CÁMARA DE REPRESENTANTES

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024.

OFICINA DE PLANEACIÓN Y SISTEMAS BOGOTÁ,
ENERO DE 2024

CONGRESO DE LA REPÚBLICA DE COLOMBIA
CÁMARA DE REPRESENTANTES

LA CÁMARA Se Transforma

CONTENIDO

1. INTRODUCCIÓN

El presente documento tiene como propósito presentar una hoja de ruta que permita el establecimiento, implementación, operación, monitoreo, revisión y mejora continua del *Sistema de Gestión de Seguridad y Privacidad de la Información* en la Cámara de Representantes.

De tal manera la Entidad se encuentra comprometida con la *Seguridad y Privacidad de la Información*, asignando los recursos necesarios para garantizar que los procesos se encuentren incluidos en el alcance de dichos sistemas, permitiéndole a la entidad dar cumplimiento a sus objetivos estratégicos.

2. OBJETIVO GENERAL

Establecer el *Plan de Seguridad y Privacidad de la Información* dentro del marco del Modelo de Seguridad y Privacidad de la Información (MSPI) en la Cámara de Representantes, a través de un mapa de ruta de proyectos estratégicos a tres (3) años para el establecimiento, implementación, operación, monitoreo, revisión y mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información en la Cámara de Representantes.

2.1 Objetivos Específicos

- Establecer un Sistema Actual en el marco del *Modelo de Seguridad y Privacidad de la Información MSPI*, establecido por un Autodiagnóstico de la Seguridad en la Cámara de Representantes.
- Presentar los proyectos a realizar como parte del PSPI, incluyendo descripción, alcance, prioridad, costo y tiempos aproximados.
- Presentar la alineación de los proyectos presentados con la estrategia de la Cámara de Representantes, mediante la asociación de los objetivos de seguridad y los planes de tratamiento de riesgos.

3. ALCANCE

Establecer las acciones transversales en Seguridad de la Información a todos los procesos y trazar una *hoja de ruta* para proteger la información, garantizando la Confidencialidad, Disponibilidad e Integridad de la Información en la Cámara de Representantes.

4. AUTODIAGNÓSTICO AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MSPI EN LA CAMARA DE REPRESENTANTES

4.1 Estado Actual de la Seguridad de la Información

Para el análisis de la situación actual de la Seguridad de la Información en la Corporación se emplearon los criterios establecidos en la herramienta de diagnóstico establecida por el Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC.

En el siguiente cuadro vemos el resultado de la evaluación de efectividad de controles – ISO 27001: 2013 ANEXO A en la Entidad.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	60	100	EFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	25	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	50	100	EFECTIVO
A.8	GESTIÓN DE ACTIVOS	25	100	REPETIBLE
A.9	CONTROL DE ACCESO	50	100	EFECTIVO
A.10	CRIPTOGRAFÍA	100	100	OPTIMIZADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	75	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	56	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	77	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	85	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	52	100	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	68	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	45	100	EFECTIVO
A.18	CUMPLIMIENTO	50	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		**58**	**100**	EFECTIVO

Fuente: Herramienta autodiagnóstico de MinTIC.

Teniendo en cuenta el análisis de la herramienta de diagnóstico, la Seguridad de la Información en cuanto a nivel de madures PHVA de la entidad, muestra un promedio de evaluación de controles de efectividad con una calificación de:

- 58%, NO ALCANZA AL NIVEL INICIAL (*ver instructivo de evaluación MSPI) documento anexo.

NIVEL	¿CUMPLE?
OPTIMIZADO	FALSO
GESTIONADO CUANTITATIVAMENTE	FALSO
DEFINIDO	FALSO
Nivel de madurez alcanzado	NO ALCANZA NIVEL INICIAL

Lo anterior significa en el punto 1 que se requiere con urgencia implementar el *Sistema de Gestión de Seguridad y Privacidad de la Información*, revisar los procesos y procedimientos del área TIC, crear las nuevas Políticas de Seguridad de la Información, sensibilizar a los usuarios de la Cámara de Representantes en las Políticas de Seguridad de la Información, implementar el Dominio de Uso y Apropiación de Arquitectura Empresarial.

Fuente: Herramienta Autodiagnóstico de MinTIC.

En el grafico anterior **BRECHA ANEXO A ISO 27001:2013,** podemos evidenciar lo expuesto anteriormente, el comportamiento de los Dominios del MSPI. La imagen evidencia el comportamiento y la madurez del MSPI en la Cámara de Representantes, lo que obedece a implementar un Plan de Mejoramiento de la Seguridad de la Información en la Entidad.

