CÁMARA DE REPRESENTANTES

DECLARACIÓN DE APLICABILIDAD (SoA)

Seguridad y Privacidad de la Información

OFICINA DE PLANEACIÓN Y SISTEMAS
BOGOTÁ

CONGRESO DE LA REPÚBLICA DE COLOMBIA
CÁMARA DE REPRESENTANTES

LA CÁMARA Se Transforma

TABLA DE CONTENIDO

1. OBJETIVO

Documentar la Declaración de Aplicabilidad (SoA) del Sistema de Gestión de Seguridad de la Información (SGSI) de la Cámara de Representantes de Colombia, estableciendo los controles aplicables del Anexo A de la norma NTC ISO/IEC 27001:2022, su estado de implementación y la justificación de inclusión o exclusión de cada uno, en alineación con el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio TIC (Resolución 02277 de 2025) y con la Política General de Seguridad y Privacidad de la Información de la entidad.

2. ALCANCE

La presente Declaración de Aplicabilidad abarca la totalidad de los 93 controles del Anexo A de la NTC ISO/IEC 27001:2022, agrupados en sus cuatro dominios: controles organizacionales (A.5), controles de personas (A.6), controles físicos (A.7) y controles tecnológicos (A.8).

Aplica a todos los procesos, sistemas de información, infraestructura tecnológica, activos de información, funcionarios, contratistas, proveedores y terceros que accedan, procesen, transmitan o almacenen información institucional de la Cámara de Representantes.

Para cada control se identifica el lineamiento o documento institucional asociado (políticas específicas PA01 a PA32 del Manual de Políticas de Seguridad y Privacidad de la Información), el estado de implementación y, cuando corresponde, la justificación de exclusión.

3. RESPONSABLES

La responsabilidad sobre la implementación, el mantenimiento y la mejora continua de los controles definidos en esta Declaración de Aplicabilidad se distribuye de la siguiente manera:

Rol	Responsabilidad
Comité Institucional de Gestión y Desempeño	Aprobar la Declaración de Aplicabilidad y sus actualizaciones; orientar y hacer seguimiento al SGSI.
Jefe de la Oficina de Planeación y Sistemas	Liderar la elaboración, revisión y actualización de la SoA; asegurar la articulación con el MSPI y la NTC ISO/IEC 27001:2022.
Oficial de Seguridad de la Información	Coordinar la implementación de los controles aplicables; mantener actualizada la SoA; reportar el estado de avance al Comité.

Líderes de procesos y dueños de activos	Implementar los controles dentro de su ámbito; aportar evidencias de cumplimiento; reportar incidentes y necesidades de ajuste.

4. DEFINICIONES

Activo de información: Elemento que tiene valor para la entidad y requiere protección.
Fuente: NTC ISO/IEC 27000:2022.

Anexo A: Conjunto de controles de referencia para el tratamiento de riesgos de seguridad de la información definidos en la NTC ISO/IEC 27001:2022.
Fuente: NTC ISO/IEC 27001:2022.

Confidencialidad: Propiedad de la información de no estar disponible ni ser divulgada a personas, entidades o procesos no autorizados.
Fuente: NTC ISO/IEC 27000:2022.

Control de seguridad de la información: Medida administrativa, técnica, física o procedimental implementada para tratar riesgos de seguridad de la información.
Fuente: NTC ISO/IEC 27000:2022.

Declaración de Aplicabilidad (SoA): Documento que contiene los controles aplicables del SGSI, su estado de implementación y la justificación de inclusión o exclusión.
Fuente: NTC ISO/IEC 27001:2022, cláusula 6.1.3 d).

Disponibilidad: Propiedad de que la información sea accesible y utilizable cuando sea requerida por un usuario autorizado.
Fuente: NTC ISO/IEC 27000:2022.

Estado del control: Clasificación utilizada para identificar la situación del control dentro del SGSI:

- (I) Implementado.
- (C) En curso.
- (E) Excluido.

  Fuente: Definición institucional.

Exclusión de control: Determinación documentada mediante la cual un control del Anexo A no aplica al alcance del SGSI.
Fuente: NTC ISO/IEC 27001:2022.

Integridad: Propiedad de exactitud y completitud de la información.
Fuente: NTC ISO/IEC 27000:2022.

