PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2024 -2027

COMISIÓN DE REGULACIÓN DE AGUA POTABLE Y SANEAMIENTO BÁSICO

CRA

Histórico de revisiones

FECHA	VERSIÓN	DESCRIPCIÓN	AUTOR
Noviembre - 2023	1.0	Plan de seguridad y privacidad de la información	Oficial de seguridad de la información.

Contenido

INTRODUCCIÓN

"En la era digital en constante evolución, la seguridad de la información se ha convertido en un desafío de vital importancia. En un mundo interconectado donde los datos fluyen libremente a través de redes globales, la protección de la información se ha vuelto más crucial que nunca. A medida que la tecnología avanza a pasos agigantados, surgen nuevos y complejos desafíos en el campo de la seguridad de la información. Desde la creciente amenaza de la inteligencia artificial maliciosa hasta la protección de datos en la computación cuántica, la seguridad de la información se encuentra en un constante estado de transformación.

La seguridad y privacidad de la información en las entidades buscan afrontar los retos que impone el negocio, la incursión de nuevas infraestructuras digitales modernas, robustas y seguras. Teniendo en cuenta el acelerado avance de las tecnologías de información y comunicaciones, genera preocupación e incertidumbre el manejo de los riesgos de la información que están asociados con las debilidades en la seguridad de las tecnologías de la información, vulnerabilidades que pueden afectar a los activos de información. Estas vulnerabilidades pueden surgir debido a una ciberseguridad inadecuada, lo que afecta la triada de la seguridad de la información: la disponibilidad, confidencialidad e integridad.

Para garantizar la seguridad de la información en las entidades públicas y privadas, es fundamental desarrollar capacidades que les permitan estar un paso adelante de las amenazas y vulnerabilidades latentes que a diario acechan a los activos de información, infraestructuras críticas y los usuarios, quienes desempeñan un papel clave en el ciberespacio.

Además, en el ámbito de la seguridad de la información, la casa de amenazas y las fuentes abiertas de investigación desempeñan un papel cada vez más importante. La casa de amenazas es una plataforma que permite a las organizaciones recopilar, analizar y compartir información sobre amenazas en tiempo real, lo que proporciona una ventaja crucial para la detección y respuesta proactiva a ataques cibernéticos.

Las fuentes abiertas de investigación, por otro lado, brindan a las entidades acceso a información valiosa y actualizada sobre vulnerabilidades, tácticas de ataque y amenazas emergentes. Esto facilita la toma de decisiones informadas y la implementación de estrategias efectivas de seguridad de la información.

En este contexto, la Comisión De Regulación De Agua Potable y Saneamiento Básico - CRA se ha comprometido a fortalecer la protección de los activos de información que respaldan sus procesos y apoyan la implementación del modelo de seguridad y privacidad de la información. Los objetivos de seguridad de la información de la Comisión incluyen fortalecer la cultura de seguridad y privacidad de la información entre su personal, identificar y clasificar los activos de información de acuerdo con requisitos legales y regulatorios,

gestionar los riesgos de seguridad y privacidad de la información, y gestionar eventos e incidentes de seguridad para preservar la integridad, confidencialidad, disponibilidad y privacidad de la información.

La Comisión reconoce la necesidad de actualizar su plan estratégico de seguridad y privacidad de la información para fortalecer las políticas de seguridad y gestionar eficazmente los posibles fallos en los procesos y la responsabilidad en el manejo de procedimientos. Esto ayudará a minimizar amenazas que puedan ser introducidas de manera accidental o intencional.

El proceso de tecnologías de la información propone abordar estos desafíos diseñando un plan estratégico de seguridad y privacidad de la información basado en estándares como ISO 27001, el Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), y directrices de Gobierno Digital. Esto fortalecerá las políticas de seguridad existentes, prevenir posibles pérdidas de información y fomentará la cultura de seguridad de la información entre los funcionarios.

El respaldo de la alta dirección es esencial para implementar con éxito el componente de seguridad y privacidad de la información y gestionar los riesgos de seguridad de la información en la entidad. Un plan estratégico de seguridad y privacidad de la información estructurado permitirá establecer iniciativas y proyectos que garanticen el cumplimiento del objetivo de proteger, asegurar y minimizar el daño que pueda afectar los activos de información de la entidad.