4.2 Nivel de Madurez de Seguridad de la Información

		NIVEL DE CUMPLIMIENTO
NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Inicial	Suficiente
	Repetible	Suficiente
	Definido	Suficiente
	Administrado	Suficiente
	Optimizado	Suficiente

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

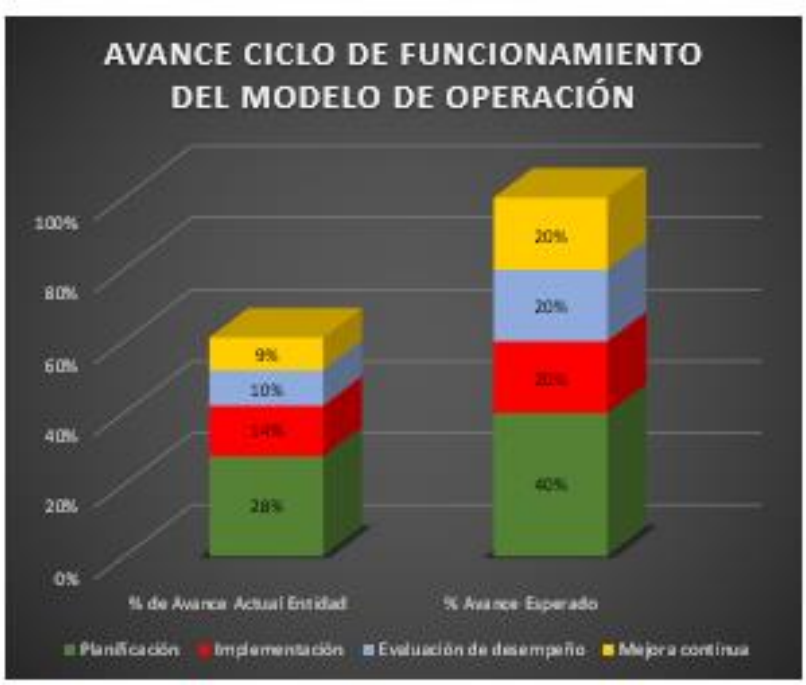
TOTAL, DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

Teniendo en cuenta el nivel donde la Cámara de Representantes se encuentra se evidencia que NO ALCANZA AL NIVEL INICIAL, en cuanto a EFECTIVIDAD DE CONTROLES con un 56% y en 57% de Avance PHVA Actual de la Entidad con respecto al avance del 100% esperado, tenemos que concluir que la Entidad debe de fortalecer los componentes de: *Implementación, Evaluación de Desempeño y Mejora*

Continua en Seguridad de la Información para permitir acercarnos más al avance esperado, como se muestra en la tabla y grafico siguientes:

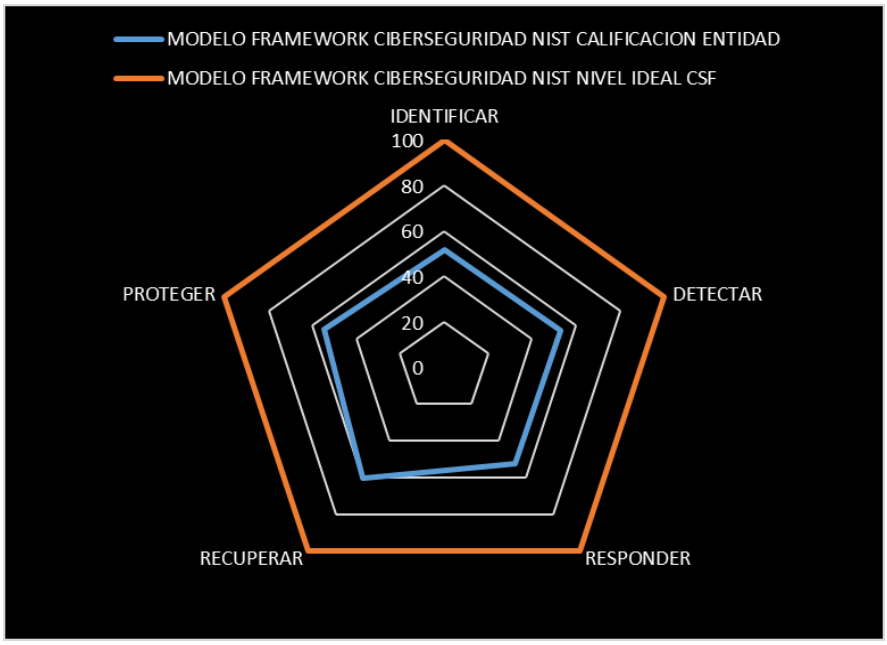
AVANCE PHVA		
COMPONENTE	**% de Avance Actual Entidad**	**% Avance Esperado**
Planificación	28%	40%
Implementación	14%	20%
Evaluación de desempeño	10%	20%
Mejora continua	9%	20%
TOTAL	**61%**	**100%**

Fuente: Herramienta autodiagnóstico de MinTIC.



