CÁMARA DE REPRESENTANTES

MANUAL DE POLÍTICAS DE 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. INTRODUCCIÓN 4
2. OBJETIVO 4
3. ALCANCE 5
4. GLOSARIO 5
5. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 9
5.1 Controles organizacionales 9
PA01 – Política General de Seguridad y Privacidad de la Información 9
PA02 – Roles y responsabilidades 10
PA03 – Gestión del riesgo de seguridad de la información 11
PA04 – Concientización y formación en seguridad de la información 11
PA05 – Seguridad con proveedores y terceros 12
PA06 – Cumplimiento legal, normativo y contractual 13
PA07 – Clasificación, etiquetado y uso aceptable de la información 14
PA08 – Trabajo remoto y dispositivos móviles 14
5.2 Controles de personas 15
PA09 – Seguridad en la gestión del personal 15
PA10 – Compromisos de confidencialidad y conducta esperada 16
5.3 Controles físicos 17
PA11 – Seguridad física y del entorno 17
PA12 – Control de acceso físico 18
PA13 – Protección de activos físicos y medios de almacenamiento 18
5.4 Controles tecnológicos 19
PA14 – Control de acceso lógico 19
PA15 – Gestión de activos de información 20
PA16 – Seguridad en redes y comunicaciones 21
PA17 – Protección contra software malicioso 22
PA18 – Copias de seguridad y restauración 22
PA19 – Uso de criptografía y autenticación 23
PA20 – Inteligencia de amenazas 23
PA21 – Seguridad en la gestión de proyectos 24
PA22 – Filtrado web y uso aceptable de Internet 25

PA23– Supervisión, monitoreo y gestión de incidentes 25
PA24 – Seguridad en servicios en la nube 26
PA25 – Eliminación y destrucción segura de información 27
PA26 – Pruebas de seguridad técnica y validación de cambios 28
PA27 – Gestión de configuraciones y control de software 28
PA28 – Registros, sincronización y continuidad TIC 29
5.5 Políticas adicionales de privacidad y continuidad 30
PA29 – Privacidad y protección de datos personales 30
PA30 – Continuidad de negocio y recuperación ante desastres 31
PA31 – Tiempos objetivo de recuperación (RTO/RPO) para activos críticos 33
6. VIGENCIA, REVISIÓN Y MEJORA 34
7. APROBACIÓN Y RESPONSABLES DEL DOCUMENTO 34
8. CONTROL DE CAMBIOS 35

1. INTRODUCCIÓN

La Cámara de Representantes de Colombia, consciente del valor estratégico de la información para el cumplimiento de sus funciones constitucionales, legales y administrativas, y de la necesidad de protegerla frente a amenazas internas y externas, adopta el presente Manual de Políticas de Seguridad y Privacidad de la Información como instrumento técnico, normativo y administrativo orientado a fortalecer la protección de sus activos de información.

Este manual consolida las políticas específicas y las normas operativas necesarias para implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) efectivo, alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), regulado mediante la Resolución 02277 de 2025 y su anexo técnico, y con la Norma Técnica Colombiana NTC ISO/IEC 27001:2022, que establece el estándar internacional vigente para los sistemas de gestión de seguridad de la información.

El contenido aquí descrito orienta la gestión de la seguridad y privacidad de la información en todos los niveles y procesos institucionales de la Cámara de Representantes, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información. Estas políticas reflejan el compromiso de la Alta Dirección y se articulan con el Sistema Integrado de Gestión, la Política de Gobierno Digital, la gestión documental institucional y los marcos de protección de datos personales.

El cumplimiento de este manual es obligatorio para todos los Honorables Representantes a la Cámara, Mesa Directiva, funcionarios, contratistas, practicantes, proveedores y terceros que accedan, procesen, transmitan o almacenen información institucional. Asimismo, este documento será revisado al menos anualmente para proteger su vigencia y pertinencia frente a los cambios en el contexto tecnológico, normativo, legislativo y de riesgos.

2. OBJETIVO

El presente manual tiene como objetivo establecer las políticas y normas específicas de seguridad y privacidad de la información diseñadas para la Cámara de Representantes de Colombia, con el fin de proteger la información institucional mediante la implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI). Estas políticas contribuyen a preservar la confidencialidad, integridad y disponibilidad de la información institucional, así como la gestión adecuada de los riesgos mediante la aplicación de controles alineados con el Modelo de

Seguridad y Privacidad de la Información (MSPI) del MinTIC y la norma NTC ISO/IEC 27001:2022.

3. ALCANCE

El presente manual de políticas y normas de seguridad y privacidad de la información aplica como anexo técnico a la Política General de Seguridad y Privacidad de la Información de la Cámara de Representantes de Colombia.

Su contenido abarca la definición, despliegue y gestión de las políticas específicas que soportan el Sistema de Gestión de Seguridad de la Información (SGSI), alineadas con el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC y la norma NTC ISO/IEC 27001:2022. Aplica de manera obligatoria a:

- Honorables Representantes a la Cámara, Mesa Directiva y sus Unidades de Trabajo Legislativo (UTL).
- Funcionarios de planta y de carrera administrativa.
- Contratistas, practicantes, pasantes y personal vinculado mediante cualquier modalidad.
- Proveedores, consultores y terceros que accedan, procesen, transmitan o almacenen información institucional.
- Todos los procesos, sistemas de información, infraestructura tecnológica, instalaciones físicas y activos de información bajo responsabilidad de la Entidad.