MSPI: Modelo de Seguridad y Privacidad de la Información emitido por el Ministerio TIC para las entidades públicas.
Fuente: Resolución 02277 de 2025 – MinTIC.

Riesgo de seguridad de la información: Posibilidad de que una amenaza explote una vulnerabilidad y afecte la confidencialidad, integridad o disponibilidad de la información.
Fuente: NTC ISO/IEC 27005:2022.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.
Fuente: NTC ISO/IEC 27000:2022.

Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos interrelacionados para establecer, implementar, mantener y mejorar continuamente la seguridad de la información en la entidad.
Fuente: NTC ISO/IEC 27001:2022.

Tratamiento de riesgos: Proceso de selección e implementación de controles para modificar los riesgos.
Fuente: NTC ISO/IEC 27005:2022.

Parámetros utilizados en la SoA del SGSI:

- **No.:** Número consecutivo asignado al control para facilitar su referencia interna.
- **Control Anexo A:** Identificador y nombre oficial del control en la NTC ISO/IEC 27001:2022.
- **Descripción del control:** Texto del control conforme a la norma, que indica el resultado esperado.
- **Lineamiento institucional asociado:** Política específica (PA01–PA32) o documento institucional que materializa el control en la Cámara.
- **Estado del control:** Etiqueta que indica el estado de implementación del control:

- **(I) Implementado:** El control está implementado y operando en el SGSI.
- **(C) En curso:** El control fue seleccionado y se encuentra en proceso de implementación o pendiente de finalización.
- **(E) Excluido:** El control no aplica al alcance del SGSI; se incluye la justificación correspondiente.

5. DESARROLLO – CONTROLES DEL ANEXO A

A continuación, se relacionan los 93 controles del Anexo A de la NTC ISO/IEC 27001:2022, agrupados por dominio. Cada control se asocia con la política específica (PA01–PA32) del Manual de Políticas de Seguridad y Privacidad de la Información, y se indica su estado.

5.1 Controles organizacionales (A.5)

No.	Control Anexo A	Descripción del control	Lineamiento PA asociado	Estado
1	A.5.1 Políticas para la seguridad de la información	Definir, aprobar, publicar, comunicar y revisar la política de seguridad de la información y políticas específicas, a intervalos planificados y ante cambios significativos.	PA01 – Política General de Seguridad y Privacidad de la Información	I
2	A.5.2 Roles y responsabilidades de seguridad de la información	Definir y asignar roles y responsabilidades de seguridad de la información conforme a las necesidades de la entidad.	PA02 – Roles y responsabilidades	C
3	A.5.3 Segregación de funciones	Separar las funciones y áreas de responsabilidad	PA02 – Roles y responsabilidades	C

		que sean conflictivas para reducir el riesgo de mal uso.		
4	A.5.4 Responsabilidades de la dirección	Exigir a todo el personal aplicar la seguridad de la información conforme a las políticas y procedimientos establecidos.	PA01 – Política General de Seguridad y Privacidad de la Información	I
5	A.5.5 Contacto con autoridades	Establecer y mantener contacto con autoridades pertinentes (CSIRT Gobierno, ColCERT, MinTIC, Fiscalía, Policía Cibernética, entre otros).	PA21 – Inteligencia de amenazas	C
6	A.5.6 Contacto con grupos de interés especial	Establecer y mantener contacto con grupos de interés especial, foros especializados y asociaciones profesionales en seguridad de la información.	PA21 – Inteligencia de amenazas	C
7	A.5.7 Inteligencia de amenazas	Recopilar y analizar información sobre amenazas a la seguridad de la información para generar	PA21 – Inteligencia de amenazas	C

		inteligencia de amenazas.		
8	A.5.8 Seguridad de la información en la gestión de proyectos	Integrar la seguridad de la información en la gestión de proyectos.	PA22 – Seguridad en la gestión de proyectos	C
9	A.5.9 Inventario de información y otros activos asociados	Desarrollar y mantener un inventario de información y otros activos asociados, incluidos los propietarios.	PA15 – Gestión de activos de información	I
10	A.5.10 Uso aceptable de la información y otros activos asociados	Identificar, documentar e implementar reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos.	PA07 – Clasificación, etiquetado y uso aceptable de la información	C
11	A.5.11 Devolución de activos	El personal y terceros devolverán todos los activos de la entidad en su poder al cambiar o terminar su empleo, contrato o acuerdo.	PA09 – Seguridad en la gestión del personal	C
12	A.5.12 Clasificación de la información	Clasificar la información según las necesidades de seguridad (confidencialidad, integridad, disponibilidad).	PA07 – Clasificación, etiquetado y uso aceptable de la información	C