Fuente: Herramienta autodiagnóstico de MinTIC

4.3 Ciberseguridad



4.4 Conclusiones y Recomendaciones

A partir de la fase de diagnóstico, determinada por la herramienta, podemos concluir que el estado actual de seguridad de la información en el área de TI necesita de un Plan de Seguridad Estratégico por parte de la Oficina de Planeación y Sistemas de la Entidad y contar con el apoyo de la alta Dirección de la Cámara de Representantes, sobre la importancia de proteger los activos de información.

Se debe seguir en la misma línea de acción del fortalecimiento, seguimiento y mejora continua de los controles de la norma ISO 27001:2013 en la Entidad; además de implementar la Ciberseguridad en la Entidad.

Por otra parte, los funcionarios, contratistas y colaboradores deben seguir comprometidos con el cumplimiento, conocimiento de las Políticas de Seguridad de la Información de la Entidad.

La OPS seguirá atenta a seguir con la sensibilización de todos los actores en la Corporación y estar atentos a las auditorías internas y externas por los Entes de Control manteniendo las evidencias del tratamiento de los controles para seguir manteniendo los niveles de cumplimiento satisfactorios del MSPI y que estén alineados con los objetivos misionales de la entidad.

El *Comité de Seguridad de la Información* se deberá crear, para establecer los roles y responsabilidades de seguridad y privacidad de la información el cual estará atento de las mejoras del modelo, propendiendo que los *Activos de Información* se encuentren actualizados y seguros.

Por último, el tratamiento de los riesgos de Seguridad de la Información debe gestionarse periódicamente para reducir las vulnerabilidades en la Entidad.

5. PLAN DE RUTA DE PROYECTOS PARA MITIGAR LAS BRECHAS DE SEGURIDAD EN LA CÁMARA DE REPRESENTANTES

Los planes estratégicos para el Sistema de Gestión de Seguridad y Privacidad de la Información en la Cámara de Representantes, se desarrollan con base en los siguientes lineamientos:

- Informe de análisis de brechas ISO 27001.
- Política de Protección de Datos Personales.
- Diagnóstico mediante el Instrumento de evaluación de MSPI.
- Análisis de vulnerabilidades a la infraestructura de la Organización.
- Plan de Tratamiento de Riesgos Digitales.
- 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.

La ejecución de este plan se proyecta realizar entre los años 2023 y 2024, de acuerdo con su prioridad (basada en la cantidad de riesgos que trata) y a las buenas prácticas de seguridad de la información.

A continuación, se presentan 16 proyectos estratégicos para tener en cuenta en el mapa de ruta de la Corporación en Seguridad de la Información.

5.1 Proyectos Estratégicos en Seguridad de la Información para la Cámara de Representantes

Nombre	Sistema de Gestión de Seguridad de la Información
Prioridad	1
Descripción	Implementación del SGSI mediante una serie de actividades solicitadas por la norma ISO 27001 y el MSPI.

Alcance	• Acompañamiento en la implementación de políticas, procedimientos y controles. • Seguimiento en la implementación de planes de tratamiento de riesgos. • Seguimiento a la ejecución del PSPI. • Acompañamiento en la implementación de los planes de cierre de brechas. • Diseño, desarrollo y ejecución del plan implementación del plan de capacitación y sensibilización (incluye capacitación a responsables de riesgos). • Medición de indicadores y definición de acciones correctivas • Participación en los comités de seguridad y privacidad • Actualización de inventario de activos de información y bases dedatos personales • Ejecución y actualización del análisis de riesgos y planes de tratamiento • Ejecución de auditoría y seguimiento al cierre de los hallazgos de auditoríasanteriores • Pruebas semestrales de ejecución de análisis de vulnerabilidades y Ethical hacking • Actualización anual de la documentación del sistema de gestión de seguridad de acuerdo con lo solicitado por la norma • Acompañamiento en la revisión gerencial del sistema y definición de acciones de mejora • Medición del nivel de madurez del sistema • Definición de proyectos de fortalecimiento del SGSI • Auditoría de cumplimiento de la ley 1581 de 2012 y protección de datos personales, desde la perspectiva de responsabilidad demostrada
Costo aproximado	$ 2.500.000.000

Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Aplicar un proceso de gestión de riesgos de seguridad de la información y bases de datos personales, mediante la ejecución de medidas apropiadas con el fin de identificar, analizar, evaluar, tratar y mitigar los riesgos y así reducir el impacto potencial a niveles aceptables sobre los riesgos asociados con la pérdida de la confidencialidad, de integridad y de disponibilidad. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información. • Disponer de medidas para atender oportunamente eventos de seguridad de la información con el fin de disminuir los impactos negativos ocasionados por los incidentes de Seguridad de la Información, que se puedan llegar a presentar en la Entidad. • Establecer las acciones necesarias, para asegurar la mejora continua del Sistema de Seguridad de la Información y Protección de Datos Personales. • Fortalecer la cultura de seguridad de la información en la Entidad, a través de la gestión del conocimiento de seguridad de la información.
Planes de Tratamiento de Riesgo Relacionados	Ver detalle de estos planes en el documento *Matriz de Riesgos Digital*.
Tiempo estimado de ejecución	12 meses

Nombre	Implementación de Prevención de Fuga de Información (DLP)
Prioridad	2
Descripción	Implementación de una solución que permita monitorear la fuga o extracción de información sensible en la Cámara de Representantes
Alcance	Contratar un tercero especializado que permita lograr el monitoreo y/o bloqueo de salida de información en la Cámara de Representantes a través de:
	Puertos USB Correo electrónico

	Servicios de red (Internet, red local) El tercero debe garantizar: Dimensionamiento de la solución Implementación operación y soporte
Costo aproximado	$ 200.000.000
Objetivos de Seguridad Relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información. • Disponer de medidas para atender oportunamente eventos de seguridad de la información con el fin de disminuir los impactos negativos ocasionados por los incidentes de Seguridad de la Información, que se puedan llegar a presentar en la Entidad. • Adopción de Responsabilidad Demostrada con el fin de reducir la Probabilidad de violación de la privacidad de los datos personales en de la Entidad.
Planes de Tratamiento de Riesgos Relacionados	• Riesgo 16 (R16) • Riesgo 25 (R25) • Riesgo 48 (R48) Ver detalle de estos planes en el documento *Matriz de Riesgos Corrupción, Digital y Gestión 2023*.
Tiempo estimado de ejecución	Anual, permanente.

Nombre	Aseguramiento de la Plataforma Tecnológica y Remediación de Vulnerabilidades
Prioridad	3
Descripción	Servicio de aseguramiento y remediación de las vulnerabilidades identificadas en los escaneos periódicos y en los informes de hacking ético.

Alcance	• Desarrollo de guías de aseguramiento y procedimientos de remediación de vulnerabilidades para todo el software base de la Cámara de Representantes, entre ellos: sistemas operativos, dispositivos de red, soluciones de seguridad, motores de bases de datos y servidores WEB. • Aplicación de las guías de aseguramiento y remediación de vulnerabilidades en ambientes pre productivos (desarrollo, pruebas, calidad, entrenamiento, etc.) • Registro en CMDB, apoyo en gestión de cambios, gestión de relación interna, casos de prueba, ejecución de pruebas funcionales mínimas, cierre de cambio. • Aplicación de las guías de aseguramiento y remediación de vulnerabilidades en ambientes productivos. • Verificación de cumplimiento de las guías de aseguramiento definidas.
Costo aproximado	$ 300.000.000
Objetivos de Seguridad Relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas
	• Internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos enla declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información.
Planes de Tratamiento de Riesgos Relacionados	• Riesgo 16 (R16) • Riesgo 25 (R25) • Riesgo 48 (R48) Ver detalle de estos planes en el documento *Matriz de Riesgos Corrupción, Digital y Gestión 2023*.
Tiempo estimado de Ejecución	Anual, permanente

Nombre	Servicio SOC o CSIRT para la Gestión de Incidentes de Seguridad y Ciberseguridad 7x24
Prioridad	4
Descripción	Proyecto orientado a lograr un monitoreo permanente y gestión de incidentes de seguridad de la información y Ciberseguridad