4. GLOSARIO

Para efectos del presente manual se adoptan las siguientes definiciones:

Aceptación del riesgo: Decisión de asumir un riesgo sin aplicar medidas adicionales de mitigación. *Fuente: ISO/IEC 27000:2022*

Activo de información: Cualquier elemento que tenga valor para la organización, incluyendo datos, personas, dispositivos, sistemas, servicios e infraestructura. *Fuente: ISO/IEC 27000:2018*

Análisis del riesgo: Proceso para comprender la naturaleza del riesgo y determinar su nivel. *Fuente: ISO/IEC 27000:2022*

Autenticidad: Propiedad que asegura que una entidad es quien dice ser. *Fuente: ISO/IEC ISO/IEC 27000:2022*

Clasificación de la información: Proceso de asignación de niveles de sensibilidad o criticidad a la información, según su valor y riesgos asociados. *Fuente: MSPI – MinTIC*

Confidencialidad: Propiedad que protege que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. *Fuente: ISO/IEC 27000:2018*

Control de seguridad: Medida implementada para modificar o mantener un riesgo dentro de niveles aceptables. *Fuente: ISO/IEC 27000:2018*

Datos personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. *Fuente: Ley 1581 de 2012*

Declaración de aplicabilidad (SoA): Documento que justifica los controles seleccionados y excluidos del Anexo A de la ISO/IEC 27001. *Fuente: ISO/IEC 27001:2022*

Disponibilidad: Propiedad que busca que la información esté accesible y utilizable por las personas autorizadas cuando se requiera. *Fuente: ISO/IEC 27000:2018*

Evaluación del riesgo: Comparación entre los niveles de riesgo estimados y los criterios establecidos, para determinar su aceptabilidad. *Fuente: ISO/IEC 27005:2018*

Evento de seguridad de la información: Ocurrencia identificada en un sistema o servicio que indica una posible violación de la política o fallo de control. *Fuente: ISO/IEC 27035-1:2016*

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización respecto al riesgo. *Fuente: ISO/IEC 27000:2018, ISO 31000:2018*

Incidente de seguridad de la información: Evento o serie de eventos inesperados o no deseados que comprometen la seguridad de la información. *Fuente: ISO/IEC 27035-1:2016*

Información pública: Toda información que un sujeto obligado genere, obtenga, adquiera o controle en su calidad de tal. *Fuente: Ley 1712 de 2014*

Información pública clasificada: Información que, por estar relacionada con derechos o intereses privados o de terceros, su acceso podrá ser negado o exceptuado. *Fuente: Ley 1712 de 2014*

Información pública reservada: Información cuyo acceso podrá ser rechazado o denegado por daño a intereses públicos. *Fuente: Ley 1712 de 2014*

Integridad: Propiedad que asegura que la información no ha sido modificada de manera no autorizada y mantiene su exactitud y completitud. *Fuente: ISO/IEC 27000:2018*

No repudio: Propiedad que asegura que una entidad no pueda negar haber realizado una acción determinada sobre un activo de información, preservando la imputabilidad de las acciones ejecutadas. *Fuente: ISO/IEC 27000:2018*

Oficial de Seguridad de la Información (OSI): Persona encargada de liderar y coordinar el SGSI en la entidad. *Fuente: MSPI – MinTIC*

PII (Información Identificable Personal): Cualquier información que pueda ser usada para identificar al individuo a quien se refiere o que esté vinculada a un individuo identificable. *Fuente: ISO/IEC 27701:2019*

Recursos informáticos: Infraestructura, hardware, software y redes utilizadas para procesar, almacenar y transmitir información. *Fuente: MSPI – MinTIC*

RPO (Recovery Point Objective): Punto objetivo de recuperación. Cantidad máxima de datos, medida en tiempo, que una organización está dispuesta a perder ante un incidente. *Fuente: ISO 22301:2019*

RTO (Recovery Time Objective): Tiempo objetivo de recuperación. Período máximo durante el cual un proceso o servicio puede permanecer interrumpido tras un incidente antes de afectar gravemente a la organización. *Fuente: ISO 22301:2019*

Riesgo: Efecto de la incertidumbre sobre los objetivos. *Fuente: ISO 31000:2018*

Riesgo inherente: Nivel de riesgo existente en ausencia de controles. *Fuente: ISO/IEC 27005:2018*

Riesgo residual: Nivel de riesgo que permanece después de aplicar controles o tratamientos. *Fuente: ISO/IEC 27005:2018*

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información. *Fuente: ISO/IEC 27000:2018*

Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos interrelacionados que establecen políticas, objetivos y procesos para proteger la información. *Fuente: ISO/IEC 27001:2022*

Sistema de información: Conjunto de elementos organizados para la recolección, procesamiento, almacenamiento y distribución de información. *Fuente: MSPI – MinTIC*

Tecnología de la información: Hardware, software y servicios que permiten el tratamiento automático de la información. *Fuente: MSPI – MinTIC*

Tratamiento del riesgo: Proceso para seleccionar e implementar acciones dirigidas a modificar el riesgo. *Fuente: ISO/IEC 27005:2018*

Trazabilidad: Propiedad que permite reconstruir las acciones realizadas sobre un activo de información, identificando origen, autor, momento y modificaciones. *Fuente: MSPI – MinTIC*

Valoración del riesgo: Proceso compuesto por el análisis y la evaluación del riesgo. *Fuente: ISO/IEC 27005:2018*

5. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Esta sección consolida las políticas específicas que soportan técnicamente la implementación de la Política General de Seguridad y Privacidad de la Información y del Sistema de Gestión de Seguridad de la Información (SGSI) de la Cámara de Representantes. Cada política está alineada con los controles y dominios establecidos en la norma NTC ISO/IEC 27001:2022 y con los componentes definidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC.

Las políticas aquí descritas tienen como objetivo orientar la aplicación de controles operativos y estratégicos que aseguren la confidencialidad, integridad y disponibilidad de los activos de información, y establecer responsabilidades claras para su cumplimiento. La estructura sigue los cuatro grupos de controles del Anexo A de la ISO/IEC 27001:2022: organizacionales, de personas, físicos y tecnológicos.

5.1 Controles organizacionales

Incluye políticas relacionadas con la estructura de gestión, roles, gobierno, riesgos, relaciones externas, concienciación y cumplimiento normativo.

PA01 – Política General de Seguridad y Privacidad de la Información

Definición:
Establece los lineamientos generales para proteger la información institucional de la Cámara de Representantes, preservar su confidencialidad, integridad y disponibilidad, y cumplir con los marcos normativos aplicables, incluyendo la NTC ISO/IEC 27001:2022 y el MSPI del MinTIC.

Alcance:
Aplica a todos los Honorables Representantes, funcionarios, contratistas y terceros que gestionen activos de información en el marco de los procesos de la Entidad.

Lineamientos clave:

- Implementar controles de seguridad acordes al nivel de riesgo identificado en cada proceso.
- Integrar el SGSI con el Sistema Integrado de Gestión y la planeación institucional.
- Promover la mejora continua del sistema mediante revisiones periódicas y auditorías.
- Sensibilizar y formar a los usuarios en seguridad y privacidad de la información.