13	A.5.13 Etiquetado de la información	Desarrollar e implementar procedimientos para el etiquetado de la información conforme al esquema de clasificación.	PA07 – Clasificación, etiquetado y uso aceptable de la información	C
14	A.5.14 Transferencia de información	Establecer reglas, procedimientos o acuerdos para la transferencia segura de información dentro y fuera de la entidad.	PA07 – Clasificación, etiquetado y uso aceptable de la información	C
15	A.5.15 Control de acceso	Establecer e implementar reglas para controlar el acceso físico y lógico a la información y otros activos asociados.	PA14 – Control de acceso lógico	I
16	A.5.16 Gestión de identidad	Gestionar el ciclo de vida completo de las identidades de usuarios.	PA14 – Control de acceso lógico	C
17	A.5.17 Información de autenticación	Controlar la asignación y gestión de la información de autenticación mediante un proceso formal.	PA20 – Uso de criptografía y autenticación	C
18	A.5.18 Derechos de acceso	Proporcionar, revisar, modificar y eliminar los derechos de acceso conforme	PA14 – Control de acceso lógico	C

		a la política de control de acceso.		
19	A.5.19 Seguridad de la información en las relaciones con los proveedores	Definir e implementar procesos para gestionar los riesgos de seguridad asociados al uso de productos o servicios de proveedores.	PA05 – Seguridad con proveedores y terceros	C
20	A.5.20 Seguridad de la información en los acuerdos con proveedores	Establecer y acordar requisitos de seguridad pertinentes con cada proveedor según el tipo de relación.	PA05 – Seguridad con proveedores y terceros	C
21	A.5.21 Gestión de la seguridad de la información en la cadena de suministro de TIC	Definir e implementar procesos para gestionar los riesgos de seguridad en la cadena de suministro de productos y servicios TIC.	PA05 – Seguridad con proveedores y terceros	C
22	A.5.22 Seguimiento, revisión y gestión de cambios de servicios de proveedores	Monitorear, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad y prestación de servicios de los proveedores.	PA05 – Seguridad con proveedores y terceros	C
23	A.5.23 Seguridad de la información	Establecer procesos de	PA25 – Seguridad en	C

	para el uso de servicios en la nube	adquisición, uso, gestión y salida de los servicios en la nube conforme a los requisitos de seguridad.	servicios en la nube	
24	A.5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información	Planificar y prepararse para la gestión de incidentes definiendo procesos, roles y responsabilidades.	PA24 – Supervisión, monitoreo y gestión de incidentes	C
25	A.5.25 Evaluación y decisión sobre eventos de seguridad de la información	Evaluar los eventos de seguridad y decidir si se clasifican como incidentes.	PA24 – Supervisión, monitoreo y gestión de incidentes	C
26	A.5.26 Respuesta a incidentes de seguridad de la información	Responder a los incidentes conforme a los procedimientos documentados.	PA24 – Supervisión, monitoreo y gestión de incidentes	C
27	A.5.27 Aprender de los incidentes de seguridad de la información	Utilizar el conocimiento obtenido de los incidentes para fortalecer y mejorar los controles.	PA24 – Supervisión, monitoreo y gestión de incidentes	C
28	A.5.28 Recopilación de evidencia	Establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con	PA24 – Supervisión, monitoreo y gestión de incidentes	C

		eventos de seguridad.		
29	A.5.29 Seguridad de la información durante una interrupción	Planificar cómo mantener la seguridad de la información en un nivel adecuado durante una interrupción.	PA31 – Continuidad de negocio y recuperación ante desastres	C
30	A.5.30 Disponibilidad de las TIC para la continuidad del negocio	Planificar, implementar, mantener y probar la preparación de las TIC con base en los objetivos y requisitos de continuidad.	PA31 – Continuidad de negocio y recuperación ante desastres	C
31	A.5.31 Requisitos legales, estatutarios, reglamentarios y contractuales	Identificar, documentar y mantener actualizados los requisitos legales y contractuales aplicables y el enfoque para cumplirlos.	PA06 – Cumplimiento legal, normativo y contractual	I
32	A.5.32 Derechos de propiedad intelectual	Implementar procedimientos para proteger los derechos de propiedad intelectual.	PA06 – Cumplimiento legal, normativo y contractual	C
33	A.5.33 Protección de registros	Proteger los registros contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada.	PA29 – Registros, sincronización y continuidad TIC	C