Alcance	Contratar un servicio de SOC/CSIRT que permita lograr: • Implementación de una solución de análisis y correlación de eventos • Habilitación de la auditoría en los diferentes sistemas de informacióny dispositivos • Identificación de eventos anómalos deseguridad • Monitoreo de modificación de archivos sensibles • Servicio de caza de amenazas de Ciberseguridad o CTH (Cyber Threat Hunting) • Servicio de inteligencia de amenazas de Ciberseguridad o CTI (Cyber Threat Intelligence) • Ejecución de simulacros de ocurrencia de incidentes de seguridady respuesta • Generación de alertas tempranas para riesgos emergentes (vulnerabilidades de día cero, nuevos ataques, nuevas amenazas, entre otros) • Identificación de lecciones aprendidas y oportunidades de mejora
Costo aproximado	$ 400.000.000
Objetivos de Seguridad Relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información. • Disponer de medidas para atender oportunamente eventos de seguridad de la información con el fin de disminuir los impactos negativos ocasionados por los incidentes de Seguridad de la Información, que se puedan llegar a presentar en la Entidad. • Adopción de Responsabilidad Demostrada con el fin de reducir la probabilidad de violación de la privacidad de los datos personales en de la Entidad. • Fortalecer la cultura de seguridad de la información en la Entidad, a través de la gestión del conocimiento de seguridad de la información.
Planes de Tratamiento de Riesgos Relacionados	• Riesgo 16 (R16) • Riesgo 25 (R25) • Riesgo 48 (R48) Ver detalle de estos planes en el documento *Matriz de Riesgos Corrupción, Digital y Gestión 2023*.
Tiempo estimado de Ejecución	Anual, permanente.

Nombre	Plan de Continuidad del Negocio y Redundancias
Prioridad	5
Descripción	Diseño, implementación y pruebas periódicas a un plan de continuidad de negocio, en el que contemplen la Cámara de Representantes Instalaciones físicas, procesos de negocio y la plataforma tecnológica de la Cámara de Representantes
Alcance	Contratar un tercero especializado que permita lograr: • Diagnóstico de cumplimiento del estándar ISO 22301 • Análisis de Impacto al Negocio (BIA) • Análisis de riesgo de continuidad del negocio • Definición de estrategias de recuperación • Desarrollo de planes de continuidad del negocio (BCP) • Desarrollo de planes de recuperación de desastres (DRP) • Acompañamiento en la implementación de los planes • Diseño de plan de pruebas • Acompañamiento en la ejecución de pruebas • Informe de pruebas y oportunidades de mejora
Costo aproximado	$ 300.000.000
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Aplicar un proceso de gestión de riesgos de seguridad de la información y bases de datos personales, mediante la ejecución de medidas apropiadas con el fin de identificar, analizar, evaluar, tratar y mitigar los riesgos y así reducir el impacto potencial a niveles aceptables sobre los riesgos asociados con la pérdida de la confidencialidad, de integridad y de disponibilidad. • Disponer de medidas para atender oportunamente eventos de seguridad de la información con el fin de disminuir los impactos negativos ocasionados por los incidentes de Seguridad de la Información, que se puedan llegar a presentar en la Entidad.
Planes de Tratamiento de Riesgo Relacionados	Ver detalle de estos planes en el documento *Matriz de Riesgos Corrupción, Digital y Gestión 2023*.
Tiempo estimado de ejecución	6 meses.

Nombre	Fortalecimiento de la Seguridad Física y Ambiental de la CAMARA DE REPRESENTANTES
Prioridad	6

Descripción	Implementación de controles orientados a mejorar la seguridad física y ambiental (centro de datos), mitigando así los riesgos relacionados.
Alcance	• Acompañamiento a los visitantes por parte del responsable de la CAMARA DE REPRESENTANTES • Verificación periódica de las condiciones ambientales de archivos físicos por parte de referentes de proceso, estableciendo planes de acción si es requerido. • Revisión periódica del cableado eléctrico y estructurado, estableciendo planes de acción si es requerido. • Auditoría externa semestral de los controles de seguridad física y análisis de riesgos
Costo aproximado	$ 20.000.000 más IVA por la auditoria externa
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Aplicar un proceso de gestión de riesgos de seguridad de la información y bases de datos personales, mediante la ejecución de medidas apropiadas con el fin de identificar, analizar, evaluar, tratar y mitigar los riesgos y así reducir el impacto potencial a niveles aceptables sobre los riesgos asociados con la pérdida de la confidencialidad, de integridad y de disponibilidad. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información.
Planes de tratamiento de Riesgo Relacionados	Ver detalle de estos planes en el documento *Matriz de Riesgos, Corrupción Digital y Gestión 2023*.
Tiempo estimado de ejecución	Anual, periódico.

Nombre	Cifrado de portátiles, dispositivos móviles y dispositivos de almacenamiento externo
Prioridad	7
Descripción	Proteger la información sensible almacenada en portátiles, dispositivos móviles y dispositivos de almacenamiento externo cuando se presente pérdida o robo de estos, mediante la implementación de una solución de cifrado.