- Cumplir con las leyes, regulaciones y normas aplicables a la actividad legislativa y administrativa.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.1 Políticas para la seguridad de la información
- A.5.35 Revisión independiente de la seguridad de la información

PA02 – Roles y responsabilidades

Definición:

Establece la asignación de responsabilidades y funciones específicas para la gestión de la seguridad y privacidad de la información en la Cámara de Representantes.

Alcance:

Aplica a todos los funcionarios, contratistas y terceros que participen en la creación, gestión o soporte de activos de información institucional.

Lineamientos clave:

- La Mesa Directiva y la Alta Dirección lideran y apoyan la implementación del SGSI.
- El Oficial de Seguridad de la Información coordina la aplicación de controles y reporta a la Dirección General Administrativa.
- La Oficina de Planeación y Sistemas es responsable de la operación técnica de los controles tecnológicos.
- Cada responsable de proceso gestiona los riesgos de seguridad de su área.
- Todo el personal debe cumplir las políticas y reportar incidentes de seguridad.
- Los proveedores deben cumplir requisitos contractuales de seguridad.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.2 Roles y responsabilidades de seguridad de la información
- A.5.3 Segregación de funciones
- A.5.4 Responsabilidades de la dirección
- A.5.5 Contacto con las autoridades
- A.5.6 Contacto con grupos de interés especial
- A.5.36 Cumplimiento de políticas, normas y estándares de seguridad de la información.

PA03 – Gestión del riesgo de seguridad de la información

Definición:
Establece los lineamientos para identificar, analizar, evaluar, tratar y monitorear los riesgos que puedan afectar la seguridad y privacidad de la información de la Cámara de Representantes.

Alcance:
Aplica a todos los procesos, activos y servicios de la Entidad que manejan información, tanto a nivel interno como en interacción con terceros.

Lineamientos clave:

- Aplicar una metodología formal y sistemática de análisis y valoración de riesgos basada en NTC ISO/IEC 27005 e ISO 31000.
- Documentar y mantener actualizada la matriz de riesgos de seguridad de la información.
- Alinear el tratamiento del riesgo con la capacidad institucional y el apetito al riesgo definido por la Alta Dirección.
- Incluir a los responsables de proceso en la identificación, valoración y seguimiento de riesgos.
- Articular la gestión de riesgos de seguridad con la gestión integral de riesgos institucionales.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- Cláusula 6.1 Acciones para abordar riesgos y oportunidades
- A.5.21 Gestión de la seguridad de la información en la cadena de suministro de las TIC
- A.5.37 Procedimientos operacionales documentados

PA04 – Concientización y formación en seguridad de la información

Definición:
Establece las directrices para sensibilizar, capacitar y mantener informados a los Honorables Representantes, funcionarios, contratistas y terceros sobre sus responsabilidades frente a la seguridad y privacidad de la información.

Alcance:
Aplica a todas las personas que accedan, procesen o gestionen información institucional de la Cámara de Representantes.

Lineamientos clave:

- Realizar actividades periódicas de sensibilización en ciberseguridad y protección de datos personales.
- Incluir temas de seguridad de la información en procesos de inducción y reinducción.
- Fortalecer capacidades técnicas en los equipos que gestionan TI, datos y riesgos.
- Realizar campañas específicas dirigidas a las Unidades de Trabajo Legislativo (UTL) y al personal de apoyo.
- Evaluar la efectividad de las acciones de formación implementadas mediante indicadores.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.6.3 Concientización, educación y entrenamiento en seguridad de la información

PA05 – Seguridad con proveedores y terceros

Definición:

Establece los lineamientos para asegurar que los proveedores y terceros que tengan acceso a información o recursos tecnológicos de la Cámara de Representantes cumplan con los requisitos de seguridad y privacidad establecidos por la Entidad.

Alcance:

Aplica a todos los contratos, convenios o acuerdos con terceros que impliquen acceso, tratamiento o soporte a activos de información institucional.

Lineamientos clave:

- Incluir cláusulas de seguridad y confidencialidad en los contratos y convenios.
- Evaluar riesgos de seguridad asociados a proveedores y servicios externos antes de la contratación.
- Supervisar el cumplimiento de los requisitos de seguridad durante la relación contractual.
- Definir medidas de control para el acceso remoto o compartido con terceros.
- Aplicar acuerdos de tratamiento de datos personales cuando corresponda según la Ley 1581 de 2012.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.14 Transferencia de información
- A.5.15 Control de acceso
- A.5.16 Gestión de la identidad
- A.5.17 Información de autenticación

- A.5.19 Seguridad de la información en la relación con proveedores
- A.5.20 Abordar la seguridad de la información en los acuerdos con los proveedores
- A.5.22 Seguimiento, revisión y gestión de cambios de servicios de proveedores
- A.5.37 Procedimientos operacionales documentados

PA06 – Cumplimiento legal, normativo y contractual

Definición:

Establece los lineamientos para preservar que la gestión de la información en la Cámara de Representantes cumpla con la legislación vigente, regulaciones aplicables y obligaciones contractuales en materia de seguridad y privacidad.

Alcance:

Aplica a todos los procesos, sistemas y relaciones contractuales que involucren tratamiento de información institucional.

Lineamientos clave:

- Identificar y aplicar la normativa vigente sobre protección de datos personales, acceso a la información, transparencia y habeas data.
- Asegurar el cumplimiento de requisitos legales en el manejo de registros, evidencia digital y contratación pública.
- Incorporar requisitos legales y contractuales en la operación de los sistemas de información.
- Mantener evidencia del cumplimiento normativo y apoyar auditorías externas, requerimientos de la Procuraduría, Contraloría o autoridades judiciales.
- Atender las disposiciones de la Ley 5 de 1992 (Reglamento del Congreso) en lo relacionado con manejo de información legislativa.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.31 Requisitos legales, estatutarios, regulatorios y contractuales
- A.5.32 Derechos de propiedad intelectual
- A.5.33 Protección de registros
- A.5.34 Privacidad y protección de la PII
- A.5.36 Cumplimiento de políticas, normas y estándares de seguridad de la información

PA07 – Clasificación, etiquetado y uso aceptable de la información

Definición:
Establece las directrices para clasificar, etiquetar y manejar adecuadamente la información institucional de acuerdo con su nivel de sensibilidad, así como definir las condiciones para su uso aceptable.