En línea con el Decreto 767 de 2022, la Comisión De Regulación De Agua Potable y Saneamiento Básico - CRA define la seguridad de la información como un principio fundamental de la Política de Gobierno Digital. Además, la entidad se ajusta al Decreto 612 de 2018 para actualizar su plan de implementación de seguridad y privacidad de la información, lo que garantiza que se cumplan los objetivos de seguridad en línea con las políticas gubernamentales y las mejores prácticas del sector.

1. OBJETIVO

Formular del Plan Estratégico de Seguridad y Privacidad de la Información 2024 -2027, el cual se enmarca en los siguientes objetivos:

• Definir los proyectos e iniciativas.

• Clasificar y priorizar los proyectos a realizar.

• Aprobar el Plan Estratégico de Seguridad y Privacidad de la Información

2. ALCANCE DEL DOCUMENTO

Este documento incorpora la definición estratégica de la Seguridad y Privacidad de la información del proceso de Tecnologías y Sistemas de Información, estableciendo el plan de implementación de los proyectos y servicios que se proponen ejecutar en las vigencias 2024 – 2027, definidos a través del plan de acción de la entidad para los diferentes ámbitos en el Modelo de Seguridad y Privacidad de la Información. Adicionalmente, como resultado de los ejercicios incorpora el plan de acción a través de la definición de la hoja de ruta. El documento describe las definiciones realizadas sobre la estrategia, objetivos, marco normativo, situación Actual, entendimiento estratégico, modelo de gestión y el respectivo el modelo de planeación definiendo el portafolio de proyectos y la hoja de ruta de implementación.

3. MARCO NORMATIVO

En el Plan Nacional de Desarrollo 2023-2026 (Ley 2294 de 2023), se define la transformación digital, como motor de oportunidades e igualdad para lo cual fortalecer el Gobierno Digital y aplicar el Marco de Referencia de Arquitectura Empresarial para el Estado permitirá avanzar en este propósito y mejorar la relación entre el Estado y el ciudadano, así como su calidad de vida de tal forma que lo acerque y solucione sus necesidades, a través del uso de datos y de tecnologías digitales.

Decreto 767 de 2022 "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". El presente capitulo establece lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual desde ahora debe ser entendida como: el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el objetivo de impactar positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del territorio nacional y la competitividad del país, promoviendo la generación de valor público a través de la transformación digital del Estado, de manera proactiva, confiable, articulada y colaborativa entre los grupos de Interés y permitir el ejercicio de los derechos de los usuarios del ciberespacio.

En el artículo 2.2.9.1.1.3 Principios, en este se encuentra: ***Confianza:*** *Los sujetos obligados propenderán por que la implementación de la Política de Gobierno Digital permita el equilibrio entre las expectativas ciudadanas y el funcionamiento de las instituciones públicas. De la misma forma, los sujetos obligados cumplirán con las disposiciones que permitan la garantía de la seguridad digital, la protección de datos, y la transparencia pública.* ***Resiliencia Tecnológica:*** *Los sujetos obligados a la aplicación de la presente Política tomarán acciones respecto de la prevención de riesgos que puedan afectar la seguridad digital y con ello propenderán por la disponibilidad de los activos, la recuperación y continuidad de la prestación del servicio ante interrupciones o incidentes.*

Como Habilitadores transversales de la Política de Gobierno Digital se encuentran elementos fundamentales como Arquitectura, Seguridad y Privacidad de la Información,

Cultura y Apropiación y Servicios Ciudadanos Digitales, que permiten el desarrollo y el logro de los propósitos de la Política de Gobierno Digital. La elaboración del Plan Estratégico de Seguridad y Privacidad de la Información se construirá siguiendo los principales marcos de referencia en materia de seguridad (ISO 27001, 27002, MSPI de Ministerio de tecnologías de información y comunicaciones) y lineamientos establecidos en Gobierno Digital y el modelo de arquitectura empresarial MRAV 3 para el dominio de seguridad de la información.

4. ANÁLISIS DE LA SITUACIÓN ACTUAL

En esta sección, se describe la situación actual de la seguridad y privacidad de la información de la entidad en relación con los dominios del modelo de Seguridad y Privacidad de la Información del MinTIC. Este análisis se alinea con las nuevas directrices de la Presidencia de la República de Colombia y las buenas prácticas de ciberseguridad y ciberdefensa. El propósito es obtener una comprensión clara de la línea base actual, desde la cual proyectar la visión de la gestión de seguridad de la información en la entidad.