Alcance	La solución puede ser libre o adquirida, sin embargo, debe contemplar la protección de los siguientes elementos: • Cifrado de portátiles • Cifrado de dispositivos móviles (teléfonos corporativos, PDA, etc.) • Cifrado de dispositivos de almacenamiento (USB, discos durosexternos, memorias SD, etc.)
Costo aproximado	Sin costo si se selecciona libre.
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información.
Planes de Tratamiento de Riesgo Relacionados	Ver detalle de estos planes en el documento *Matriz de Riesgos Corrupción, Digital y Gestión 2023*.
Tiempo estimado de ejecución	6 meses

Nombre	Implementación de un proceso de desarrollo seguro
Prioridad	8
Descripción	Garantizar aplicaciones WEB seguras mediante la implementación de un proceso de desarrollo que contemple seguridad a lo largo del ciclo.
Alcance	• Curso de desarrollo y codificación segura para 5 integrantes del área OTIC • Definición de guías de codificación segura • Acompañamiento en la implementación de la metodología de desarrollo seguro y las guías
Costo aproximado	$ 50.000.000

Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información. • Fortalecer la cultura de seguridad de la información en la Entidad, a través de la gestión del conocimiento de seguridad de la información.
Planes de Tratamiento de Riesgo Relacionados	Ver detalle de estos planes en el documento *Matriz de Riesgos Corrupción, Digital y Gestión 2023*.
Tiempo estimado de ejecución	3 meses

Nombre	Diseño de Arquitectura de Seguridad Informática
Prioridad	9
Descripción	Proyecto orientado a obtener un diseño de ingeniería que permita fortalecer la seguridad informática de la Cámara de Representantes
Alcance	Contratar un tercero especialista en diseño de arquitecturas de seguridad informática que permita: • Identificar el estado actual de la arquitectura • Diseñar y planificar las soluciones de seguridad informática necesarias, teniendo en cuenta los análisis de riesgos
	• Proponer un plan de adquisición e implementación para las soluciones que sea necesario contratar y/o reemplazar, si fuera el caso.
Costo aproximado	$ 80.000.000
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información.

Planes de Tratamiento de Riesgo Relacionados	Ver detalle de estos planes en el documento *Matriz de Riesgos Corrupción, Digital y Gestión 2023*.
Tiempo estimado de ejecución	2 meses.

Nombre	Implementación de una Solución IDS/IPS
Prioridad	10
Descripción	Implementación de una solución de detección y prevención de intrusos en las redes de la Cámara de Representantes.
Alcance	Contratar un tercero para implementar y operar una solución IDS/IPS que permita detectar y/o prevenir intrusiones. La solución debe contar con al menos las siguientes características: • Actualización permanente de firmas • Creación de reglas y excepciones • Integración con SIEM • Generación de alertas • Generación de informes personalizados • Soporte del troughput de LA CAMARA DE REPRESENTANTES actual y proyectado
Costo aproximado	$ 60.045.000 más IVA
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información. • Disponer de medidas para atender oportunamente eventos de seguridad de la información con el fin de disminuir los impactos negativos ocasionados por los incidentes de Seguridad de la Información, que se puedan llegar a presentar en la Entidad.
Planes de Tratamiento de Riesgo Relacionados	Ver detalle de estos planes en el documento *Matriz de Riesgos Corrupción, Digital y Gestión 2023*.
Tiempo estimado de ejecución	Anual, permanente.

Nombre	Borrado y Destrucción Segura de Información
Prioridad	11

Descripción	Garantizar una eliminación segura de la información digital e impresa, cuando se tiene la certeza de que ya no se necesita.
Alcance	• Adquisición de 20 destructoras de papel • La Cámara de Representantes, permitirá la instalación de una solución de borrado seguro (puede ser libre) que cumpla con el estándar DOD5220.22
Costo aproximado	$ 20.000.000
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información.
Planes de Tratamiento de Riesgo Relacionados	Ver detalle de estos planes en el documento *Matriz de Riesgos Corrupción, Digital y Gestión 2023*.
Tiempo estimado de ejecución	3 meses