34	A.5.34 Privacidad y protección de la información de identificación personal (PII)	Identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la PII conforme a las leyes aplicables.	PA30 – Privacidad y protección de datos personales	C
35	A.5.35 Revisión independiente de la seguridad de la información	Revisar de forma independiente el enfoque para gestionar la seguridad de la información a intervalos planificados o ante cambios significativos.	PA01 – Política General de Seguridad y Privacidad de la Información	C
36	A.5.36 Cumplimiento de políticas, normas y estándares de seguridad de la información	Revisar periódicamente el cumplimiento de las políticas, reglas y estándares de seguridad de la información.	PA06 – Cumplimiento legal, normativo y contractual	C
37	A.5.37 Procedimientos operacionales documentados	Documentar y poner a disposición del personal los procedimientos operativos para las instalaciones de procesamiento de información.	PA28 – Gestión de configuraciones y control de software	C

5.2 Controles de personas (A.6)

No.	Control Anexo A	Descripción del control	Lineamiento PA asociado	Estado
38	A.6.1 Verificación de antecedentes	Realizar controles de verificación de antecedentes de todos los candidatos antes de ingresar y de manera continua, conforme a leyes, reglamentos y ética aplicables.	PA09 – Seguridad en la gestión del personal	I
39	A.6.2 Términos y condiciones de empleo	Establecer en los acuerdos contractuales las responsabilidades del personal y de la entidad en materia de seguridad de la información.	PA09 – Seguridad en la gestión del personal	I
40	A.6.3 Concientización, educación y formación en seguridad de la información	Brindar concientización, educación, formación y actualizaciones periódicas en seguridad de la información al personal y partes interesadas relevantes.	PA04 – Concientización y formación en seguridad de la información	C
41	A.6.4 Proceso disciplinario	Formalizar y comunicar un proceso disciplinario para tomar acciones contra el personal que cometa violaciones a la	PA09 – Seguridad en la gestión del personal	C

		política de seguridad de la información.		
42	A.6.5 Responsabilidades después de la terminación o cambio de empleo	Definir, aplicar y comunicar al personal pertinente las responsabilidades de seguridad de la información que sigan siendo válidas después de la terminación o cambio de empleo.	PA09 – Seguridad en la gestión del personal	C
43	A.6.6 Acuerdos de confidencialidad o no divulgación	Identificar, documentar, revisar regularmente y firmar acuerdos de confidencialidad o no divulgación con el personal y otras partes interesadas relevantes.	PA10 – Compromisos de confidencialidad y conducta esperada	C
44	A.6.7 Trabajo remoto	Implementar medidas de seguridad cuando el personal trabaje de forma remota para proteger la información a la que se acceda, procese o almacene fuera de las instalaciones.	PA08 – Trabajo remoto y dispositivos móviles	C

45	A.6.8 Reporte de eventos de seguridad de la información	Proporcionar un mecanismo para que el personal informe oportunamente eventos de seguridad observados o sospechados a través de canales apropiados.	PA24 – Supervisión, monitoreo y gestión de incidentes	C

5.3 Controles físicos (A.7)

No.	Control Anexo A	Descripción del control	Lineamiento PA asociado	Estado
46	A.7.1 Perímetros de seguridad física	Definir y utilizar perímetros de seguridad para proteger las áreas que contienen información y otros activos asociados.	PA11 – Seguridad física y del entorno	I
47	A.7.2 Entrada física	Proteger las áreas seguras mediante controles de entrada y puntos de acceso apropiados.	PA12 – Control de acceso físico	I
48	A.7.3 Aseguramiento de oficinas, recintos e instalaciones	Diseñar e implementar la seguridad física de oficinas, recintos e instalaciones.	PA11 – Seguridad física y del entorno	I