Los resultados de cada análisis revelan el grado de cumplimiento del modelo, respaldado por un análisis cualitativo. Estos indicadores señalan las brechas existentes que deben cerrarse y que son fundamentales para la planificación del modelo, así como para su inclusión en el portafolio de proyectos. Todo esto se realiza considerando la cuantificación y los criterios de calidad definidos, en sintonía con el autodiagnóstico de los componentes de Gobierno Digital, especialmente en lo que respecta al componente habilitador de Seguridad y Privacidad de la Información.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	95	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	100	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	91	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	100	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	100	100	OPTIMIZADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	99	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	94	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	94	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	99	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	100	100	OPTIMIZADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	100	100	OPTIMIZADO
A.18	CUMPLIMIENTO	100	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		**98**	**100**	OPTIMIZADO

Tabla 1. Herramienta autodiagnóstico MSPI 2023 – CRA

5. CONSOLIDADO DE BRECHAS.

Análisis de Brechas en el presente capítulo se desarrolla lo siguiente:

a. Se toman las brechas identificadas por componente de Gobierno digital y el autodiagnóstico de MinTIC para el MSPI.
b. Se establecen actividades de cumplimiento para la vigencia 2024 - 2027
c. Se determinan las entregas de valor o productos.
d. Se establecen líneas base del dominio de gestión de seguridad MRAE V3 y directrices de gobierno nacional.

6. HOJA DE RUTA.

Presentamos la hoja de ruta elaborada a partir de brechas identificadas y agrupadas en paquetes de trabajo que buscan fortalecer las capacidades de la entidad. Se destacan las iniciativas relacionadas con la seguridad y privacidad de la información, las cuales están alineadas con el Plan Estratégico de Tecnologías de la Información. Estas iniciativas se derivan del diagnóstico realizado para evaluar el cumplimiento y nivel de madurez del modelo de seguridad y privacidad de la información.

Las acciones propuestas se enmarcan en los controles recomendados, orientados a establecer una arquitectura sólida de seguridad y privacidad de la información. Se incorporan soluciones tecnológicas y se siguen las últimas tendencias en seguridad de la información, manteniendo el progreso logrado en períodos anteriores.