Alcance:
Aplica a todos los documentos, datos y sistemas que contengan información institucional, sin importar su formato o medio de almacenamiento.

Lineamientos clave:

- Clasificar la información como pública, pública clasificada, pública reservada o de uso interno, según MSPI Resolución 02277 de 2025.
- Etiquetar los activos de información conforme a su clasificación.
- Preservar que el tratamiento de la información se realice de acuerdo con su nivel de sensibilidad y reserva legal.
- Definir y divulgar reglas claras de uso aceptable para el acceso, almacenamiento y transmisión de información.
- Articular la clasificación con las Tablas de Retención Documental (TRD) y los lineamientos del Archivo General.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.10 Uso aceptable de activos de información y otros asociados a la misma
- A.5.11 Devolución de activos
- A.5.12 Clasificación de la información
- A.5.13 Etiquetado de la información

PA08 – Trabajo remoto y dispositivos móviles

Definición:
Establece los lineamientos para proteger la información institucional cuando es accedida o procesada mediante dispositivos móviles o fuera de las instalaciones de la Cámara de Representantes.

Alcance:
Aplica al personal, contratistas y terceros que utilicen equipos móviles o accedan a los sistemas de la Entidad desde ubicaciones remotas.

Lineamientos clave:

- Autorizar previamente el acceso remoto y el uso de dispositivos móviles para fines institucionales.
- Aplicar cifrado, autenticación multifactor y control de acceso en conexiones remotas mediante VPN.
- Definir condiciones y restricciones para el uso institucional de equipos personales (BYOD).
- Supervisar y limitar el almacenamiento de información sensible o reservada en dispositivos móviles.
- Establecer obligaciones de bloqueo de pantalla, reporte de pérdida y borrado remoto.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.18 Derechos de acceso
- A.5.37 Procedimientos operacionales documentados
- A.6.7 Trabajo remoto
- A.7.6 Trabajar en áreas seguras

5.2 Controles de personas

Controles relacionados con la seguridad antes, durante y después del vínculo laboral o contractual.

PA09 – Seguridad en la gestión del personal

Definición:
Establece los lineamientos para asegurar que el personal que tenga acceso a información institucional conozca y cumpla con las responsabilidades de seguridad durante todo el ciclo del vínculo laboral o contractual.

Alcance:

Aplica a funcionarios, contratistas y demás personas con acceso a los sistemas o activos de información de la Cámara de Representantes.

Lineamientos clave:

- Verificar antecedentes y compromisos de confidencialidad antes del ingreso, conforme a las disposiciones aplicables al empleo público.
- Incluir responsabilidades de seguridad en los perfiles de cargo, manuales de funciones y contratos.
- Definir procedimientos formales para el retiro o cambio de funciones, Preservando el retiro oportuno de accesos y activos.
- Articular los procesos con la Dirección Administrativa y la División de Personal.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.37 Procedimientos operacionales documentados
- A.6.1 Revisión de antecedentes
- A.6.2 Términos y condiciones de empleo
- A.6.4 Proceso disciplinario
- A.6.5 Responsabilidades después de la finalización o cambio de empleo

PA10 – Compromisos de confidencialidad y conducta esperada

Definición:

Establece los compromisos que deben asumir funcionarios, contratistas y terceros respecto al uso responsable de la información y el cumplimiento de normas de conducta relacionadas con la seguridad de la información.

Alcance:

Aplica a toda persona que tenga acceso a activos de información de la Cámara de Representantes, de forma directa o indirecta.

Lineamientos clave:

- Firmar acuerdos o compromisos de confidencialidad como parte de la vinculación contractual o laboral.
- Incluir cláusulas de uso adecuado de la información en contratos y convenios.
- Establecer consecuencias por el incumplimiento de las normas de seguridad, en concordancia con el régimen disciplinario aplicable.

- Reforzar principios éticos en la gestión de la información institucional, en particular sobre información legislativa reservada.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.6.2 Términos y condiciones de empleo
- A.6.6 Acuerdos de confidencialidad o no divulgación

5.3 Controles físicos

Políticas relacionadas con el entorno físico y protección de instalaciones, equipos y medios.

PA11 – Seguridad física y del entorno

Definición:
Establece las medidas para proteger las instalaciones, equipos y áreas donde se maneja información institucional, frente a accesos no autorizados, daños o interferencias.

Alcance:
Aplica a todos los espacios físicos bajo responsabilidad de la Cámara de Representantes donde se ubiquen sistemas de información o se almacene información institucional, incluyendo el Capitolio Nacional, el Edificio Nuevo del Congreso y las demás sedes.

Lineamientos clave:

- Restringir el acceso físico a zonas críticas como salas de servidores, archivos confidenciales y oficinas que custodien información reservada.
- Implementar mecanismos de control de acceso físico (cerraduras, tarjetas, biometría, registros).
- Proteger los equipos contra daños por fuego, agua, fallas eléctricas y otros eventos ambientales.
- Asegurar la continuidad de los servicios ante cortes de energía mediante UPS y plantas eléctricas.
- Coordinar con la División de Servicios Generales y el área de seguridad institucional.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.37 Procedimientos operacionales documentados
- A.7.1 Perímetros de seguridad física
- A.7.2 Entrada física

- A.7.4 Supervisión de la seguridad física
- A.7.12 Seguridad del cableado
- A.7.13 Mantenimiento de equipos

PA12 – Control de acceso físico

Definición:
Establece los mecanismos para gestionar y restringir el acceso físico a las instalaciones y recursos donde se almacena o procesa información de la Cámara de Representantes.

Alcance:
Aplica a todas las sedes, zonas restringidas, centros de datos, cuartos de comunicaciones y demás espacios físicos relacionados con el manejo de información institucional.