49	A.7.4 Monitoreo de seguridad física	Monitorear continuamente las instalaciones para detectar accesos físicos no autorizados.	PA12 – Control de acceso físico	I
50	A.7.5 Protección contra amenazas físicas y ambientales	Diseñar e implementar protección contra amenazas físicas y ambientales (desastres naturales y otras amenazas intencionales o no).	PA11 – Seguridad física y del entorno	I
51	A.7.6 Trabajo en áreas seguras	Diseñar e implementar medidas de seguridad para el trabajo en áreas seguras.	PA11 – Seguridad física y del entorno	C
52	A.7.7 Escritorio limpio y pantalla limpia	Definir y hacer cumplir reglas de escritorio limpio para documentos y medios extraíbles, y de pantalla limpia para las instalaciones de procesamiento de información.	PA11 – Seguridad física y del entorno	I
53	A.7.8 Ubicación y protección de equipos	Ubicar y proteger los equipos de forma segura.	PA13 – Protección de activos físicos y medios de almacenamiento	I

54	A.7.9 Seguridad de activos fuera de las instalaciones	Proteger los activos cuando se encuentren fuera de las instalaciones de la entidad.	PA13 – Protección de activos físicos y medios de almacenamiento	C
55	A.7.10 Medios de almacenamiento	Gestionar los medios de almacenamiento a lo largo de su ciclo de vida conforme al esquema de clasificación y a los requisitos de manipulación.	PA13 – Protección de activos físicos y medios de almacenamiento	C
56	A.7.11 Servicios de soporte	Proteger las instalaciones de procesamiento de información contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.	PA11 – Seguridad física y del entorno	I
57	A.7.12 Seguridad del cableado	Proteger los cables que transportan energía, datos o servicios de información de apoyo contra intercepciones, interferencias o daños.	PA11 – Seguridad física y del entorno	I
58	A.7.13 Mantenimiento de equipos	Mantener los equipos correctamente	PA13 – Protección de activos físicos y	I

		para garantizar la disponibilidad, integridad y confidencialidad de la información.	medios de almacenamiento	
59	A.7.14 Eliminación o reutilización segura de equipos	Verificar los equipos que contengan medios de almacenamiento para asegurar la eliminación o sobreescritura segura de datos confidenciales y software licenciado antes de su eliminación o reutilización.	PA26 – Eliminación y destrucción segura de información	C

5.4 Controles tecnológicos (A.8)

No.	Control Anexo A	Descripción del control	Lineamiento PA asociado	Estado
60	A.8.1 Dispositivos de punto final de usuario	Proteger la información almacenada, procesada o accesible a través de los dispositivos finales de usuario.	PA08 – Trabajo remoto y dispositivos móviles	I
61	A.8.2 Derechos de acceso privilegiado	Restringir y gestionar la asignación y uso de los derechos de acceso privilegiado.	PA14 – Control de acceso lógico	I
62	A.8.3 Restricción de acceso a la información	Restringir el acceso a la información y otros activos asociados conforme a la política específica de control de acceso.	PA14 – Control de acceso lógico	I
63	A.8.4 Acceso al código fuente	Gestionar adecuadamente el acceso de lectura y escritura al código fuente, herramientas de desarrollo y bibliotecas de software.	No aplica	E

64	A.8.5 Autenticación segura	Implementar tecnologías y procedimientos de autenticación segura en función de las restricciones de acceso y la política específica de control de acceso.	PA20 – Uso de criptografía y autenticación	C
65	A.8.6 Gestión de capacidad	Controlar y ajustar el uso de los recursos conforme a los requisitos de capacidad actuales y previstos.	PA29 – Registros, sincronización y continuidad TIC	I
66	A.8.7 Protección contra malware	Implementar protección contra malware respaldada por la concientización del usuario.	PA17 – Protección contra software malicioso	I
67	A.8.8 Gestión de vulnerabilidades técnicas	Obtener información sobre las vulnerabilidades técnicas de los sistemas en uso, evaluar la exposición y tomar las medidas apropiadas.	PA27 – Pruebas de seguridad técnica y validación de cambios	I
68	A.8.9 Gestión de la configuración	Establecer, documentar, implementar, monitorear y	PA28 – Gestión de configuraciones	I