Nombre	Fortalecimiento de la Seguridad de la Red
Prioridad	12
Descripción	Incrementar la seguridad de la red para evitar incidentes de seguridad de la información.
Alcance	• Creación de una lista blanca de las extensiones (por ejemplo PDF, DOCX, XLSX, PPTX, etc.) permitidas para descarga en el LA CAMARA DE REPRESENTANTES, garantizando que se bloqueen archivos con extensiones de tipo ejecutables, librerías, imágenes ISO, en el firewall, con el fin de prevenir la descarga de malware en equipos del LA CAMARA DE REPRESENTANTES. • Cifrado de canales de comunicación o implementación de VPN • Contratación de un tercero experto en diseño de redes seguras, permitiendo: ○ Lograr una segmentación de red adecuada ○ Revisar las políticas a nivel de firewall ○ Crear listas de control de acceso • Renovación o implementación de los certificados digitales para protección de las comunicaciones de las aplicaciones WEB, considerando la compra de un certificado wildcard (p.ej *.ing.gov.co) que permita proteger todos los subdominios del dominio principal de LA CAMARA DE REPRESENTANTES.
Costo aproximado	$ 30.000.000 de consultoría de red segura más $ 10.000.000 certificado wildcard

Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información.
Planes de Tratamiento de Riesgo Relacionados	Ver detalle de estos planes en el documento *Matriz de Riesgos Corrupción, Digital y Gestión 2023*.

Nombre	Seguridad de la Información como parte de la Arquitectura Empresarial
Prioridad	13
Descripción	Incluir la seguridad de la información en el proyecto de Arquitectura Empresarial.
Alcance	• Definición de requerimientos de seguridad de la información • Definición de requerimientos de ciberseguridad • Apoyo en actividades de diagnóstico y proyección (AS-IS / TO-BE)
Costo aproximado	Directo ninguno, indirecto el tiempo del Oficial de Seguridad para atender la consultoría.
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Adopción de Responsabilidad Demostrada con el fin de reducir la probabilidad de violación de la privacidad de los datos personales en de la Entidad. • Establecer las acciones necesarias, para asegurar la mejora continua del Sistema de Seguridad de la Información y Protección de Datos Personales. • Fortalecer la cultura de seguridad de la información en la Entidad, a través de la gestión del conocimiento de seguridad de la información.
Planes de tratamiento de riesgo relacionados	Ver detalle de estos planes en el documento *Matriz de Riesgos Corrupción, Digital y Gestión 2023*.
Tiempo estimado de ejecución	Según programación del proyecto de arquitectura empresarial de la Cámara de Representantes.

Nombre	Protección de amenazas avanzadas para correo electrónico
Prioridad	14
Descripción	Incrementar la protección de los buzones de correo electrónico mediante la implementación de una solución de prevención de amenazas avanzadas.
Alcance	La solución debe garantizar protección contra al menos las siguientes amenazas: • APT • Spear Phishing • Ransomware • Scam
Costo aproximado	$ 20.000.000
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información. • Disponer de medidas para atender oportunamente eventos de seguridad de la información con el fin de disminuir los impactos negativos ocasionados por los incidentes de Seguridad de la Información, que se puedan llegar a presentar en la Entidad.
Planes de tratamiento de riesgo relacionados	Ver detalle de estos planes en el documento *Matriz de Riesgos Corrupción, Digital y Gestión 2023*.
Tiempo estimado de ejecución	Anual, permanente.

Nombre	Implementación de una solución Web Application Firewall (WAF)
Prioridad	15
Descripción	Incrementar la protección de las aplicaciones WEB de LA CAMARA DE REPRESENTANTES antes ataques web bien conocidos, a través de una solución especializada para tal fin.

Alcance	Contratar un tercero para implementar y operar una solución WAF. La solución debe contar con al menos las siguientes características: • Actualización permanente de firmas • Creación de reglas y excepciones • Integración con SIEM • Generación de alertas • Generación de informes personalizados • Soporte del troughput y cantidad de eventos por segundo en la red de la Cámara de Representantes
Costo aproximado	$ 250.000.000
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información. • Disponer de medidas para atender oportunamente eventos de seguridad de la información con el fin de disminuir los impactos negativos ocasionados por los incidentes de Seguridad de la Información, que se puedan llegar a presentar en la Entidad.
Planes de tratamiento de riesgo relacionados	Ver detalle de estos planes en el documento *Matriz de Riesgos Corrupción, Digital y Gestión 2023*.
Tiempo estimado de ejecución	Anual, permanente.

Nombre	Implementación de una solución Data Base Firewall (DBFW)
Prioridad	16
Descripción	Incrementar la protección de las bases de datos de la Cámara de Representantes antes ataques comunes que afectan estas tecnologías, a través de una solución especializada para tal fin.