ANEXO 1. HOJA DE RUTA SEGURIDAD DIGITAL Y DE LA INFORMACIÓN

No	Actividad	Responsable	Producto o resultado esperado	Presupuesto estimado 2024	Presupuesto estimado 2025	Presupuesto estimado 2026	Presupuesto estimado 2027	2024				2025				2026				2027			
								Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1. Activos de información																							
1.1	Actualización de Instrumentos de gestión de la información pública	Todos los procesos	Matriz de Activos de Información, Índice de Información Clasificada y Reservada	$ -	$ -	$ -	$ -				x				x				x				x
2. Riesgos de Seguridad y Privacidad de la Información																							
2.1	Actualización y análisis de Riesgos Seguridad de la información	Todos los procesos	Matriz de riesgos - digitales	$ -	$ -	$ -	$ -			x	x			x	x			x	x			x	x
2.2	Definición y/o actualización del Tratamiento de Riesgos Seguridad de la Información	Todos los procesos	Plan de Tratamiento de Riesgos de Seguridad de la Información								x				x				x				x
2.3	Actualización de la Declaración de Aplicabilidad - SOA	CISO	Documento con la declaración de aplicabilidad								x				x				x				x
2.4	Identificación de proyectos de apoyo de Ciberdefensa	CISO	Plan de adquisiciones relacion de proyectos de seguridad y Contratos de Seguridad Digital								x				x				x				x
3. Concienciación y Sensibilización en Seguridad y Privacidad de la Información																							
3.1	Actualización del Plan de comunicación, sensibilización y capacitación en seguridad Digital	CISO - Comunicaciones	Plan de comunicación, sensibilización y capacitación en seguridad Digital	$ -	$ -	$ -	$ -				x				x				x				x
3.2	Ejecución del Plan de comunicación, sensibilización y capacitación en seguridad Digital	CISO - Comunicaciones	Informe de ejecución.								x				x				x				x
3.3	Análisis de resultados del Plan de comunicación, sensibilización y capacitación en seguridad Digital	CISO	Informe de resultados del Plan de comunicación,sensibilización y capacitación en seguridad Digital								x				x				x				x
4. Protección de Datos Personales																							
4.1	Revisión y/o actualización de la Protección de Datos Personales (Habeas Data)	CISO - Comunicaciones	Politica de Protección de Datos Personales y/o Registro RNBD	$ -	$ -	$ -	$ -				x				x				x				x
4.2	Divulgación de la política protección de Datos Personales (Habeas Data)	CISO - Comunicaciones	Correo Electronico y/o Registro de asistencia								x				x				x				x
5. Sistema de Gestión de Seguridad de la Información																							
5.1	Revisión y/o actualización de la Política y Manual de Políticas de Seguridad y Privacidad de la información	CISO	Política y Manual de Seguridad de la Información.	Plan Anual de Adquisiciones - PAA	Plan Anual de Adquisiciones - PAA	Plan Anual de Adquisiciones - PAA	Plan Anual de Adquisiciones - PAA				x				x				x				x
5.2	Apoyar en la definición y/o actualización de la documentación asociada a Seguridad y Privacidad de la información	CISO	Documentos, procedimientos, guías, etc.								x				x				x				x
5.3	Socialización de políticas de seguridad de la información / Buenas practicas de seguridad	CISO	Registros de asistencias, Informes de resultado de las revisiones								x				x				x				x
5.4	Revisión y aprobación de documentos del SGSI por el comité SIGC	CISO -PTIC	Acta de Revisión aprobación documentos de seguridad por el comité SIGC								x				x				x				x
5.5	Gestionar auditoría interna al Sistema de Gestión de Seguridad de la Información	CISO -PTIC	Contrato prestación de servicios auditoria								x				x				x				x
5.6	Proyectos de seguridad información para apoyo a la gestión de Ciberseguridad y CiberInteligencia	CISO	Plan Anual de Adquisiciones - Seguridad Informática																				
6. Continuidad del Negocio																							
6.1	Revisar y actualizar del Plan de Continuidad y Disponibilidad de tecnología	CISO	Plan de Continuidad y Disponibilidad	$ -	$ -	$ -	$ -				x				x				x				x
7. Cumplimiento																							
7.1	Actualización de RNBD de la SIC	CISO	Certificado de actualización de base de datos RNBD	$ -	$ -	$ -	$ -		x				x					x				x		
7.2	Diligenciamiento del Autodiagnóstico de MSPI	CISO	Diligenciamiento herramienta de medición y autodiagnóstico del MSPI								x				x				x				x
7.3	Diligenciamiento del FURAG de seguridad digital o quien haga de sus veces.	CISO	Herramienta de medición de FURAG ámbito de seguridad digital o quien haga de sus veces.								x				x				x				x
7.4	Identificación y gestión de vulnerabilidades	CISO	Seguimiento a el cierre de brechas de vulnerabilidades								x				x				x				x
7.5	Gestión de Incidentes de seguridad	CISO	Reportes e informes de gestión de incidentes								x				x				x				x
7.6	Realizar Auditoria Interna al sistema de seguridad y privacidad de la información.	CISO Auditor Externo SGSI	Informe de auditoria de seguridad y privacidad de la información								x				x				x				x
7.7	Publicación de Instrumentos de gestión de la información pública	Gestión Documental	Registro de Activos de Información, Índice de Información Clasificada y Reservada								x				x				x				x
7.8	Analisis de la matriz de riesgos de seguridad digital	CISO	Informe seguimiento a los riesgos de seguridad digital institucionales							x	x				x			x	x			x	x
7.9	Ejecución de las pruebas definidas en el Plan de Continuidad y Disponibilidad de tecnología	PTIC	Informe de resultados de las pruebas realizadas								x				x				x				x
7.10	Seguimiento a la implementación de los planes de tratamiento	CISO	Matriz de seguimiento de los planes de tratamiento								x				x				x				x
7.11	Seguimiento al Plan de Acción Institucional - PAI - Seguridad de la Información	CISO	Matriz Plan de Acción Institucional - PAI - Seguridad de la Información.								x				x				x				x