		revisar las configuraciones (incluidas las de seguridad) de hardware, software, servicios y redes.	y control de software	
69	A.8.10 Eliminación de información	Eliminar la información almacenada en sistemas de información, dispositivos o cualquier otro medio cuando ya no sea necesaria.	PA26 – Eliminación y destrucción segura de información	I
70	A.8.11 Enmascaramiento de datos	Usar el enmascaramiento de datos conforme a la política de control de acceso, otras políticas relacionadas, los requisitos del negocio y la legislación aplicable.	PA20 – Uso de criptografía y autenticación	C
71	A.8.12 Prevención de fuga de datos	Aplicar medidas de prevención de fuga de datos a los sistemas, redes y otros dispositivos que procesen, almacenen o transmitan información sensible.	PA30 – Privacidad y protección de datos personales	C

72	A.8.13 Copia de seguridad de la información	Mantener y probar periódicamente copias de seguridad de la información, el software y los sistemas conforme a la política específica acordada.	PA18 – Copias de seguridad y restauración	I
73	A.8.14 Redundancia de instalaciones de procesamiento de información	Implementar las instalaciones de procesamiento de información con suficiente redundancia para cumplir con los requisitos de disponibilidad.	PA31 – Continuidad de negocio y recuperación ante desastres	I
74	A.8.15 Registro de eventos (logs)	Producir, almacenar, proteger y analizar registros que documenten actividades, excepciones, fallas y otros eventos relevantes.	PA29 – Registros, sincronización y continuidad TIC	I
75	A.8.16 Actividades de monitoreo	Monitorear redes, sistemas y aplicaciones para detectar comportamiento anómalo y tomar acciones apropiadas para evaluar posibles incidentes.	PA24 – Supervisión, monitoreo y gestión de incidentes	I

76	A.8.17 Sincronización de relojes	Sincronizar los relojes de los sistemas de procesamiento de información con fuentes de tiempo aprobadas.	PA29 – Registros, sincronización y continuidad TIC	I
77	A.8.18 Uso de programas utilitarios privilegiados	Restringir y controlar estrictamente el uso de programas utilitarios que puedan anular los controles del sistema y de las aplicaciones.	PA14 – Control de acceso lógico	C
78	A.8.19 Instalación de software en sistemas operativos	Implementar procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.	PA28 – Gestión de configuraciones y control de software	I
79	A.8.20 Seguridad de redes	Asegurar, administrar y controlar las redes y dispositivos de red para proteger la información en sistemas y aplicaciones.	PA16 – Seguridad en redes y comunicaciones	I
80	A.8.21 Seguridad de los servicios de red	Identificar, implementar y controlar los mecanismos de seguridad,	PA16 – Seguridad en redes y comunicaciones	I

		niveles de servicio y requisitos de los servicios de red.		
81	A.8.22 Segregación de redes	Segregar grupos de servicios de información, usuarios y sistemas de información en las redes de la entidad.	PA16 – Seguridad en redes y comunicaciones	I
82	A.8.23 Filtrado web	Gestionar el acceso a sitios web externos para reducir la exposición a contenido malicioso.	PA23 – Filtrado web y uso aceptable de Internet	C
83	A.8.24 Uso de criptografía	Definir e implementar reglas para el uso efectivo de la criptografía, incluida la gestión de claves criptográficas.	PA20 – Uso de criptografía y autenticación	C
84	A.8.25 Ciclo de vida de desarrollo seguro	Establecer y aplicar reglas para el desarrollo seguro de software y sistemas.	No aplica	E
85	A.8.26 Requisitos de seguridad de la aplicación	Identificar, especificar y aprobar los requisitos de seguridad de la información al desarrollar o	No aplica	E

		adquirir aplicaciones.		
86	A.8.27 Principios de arquitectura e ingeniería de sistemas seguros	Establecer, documentar, mantener y aplicar principios para la ingeniería de sistemas seguros en cualquier actividad de desarrollo de sistemas de información.	No aplica	E
87	A.8.28 Codificación segura	Aplicar los principios de codificación segura al desarrollo de software.	No aplica	E
88	A.8.29 Pruebas de seguridad en desarrollo y aceptación	Definir e implementar procesos de pruebas de seguridad en el ciclo de vida del desarrollo.	No aplica	E
89	A.8.30 Desarrollo tercerizado	Dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas tercerizados.	No aplica	E
90	A.8.31 Separación de entornos de desarrollo,	Separar y proteger los entornos de desarrollo,	PA28 – Gestión de configuraciones y control de software	C

