recursos, los requisitos del catálogo de servicios a prestar, las políticas e identificar y abordar los riesgos como oportunidad de mejora.

Fase Implementación (Hacer): La Biblioteca Departamental JGB Implementará el plan, procedimientos y políticas establecidas con los recursos apoyados por la Entidad.

Fase Evaluación de desempeño (Verificar): La Biblioteca Departamental JGB realizará evaluación una vez implantado el plan, procedimientos contra la política o lineamiento, y establecerá un seguimiento de medición de los procesos y servicios en cumplimiento de los objetivos de seguridad, con sus actividades planificadas e informará sobre los resultados en un periodo definido.

Fase Mejora Continua (Actuar): Según el resultado de los informes de auditoría interna y previa verificación de la dirección, La Biblioteca Departamental JGB emprenderá acciones correctivas y/o preventivas, con la finalidad de lograr mejora continua.

Alineación NORMA ISO 27001 Vs Ciclo De Operación

A la hora de implementar un Sistema de Gestión de Seguridad de la Información basado en el estándar internacional ISO 27001 se adaptaran con una serie de lineamientos, se debe utilizar el ciclo PDCA (siglas en inglés) o PHVA (siglas en español), logrando alinear el ciclo de mejora continua.

Ciclo operaciones PHVA cuenta con los siguientes pasos:

Planificar: se establece el Sistema de Gestión de Seguridad de la Información.

Hacer: se implementa el SGSI.

Verificar: revisión del Sistema de Gestión de Seguridad de la Información.

Actuar: en este paso del ciclo lo que se hace es mantener y mejorar el SGSI.

Ciclo ISO 27001.

Dado lo anterior el modelo se va a basar en el ciclo PHVA, el cual es recomendado por la norma NTC-ISO/IEC 27001 Centrándose en los requisitos cubiertos en los capítulos 4 a 10, y si bien ISO-27002 deja de ser una referencia normativa aún es necesaria para implementar este estándar.

Figura sustraída del Ciclo de mejora continua norma ISO/IEC 27001:2013

8. SITUACIÓN ACTUAL

Entiéndase por situación actual, al nivel de madurez sobre los dominios de seguridad informática que tiene la Biblioteca Departamental Jorge Garcés Borrero, este estado de conciencia se consigue basándose en el uso de una herramienta de diagnóstico del MSPI de MINTIC , datos necesarios para implementar la metodología PHVA que a su vez es una propuesta sugerida en la NTC-ISO/IEC 27001, que se trabajar con un enfoque en cambiar el estado de conciencia de la situación actual en cuanto a Gestión de seguridad de la información.

A pesar de que se vienen trabajando en la seguridad y privacidad de la información de la Biblioteca y se tienen algunos productos y avances, y teniendo en cuenta los cambios estratégicos y de infraestructura que se vienen adelantando y los que se planear hacer en la vigencia 2025, se toma la decisión de implementar todo el modelo desde el inicio.

9. HOJA DE RUTA

FASE	DESCRIPCIÓN	ACTIVIDADES
0	Comité de Seguridad de la Información.	• Conformar el Comité de Seguridad de la Información mediante acto administrativo.
1	Planificación de la GRSD	• Definición del contexto interno, externo y de los procesos de la entidad pública. • Definición de la política de administración de riesgo. • Designación de roles y responsabilidades. • Definición de criterios de probabilidad, impacto y zonas de riesgo aceptable. • Identificación de activos de información. • Identificación de riesgos. • Valoración de riesgos. • Definición del tratamiento de los riesgos
2	Ejecución	• Implementación de los planes de tratamiento de riesgos definidos
3	Monitoreo y revisión	• Realizar seguimiento y monitoreo al plan de acción en la etapa de implementación y finalización de los planes de acción. • Revisar periódicamente las actividades de control para determinar su relevancia y actualizarlas de ser necesario. • Realizar monitoreo de los riesgos y controles tecnológicos. • Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad de la información para verificar su efectividad. • Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos. • Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles

FASE	DESCRIPCIÓN	ACTIVIDADES
4	Mejoramiento continuo de la gestión del riesgo de seguridad de la información	• Revisar y evaluar los hallazgos encontrados en las auditorías internas, otras auditorías e informes de los entes de control realizadas. • Establecer las posibles causas y consecuencias del hallazgo. • Determinar si existen otros hallazgos similares para establecer acciones correctivas y evitar así que se lleguen a materializar. • Emprender acciones de revisión continua, que permitan gestionar el riesgo a tiempo, disminuir el impacto y la probabilidad de ocurrencia del riesgo detectado, así como la aparición de nuevos riesgos que puedan afectar el desempeño de la entidad pública o de los servicios que presta al ciudadano.

10. MEDICIÓN Y SEGUIMIENTO

La verificación del cumplimiento del plan se realizará a través del indicador "Ejecución del Plan de Seguridad y Privacidad de la Información" asociado al proceso Telemática. De igual forma, el Oficial de seguridad de la información podrá realizar autoevaluaciones que consideren necesarias al Modelo de Seguridad y Privacidad de la Información implementado, para verificar el estado actual y realizar los ajustes pertinentes al plan de acción o por medio de los instrumentos de planes de mejoramiento definidos en la Entidad.

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