Lineamientos clave:
- Implementar controles de acceso físico diferenciados por niveles de criticidad.
- Registrar ingresos y salidas del personal y visitantes en zonas sensibles.
- Revocar el acceso físico inmediatamente al finalizar la relación contractual o laboral.
- Inspeccionar periódicamente el estado de los controles de acceso físico.
- Establecer procedimientos para visitantes, contratistas y personal de mantenimiento.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:
- A.5.37 Procedimientos operacionales documentados
- A.7.3 Aseguramiento de oficinas, salas e instalaciones
- A.7.4 Supervisión de la seguridad física

PA13 – Protección de activos físicos y medios de almacenamiento

Definición:
Establece las medidas para proteger los activos físicos y los medios que contienen información institucional, asegurando su uso adecuado, almacenamiento seguro y disposición controlada.

Alcance:
Aplica a todos los equipos, dispositivos, documentos impresos y medios digitales utilizados o almacenados en las instalaciones de la Cámara de Representantes o por terceros autorizados.

Lineamientos clave:
- Mantener inventario actualizado de los activos físicos y medios de almacenamiento.

- Prevenir accesos no autorizados, daños o pérdidas de medios físicos.
- Aplicar controles de almacenamiento seguro para medios removibles.
- Establecer procesos de destrucción segura de medios que contengan información sensible o reservada.
- Aplicar la política de escritorio despejado y pantalla despejada en todas las áreas de trabajo.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.37 Procedimientos operacionales documentados
- A.7.5 Protección contra amenazas físicas y ambientales
- A.7.6 Trabajar en áreas seguras
- A.7.7 Escritorio despejado y pantalla despejada
- A.7.8 Ubicación y protección del equipo
- A.7.9 Seguridad de los activos fuera de las instalaciones
- A.7.10 Medios de almacenamiento
- A.7.11 Servicios de apoyo

5.4 Controles tecnológicos

Incluye políticas orientadas a la gestión segura de tecnologías de la información, sistemas, redes y datos.

PA14 – Control de acceso lógico

Definición:

Establece los lineamientos para controlar el acceso a sistemas, redes, aplicaciones y datos institucionales, asegurando que solo usuarios autorizados puedan acceder a los recursos de información según su rol.

Alcance:

Aplica a todos los sistemas de información, plataformas, aplicaciones y servicios tecnológicos utilizados en la Cámara de Representantes.

Lineamientos clave:

- Asignar accesos de acuerdo con los principios de mínima autoridad (least privilege) y necesidad de conocer (need-to-know).
- Gestionar credenciales de forma segura, incluyendo autenticación fuerte y multifactor cuando aplique.
- Establecer procedimientos formales para altas, modificaciones y bajas de usuarios.
- Monitorear y revisar periódicamente los permisos y cuentas activas.
- Aplicar controles especiales a cuentas privilegiadas y de servicio.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.15 Control de acceso
- A.5.16 Gestión de la identidad
- A.5.17 Información de autenticación
- A.5.37 Procedimientos operacionales documentados
- A.8.2 Derechos de acceso privilegiado
- A.8.3 Restricción de acceso a la información
- A.8.5 Autenticación segura
- A.8.11 Enmascaramiento de datos

PA15 – Gestión de activos de información

Definición:

Establece los lineamientos para identificar, clasificar, mantener y proteger los activos de información de la Cámara de Representantes a lo largo de su ciclo de vida.

Alcance:

Aplica a todos los activos relacionados con la información, incluyendo datos, aplicaciones, infraestructura tecnológica, documentación y servicios de la Entidad.

Lineamientos clave:

- Mantener un inventario actualizado de activos de información.
- Asignar responsables (custodios y propietarios) a cada activo para su gestión.
- Aplicar controles adecuados según la clasificación y criticidad del activo.
- Preservar la protección de los activos durante cambios, traslado o baja.
- Articular el inventario de activos con la matriz de riesgos y el SGSI.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.9 Inventario de activos de información y otros asociados a la misma
- A.5.10 Uso aceptable de activos de información y otros asociados a la misma
- A.5.37 Procedimientos operacionales documentados
- A.8.1 Dispositivos de punto final de usuario

PA16 – Seguridad en redes y comunicaciones

Definición:

Establece los controles para proteger la infraestructura de red y las comunicaciones de datos institucionales contra accesos no autorizados, alteraciones o pérdidas.

Alcance:

Aplica a todas las redes internas, conexiones remotas, canales de comunicación, servicios en la nube y medios utilizados para la transmisión de información en la Cámara de Representantes.

Lineamientos clave:

- Segmentar la red y aplicar controles de acceso a nivel de red y dispositivos.
- Proteger las comunicaciones mediante cifrado y autenticación cuando sea requerido.
- Monitorear el tráfico y los eventos de red para detectar actividades anómalas.
- Asegurar las configuraciones de routers, switches, firewalls y puntos de acceso inalámbricos.
- Implementar redundancia para servicios críticos como streaming de plenarias y comisiones.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.37 Procedimientos operacionales documentados
- A.8.6 Gestión de la capacidad
- A.8.14 Redundancia de las instalaciones de procesamiento de información
- A.8.20 Seguridad en redes
- A.8.21 Seguridad de los servicios de red
- A.8.22 Segregación de redes

PA17 – Protección contra software malicioso

Definición:

Establece las medidas para prevenir, detectar y responder ante la presencia de software malicioso que pueda comprometer la seguridad de los sistemas y la información de la Cámara de Representantes.

Alcance:
Aplica a todos los dispositivos, servidores, estaciones de trabajo, sistemas de información y redes de la Entidad.

Lineamientos clave:

- Implementar soluciones antimalware y capacidades avanzadas de detección y respuesta actualizadas en los equipos institucionales.
- Restringir la ejecución de software no autorizado o proveniente de fuentes no confiables.
- Configurar políticas de protección en correo electrónico y navegación web.
- Monitorear eventos y alertas para responder a infecciones o intentos de ataque.
- Aplicar controles específicos contra ransomware y amenazas avanzadas persistentes (APT).

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.37 Procedimientos operacionales documentados
- A.8.7 Protección contra malware
- A.8.8 Gestión de vulnerabilidades técnicas

PA18 – Copias de seguridad y restauración

Definición:
Establece los lineamientos para realizar y gestionar copias de seguridad de la información crítica, asegurando su disponibilidad y recuperación ante pérdida o incidente.