	prueba y producción	prueba y producción.		
91	A.8.32 Gestión de cambios	Someter los cambios en las instalaciones de procesamiento de información y los sistemas de información a procedimientos de gestión de cambios.	PA28 – Gestión de configuraciones y control de software	C
92	A.8.33 Información de pruebas	Seleccionar, proteger y gestionar adecuadamente la información usada para pruebas.	No aplica	E
93	A.8.34 Protección de sistemas de información durante las pruebas de auditoría	Planificar y acordar entre el auditor y la dirección las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de sistemas operativos.	PA27 – Pruebas de seguridad técnica y validación de cambios	C

6. JUSTIFICACIÓN DE EXCLUSIONES

Los controles que se relacionan a continuación se han identificado como (E) Excluidos del alcance del SGSI de la Cámara de Representantes, considerando que la entidad no realiza desarrollo de

software propio. Las funciones legislativas, administrativas y misionales de la Cámara no contemplan el ciclo de vida de desarrollo de aplicaciones; las herramientas de apoyo se adquieren a proveedores externos. Por lo tanto, los siguientes controles del Anexo A no aplican:

Control	Justificación de exclusión
A.8.4 Acceso al código fuente	La Cámara de Representantes no desarrolla software propio. No existe código fuente, herramientas de desarrollo ni bibliotecas internas bajo gestión de la entidad.
A.8.25 Ciclo de vida de desarrollo seguro	No aplica. La entidad no realiza desarrollo de software interno; los sistemas se adquieren a proveedores externos quienes asumen el ciclo de vida de desarrollo.
A.8.26 Requisitos de seguridad de la aplicación	No aplica. La definición y aprobación de requisitos de seguridad para aplicaciones se realiza al momento de la adquisición a proveedores (cubierto por A.5.20).
A.8.27 Principios de arquitectura e ingeniería de sistemas seguros	No aplica. La Cámara no efectúa actividades de ingeniería ni desarrollo de sistemas; estos son provistos por terceros.
A.8.28 Codificación segura	No aplica. No se realiza desarrollo de software propio, por lo que no se aplican principios de codificación segura interna.
A.8.29 Pruebas de seguridad en desarrollo y aceptación	No aplica para desarrollo interno. Las pruebas de seguridad técnica sobre sistemas adquiridos se realizan bajo la PA27 (Pruebas de seguridad técnica y validación de cambios).
A.8.30 Desarrollo tercerizado	No aplica. No se tercerizan actividades de desarrollo de software por parte de la entidad. Los sistemas de información se adquieren como productos terminados a proveedores externos.
A.8.33 Información de pruebas	No aplica. La Cámara no opera entornos de prueba de desarrollo; los sistemas en uso corresponden a entornos productivos administrados por sus proveedores o por la OPS.

7. ANEXOS Y DOCUMENTOS RELACIONADOS

La presente Declaración de Aplicabilidad debe ser leída en conjunto con los siguientes documentos institucionales:

- Política General de Seguridad y Privacidad de la Información
- Manual de Políticas de Seguridad y Privacidad de la Información de la Cámara de Representantes
- Plan de Seguridad y Privacidad de la Información 2026
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026
- Modelo de Seguridad y Privacidad de la Información (MSPI) – MinTIC, Resolución 02277 de 2025.
- NTC ISO/IEC 27001:2022 – Anexo A (referencia normativa).

8. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio
01	28/05/2026	Declaración de Aplicabilidad inicial, anexa a la Política de Seguridad y Privacidad de la Información (versión ISO/IEC 27001:2022).

JORGE EDISON CASTRO SALCEDO
Jefe Oficina de Planeación y Sistemas
Cámara de Representantes
Revisión: Ing. Daniela Andrade cps_0529_2026
Ing. Elkin Rojas Roa cps_0384_2026
Ing. Fabian Lizarazo