Alcance	Contratar un tercero para implementar y operar una solución DBFW. La solución debe contar con al menos las siguientes características: • Actualización permanente de firmas • Creación de reglas y excepciones • Integración con SIEM • Generación de alertas • Generación de informes personalizados • Soporte del troughput y cantidad de eventos por segundo en la red de la Cámara de Representantes
Costo aproximado	$ 350.000.000
Objetivos de seguridad relacionados	• Proteger, preservar y administrar los activos de información, las bases de datos personales y las tecnologías utilizadas para su procesamiento, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, la integridad y disponibilidad, de manera coordinada con las partes involucradas. • Implementar, operar y revisar periódicamente los controles establecidos en la declaración de aplicabilidad, para la prevención y mitigación de los riesgos de seguridad de la información. • Disponer de medidas para atender oportunamente eventos de seguridad de la información con el fin de disminuir los impactos negativos ocasionados por los incidentes de Seguridad de la Información, que se puedan llegar a presentar en la Entidad.
Tiempo estimado de ejecución	Anual, permanente.

Programación 2023 - 2024

A continuación, se propone la programación de la ejecución de los proyectos a 2 años:

No.	Proyecto	2023												2024											
		ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
1	Gestión de Seguridad de la Información																								
2	Implementación de Prevención de Fuga de Información (DLP)																								
3	Aseguramiento de la plataforma tecnológica y remediación de vulnerabilidades																								
4	Servicio SOC o CSIRT para la gestión de incidentes de seguridad y ciberseguridad 7x24																								
5	Plan de continuidad del negocio y redundancias																								
6	Fortalecimiento de la seguridad física y ambiental del la Cámara de Representantes																								
7	Cifrado de portátiles, dispositivos móviles y dispositivos de almacenamiento externo																								
8	Implementación de un proceso de desarrollo seguro																								
9	Diseño de arquitectura de seguridad informática																								
10	Implementación de una solución IDS/IPS																								
11	Borrado y destrucción segura de información																								
12	Fortalecimiento de la seguridad de la red																								
13	Seguridad de la información como parte de la Arquitectura Empresarial																								
14	Protección de amenazas avanzadas para correo electrónico																								
15	Implementación de una solución Web Application Firewall (WAF)																								
16	Implementación de una solución Data Base Firewall																								

	(DBFW)																						

Como se ve en la tabla anterior, algunos proyectos se convierten en operación periódica y/o permanente.

5.2 Actualización del Plan de Seguridad y Privacidad de la Información

Este plan estratégico se podrá actualizar dependiendo de la ocurrencia de los siguientes hechos:
Cambios en la estrategia general de la Cámara de Representantes, Cambios significativos en la infraestructura tecnológica de la Entidad e Incidentes de seguridad de la información o ciberseguridad con impacto muy alto.
Cabe recordar que las modificaciones al plan deberán ser autorizadas por el Comité de Seguridad de la Información de la Cámara de Representantes.

6 BIBLIOGRAFÍA

- DAFP. (2018). Guía para la Gestión del Riesgo y Diseño de Controles, en entidades públicas.
- Ministerio de las Tecnologías de Información y Comunicaciones (1 de abril de 2016).
- Guía 7 - Guía de Gestión de Riesgos. Bogotá, Colombia. http://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

7 CONTROL DE CAMBIOS

REVISIONES DEL DOCUMENTO				
Versión	Fecha	Proyectado por	Descripción	Aprobado por
1.0	20/10/2021	Ing. Carlos Manuel Gómez Damián	Creación del Documento	**Oficina de Planeación y Sistemas** Dr. Juan José Gómez Vélez – Jefe OPS Revisión Técnica: Ing. Alejandro Muñoz Sandoval Aprobado en el Comité Institucional de Gestión y Desempeño, mediante Acta No. 3 del 16 de Diciembre de 2021.
2.0	15/12/2022	Oficina de Planeación y Sistemas	Ajustes al documento	**Oficina de Planeación y Sistemas** Dr. Andrés Francisco Lozano Campos – Jefe OPS Revisión y ajustes: Ing. Alejandro Muñoz Sandoval Aprobado en el Comité Institucional de Gestión y Desempeño, mediante Acta No. 01 del 31 de Enero de 2023.

3.0	**24/01/2024**	Oficina de Planeación y Sistemas	Ajustes al documento	**Oficina de Planeación y Sistemas** Dr. Jorge Edison Castro – Jefe (E) OPS Revisión y ajustes: Ing. Daniela Andrade Muñoz Juan David Acosta Jiménez Aprobado en el Comité Institucional de Gestión y Desempeño, mediante Acta No. 01 del 31 de Enero de 2024.