Alcance:
Aplica a todos los sistemas, bases de datos, archivos y configuraciones relevantes para la operación de la Cámara de Representantes.

Lineamientos clave:

- Definir y aplicar una política de respaldos con periodicidad adecuada según la criticidad.
- Verificar regularmente la integridad y restauración de las copias mediante pruebas.
- Almacenar respaldos en ubicaciones seguras, preferiblemente fuera del sitio principal.
- Proteger las copias mediante cifrado y control de acceso.

- Aplicar el esquema 3-2-1 (tres copias, dos medios distintos, una externa) en activos críticos.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.37 Procedimientos operacionales documentados
- A.8.13 Copia de seguridad de la información

PA19 – Uso de criptografía y autenticación

Definición:

Establece los lineamientos para proteger la información mediante el uso adecuado de técnicas criptográficas y mecanismos de autenticación, preservando la confidencialidad, integridad y control de acceso.

Alcance:

Aplica a todos los sistemas, servicios, plataformas y dispositivos de la Cámara de Representantes que gestionen información sensible o realicen intercambio de datos.

Lineamientos clave:

- Utilizar algoritmos criptográficos robustos y actualizados, alineados con estándares y buenas prácticas internacionales vigentes para la protección de la información.
- Proteger las claves criptográficas mediante almacenamiento seguro y controles de acceso.
- Establecer autenticación multifactor (MFA) en servicios críticos, accesos remotos y cuentas privilegiadas.
- Documentar y revisar periódicamente las políticas de cifrado, gestión de llaves y autenticación.
- Aplicar firma electrónica conforme a la Ley 527 de 1999 cuando sea requerido.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.37 Procedimientos operacionales documentados
- A.8.3 Restricción de acceso a la información
- A.8.24 Uso de criptografía

PA20 – Inteligencia de amenazas

Definición:

Establece los lineamientos para identificar, recopilar, analizar y utilizar información relevante sobre amenazas de seguridad que puedan afectar a la Cámara de Representantes, con el fin de anticiparse y fortalecer la postura defensiva.

Alcance:
Aplica a todas las áreas encargadas de la seguridad de la información, incluyendo monitoreo, análisis, respuesta y gestión del riesgo.

Lineamientos clave:

- Obtener inteligencia de amenazas de fuentes internas y externas confiables (CSIRT Gobierno, ColCERT, MinTIC, entre otros).
- Establecer procesos para analizar y filtrar indicadores de compromiso (IoC).
- Incorporar la inteligencia de amenazas en la evaluación de riesgos y en la toma de decisiones.
- Actualizar y compartir información relevante con las partes interesadas pertinentes.
- Considerar amenazas específicas al sector legislativo y gubernamental.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.7 Inteligencia de amenazas
- A.5.25 Evaluación y decisión sobre los eventos de seguridad de la información
- A.5.37 Procedimientos operacionales documentados

PA21 – Seguridad en la gestión de proyectos

Definición:
Define los principios que aseguran la incorporación de requisitos de seguridad de la información en todas las fases del ciclo de vida de los proyectos institucionales.

Alcance:
Aplica a todos los proyectos institucionales que involucren sistemas, servicios o procesos que usen información de la Cámara de Representantes.

Lineamientos clave:

- Identificar requisitos de seguridad desde la planificación del proyecto.
- Articular con la metodología de gestión de proyectos institucional.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.8 Seguridad de la información en la gestión de proyectos

PA22 – Filtrado web y uso aceptable de Internet

Definición:
Regula el acceso a contenidos web a través de mecanismos de filtrado y establece criterios de uso aceptable de Internet en los equipos de la Cámara de Representantes.

Alcance:
Aplica a todos los usuarios, dispositivos y redes que utilicen acceso a Internet desde los sistemas institucionales.

Lineamientos clave:

- Bloquear sitios maliciosos o que representen riesgos de seguridad.
- Establecer categorías de contenido permitidas y restringidas.
- Monitorear el uso de Internet para detectar abusos o incidentes.
- Sensibilizar a los usuarios sobre las consecuencias del uso indebido.
- Permitir excepciones justificadas mediante procedimiento formal.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.37 Procedimientos operacionales documentados
- A.8.23 Filtrado web

PA23– Supervisión, monitoreo y gestión de incidentes

Definición:
Establece los mecanismos para registrar, supervisar y analizar las actividades que afectan la seguridad de la información dentro de los sistemas institucionales, así como para gestionar los incidentes de seguridad.

Alcance:
Aplica a todos los sistemas, procesos y usuarios que interactúan con activos de información.

Lineamientos clave:

- Implementar registros de auditoría (logs) en sistemas críticos.
- Establecer herramientas y procedimientos de monitoreo continuo (SIEM, SOC).
- Definir alertas e indicadores para detectar eventos anómalos.
- Revisar los registros periódicamente para mejorar la detección de incidentes.
- Establecer procedimiento formal de gestión de incidentes alineado con NTC ISO/IEC 27035.

- Reportar incidentes graves al CSIRT Gobierno y, cuando aplique, a la Superintendencia de Industria y Comercio.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información
- A.5.25 Evaluación y decisión sobre los eventos de seguridad de la información
- A.5.26 Respuesta a los incidentes de seguridad de la información
- A.5.27 Aprendizaje sobre los incidentes de seguridad de la información
- A.5.28 Recopilación de pruebas
- A.5.33 Protección de registros
- A.5.37 Procedimientos operacionales documentados
- A.6.8 Reportes de eventos de seguridad de la información
- A.8.12 Prevención de fuga de datos
- A.8.15 Registro
- A.8.16 Actividades de seguimiento

PA24 – Seguridad en servicios en la nube

Definición:

Define los lineamientos para preservar la protección de la información institucional cuando se adquieren o utilizan servicios de computación en la nube.

Alcance:

Aplica a todos los servicios contratados o utilizados por la Cámara de Representantes que se ejecuten en plataformas de nube pública, privada o híbrida.

Lineamientos clave:

- Establecer cláusulas contractuales que aseguren la protección de la información, incluyendo localización de datos.
- Asegurar que el proveedor implemente controles alineados con estándares y buenas prácticas internacionales de seguridad de la información.
- Cifrar la información almacenada o procesada en la nube.
- Evaluar la seguridad y cumplimiento del proveedor antes de la contratación.

- Aplicar las directrices del MinTIC sobre adopción de servicios en la nube en el sector público.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.23 Seguridad de la información para el uso de servicios en la nube
- A.5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información
- A.5.37 Procedimientos operacionales documentados

PA25 – Eliminación y destrucción segura de información

Definición:

Establece los mecanismos para eliminar o destruir de forma segura información y medios de almacenamiento cuando ya no sean necesarios.

Alcance:

Aplica a todos los dispositivos, documentos y medios que contengan información sensible o institucional.

Lineamientos clave:

- Utilizar herramientas y procedimientos certificados para la eliminación de datos (borrado seguro, desmagnetización, destrucción física).
- Documentar la destrucción de medios críticos mediante actas.
- Asegurar que terceros contratados para destrucción cumplan con requisitos de seguridad.
- Capacitar al personal en las prácticas seguras de eliminación de información.
- Articular la eliminación con las Tablas de Retención Documental y la normatividad archivística.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.37 Procedimientos operacionales documentados
- A.7.14 Eliminación segura o reutilización de equipos
- A.8.10 Eliminación de información

PA26 – Pruebas de seguridad técnica y validación de cambios

Definición:

Define los criterios para realizar pruebas técnicas de seguridad en sistemas y para validar que los cambios no introduzcan nuevas vulnerabilidades.

Alcance:
Aplica a todos los sistemas, aplicaciones e infraestructuras sujetas a mantenimiento, desarrollo o mejora.

Lineamientos clave:

- Ejecutar pruebas de penetración (pentesting) y escaneo de vulnerabilidades regularmente.
- Realizar pruebas después de cambios mayores en infraestructura o aplicaciones.
- Documentar y mitigar los hallazgos de seguridad mediante planes de remediación.
- Asegurar que el entorno de pruebas esté separado del de producción.
- Proteger los sistemas durante las pruebas de auditoría minimizando impactos operacionales.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.29 Seguridad de la información durante interrupciones
- A.5.37 Procedimientos operacionales documentados
- A.8.31 Separación de los entornos de desarrollo, prueba y producción
- A.8.34 Protección de sistemas de información durante pruebas de auditoría

PA27 – Gestión de configuraciones y control de software

Definición:
Establece los lineamientos para mantener configuraciones seguras y controlar la instalación de software en los sistemas institucionales.

Alcance:
Aplica a todos los equipos, servidores, redes y sistemas operativos de la Cámara de Representantes.

Lineamientos clave:

- Establecer configuraciones base seguras (hardening baselines) para cada tipo de sistema.
- Controlar la instalación de software con listas blancas o sistemas de aprobación.
- Prohibir el uso de software no autorizado o sin licenciamiento.
- Revisar y actualizar las configuraciones regularmente.
- Aplicar gestión centralizada de configuraciones mediante GPO o herramientas equivalentes.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.37 Procedimientos operacionales documentados

- A.8.9 Gestión de la configuración

PA28 – Registros, sincronización y continuidad TIC

Definición:

Establece los lineamientos para la generación, gestión, monitoreo y protección de registros técnicos asociados a eventos de seguridad, actividades de usuario, sincronización de sistemas y control del uso de software y programas privilegiados, así como la preparación de las TIC para la continuidad de negocio.

Alcance:

Aplica a todos los sistemas, servidores, estaciones de trabajo y dispositivos que hagan parte de la infraestructura tecnológica de la Cámara de Representantes.

Lineamientos clave:

- Elaborar, conservar y revisar periódicamente los registros que documenten actividades de los usuarios, eventos de seguridad, fallas y excepciones.
- Generar y analizar registros que incluyan actividades relevantes para la seguridad, incluyendo fallas, excepciones y eventos operativos.
- Mantener todos los sistemas sincronizados con una fuente única y confiable de tiempo (NTP).
- El uso de programas con privilegios elevados debe estar estrictamente restringido y controlado.
- La instalación de software en sistemas operativos debe estar sujeta a procedimientos definidos y autorizaciones formales.
- Mantener planes de continuidad TIC alineados con el plan de continuidad institucional, preservando la operatividad del proceso legislativo.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.27 Aprendizaje sobre los incidentes de seguridad de la información
- A.5.30 Preparación de las TIC para la continuidad de negocio
- A.5.37 Procedimientos operacionales documentados
- A.8.6 Gestión de la capacidad
- A.8.15 Registro
- A.8.16 Actividades de seguimiento

- A.8.17 Sincronización del reloj
- A.8.18 Uso de programas de utilidad privilegiados
- A.8.19 Instalación de software en sistemas operativos
- A.8.34 Protección de sistemas de información durante pruebas de auditoría

5.5 Políticas adicionales de privacidad y continuidad

Las siguientes políticas complementan los cuatro grupos de controles del Anexo A de la NTC ISO/IEC 27001:2022 y profundizan los aspectos de privacidad de la información, continuidad del proceso legislativo y definición de tiempos objetivo de recuperación, atendiendo la naturaleza misional de la Cámara de Representantes.

PA29 – Privacidad y protección de datos personales

Definición:

Establece los lineamientos para preservar el tratamiento adecuado de los datos personales que la Cámara de Representantes recolecta, almacena, usa, circula, transmite o suprime, asegurando el cumplimiento de la Ley 1581 de 2012, el Decreto 1377 de 2013, las Circulares de la Superintendencia de Industria y Comercio (SIC) y los principios de privacidad por diseño y por defecto.

Alcance:

Aplica a todas las bases de datos personales bajo responsabilidad de la Cámara de Representantes, incluyendo las relacionadas con Honorables Representantes, funcionarios, contratistas, ciudadanos peticionarios, asistentes a sesiones y participantes en eventos institucionales, así como a los encargados del tratamiento contratados por la Entidad.

Lineamientos clave:

- Mantener actualizada la inscripción de las bases de datos personales en el Registro Nacional de Bases de Datos (RNBD) de la SIC.
- Publicar y mantener vigentes la Política de Tratamiento de Datos Personales y los avisos de privacidad en los canales institucionales.
- Atender las peticiones, quejas, reclamos y consultas (PQRC) de titulares en los plazos legales: diez (10) días hábiles para consultas, prorrogables por cinco (5) días adicionales,

y quince (15) días hábiles prorrogables por ocho (8) adicionales para reclamos, conforme a la Ley 1581 de 2012.

- Suscribir contratos de transmisión y transferencia de datos personales con encargados del tratamiento, incluyendo cláusulas mínimas exigidas por la SIC.
- Aplicar los principios de privacidad por diseño y por defecto en todos los proyectos que involucren tratamiento de datos personales.
- Notificar a la SIC los incidentes que afecten datos personales dentro de los quince (15) días calendario siguientes a su detección, conforme a la Circular Externa 002 de 2024 de la SIC.
- Realizar evaluaciones de impacto en la protección de datos (EIPD) para tratamientos de alto riesgo.
- Preservar el ejercicio de los derechos de los titulares: conocer, actualizar, rectificar, suprimir y revocar la autorización.
- Aplicar medidas técnicas y organizativas reforzadas para el tratamiento de datos sensibles y de menores de edad.
- Mantener trazabilidad de las autorizaciones de tratamiento obtenidas de los titulares.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.34 Privacidad y protección de la PII
- A.5.14 Transferencia de información
- A.5.31 Requisitos legales, estatutarios, regulatorios y contractuales
- A.5.37 Procedimientos operacionales documentados
- A.8.11 Enmascaramiento de datos
- A.8.12 Prevención de fuga de datos

PA30 – Continuidad de negocio y recuperación ante desastres

Definición:

Establece los lineamientos para asegurar la disponibilidad de los procesos críticos, los servicios tecnológicos y la información de la Cámara de Representantes ante eventos disruptivos, preservando la continuidad del proceso legislativo, la capacidad de respuesta ante incidentes mayores y la recuperación oportuna de las operaciones, en alineación con la norma NTC ISO 22301:2019.

Alcance:

Aplica a todos los procesos misionales, estratégicos y de apoyo de la Cámara de Representantes, así como a la infraestructura tecnológica, sistemas de información, instalaciones físicas y servicios provistos por terceros que soporten la operación institucional, incluyendo sesiones plenarias, comisiones, votaciones y publicación de actos legislativos.

Lineamientos clave:

- Elaborar y mantener actualizado el Plan de Continuidad de Negocio (BCP) y el Plan de Recuperación ante Desastres (DRP) institucionales.
- Realizar el Análisis de Impacto al Negocio (BIA) para identificar procesos críticos, dependencias y tiempos máximos tolerables de interrupción (MTPD).
- Definir, documentar y aprobar los tiempos objetivo de recuperación (RTO) y el punto objetivo de recuperación (RPO) por cada proceso y sistema crítico.
- Establecer y mantener sitios alternos de operación y centros de datos secundarios para servicios críticos como votación electrónica, streaming de plenarias y publicación de actos.
- Ejecutar pruebas anuales del BCP/DRP, incluyendo simulacros funcionales y técnicos, y documentar lecciones aprendidas.
- Coordinar la continuidad TIC con la continuidad institucional liderada por la Alta Dirección y la Oficina de Planeación y Sistemas.
- Establecer estrategias de comunicación durante crisis hacia Honorables Representantes, funcionarios, ciudadanía y medios.
- Articular el BCP con los planes de manejo de emergencias y los protocolos de seguridad física del Capitolio Nacional y del Edificio Nuevo del Congreso.
- Mantener acuerdos con proveedores críticos para preservar la disponibilidad de servicios en escenarios de contingencia.
- Revisar el BCP/DRP al menos anualmente o tras cambios significativos en la operación o luego de incidentes mayores.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.29 Seguridad de la información durante interrupciones
- A.5.30 Preparación de las TIC para la continuidad de negocio
- A.5.37 Procedimientos operacionales documentados
- A.8.13 Copia de seguridad de la información
- A.8.14 Redundancia de las instalaciones de procesamiento de información

PA31 – Tiempos objetivo de recuperación (RTO/RPO) para activos críticos

Definición:

Establece los tiempos máximos de recuperación (RTO) y los puntos máximos de pérdida de información tolerable (RPO) por categoría de activo de información, como referencia base para el diseño de respaldos, redundancia, contingencia y continuidad operativa de los servicios de la Cámara de Representantes.

Alcance:

Aplica a los sistemas de información, bases de datos, servicios tecnológicos y aplicaciones que soporten procesos misionales, estratégicos y de apoyo de la Entidad. Los valores aquí establecidos constituyen un mínimo de referencia y pueden ser refinados en el BIA con base en la criticidad específica de cada activo.

Lineamientos clave:

- Categoría CRÍTICA (sistemas de votación, gestión legislativa, streaming de plenarias): RTO objetivo ≤ 2 horas y RPO objetivo ≤ 15 minutos. .
- Categoría ALTA (correo institucional, gestión documental, portal web, intranet): RTO ≤ 8 horas, RPO ≤ 1 hora.
- Categoría MEDIA (sistemas administrativos, contabilidad, gestión de personal): RTO ≤ 24 horas, RPO ≤ 4 horas.
- Categoría BAJA (sistemas de apoyo no críticos, herramientas de productividad estándar): RTO ≤ 72 horas, RPO ≤ 24 horas.
- Los responsables de cada sistema deben validar y aprobar los RTO/RPO aplicables a sus servicios.
- Los proveedores de servicios en la nube deben acreditar contractualmente niveles de servicio (SLA) consistentes con los RTO/RPO definidos.
- Cualquier excepción debe ser autorizada por el Oficial de Seguridad de la Información y aprobada por la Alta Dirección.

Controles relacionados del Anexo A – NTC ISO/IEC 27001:2022:

- A.5.29 Seguridad de la información durante interrupciones
- A.5.30 Preparación de las TIC para la continuidad de negocio
- A.8.13 Copia de seguridad de la información
- A.8.14 Redundancia de las instalaciones de procesamiento de información

6. VIGENCIA, REVISIÓN Y MEJORA

El presente Manual de Políticas de Seguridad y Privacidad de la Información entra en vigencia a partir de su aprobación por la instancia institucional competente de la Cámara de Representantes y su publicación oficial.

El contenido del manual será revisado al menos una vez al año, o cuando ocurran cambios significativos en los riesgos, procesos, tecnologías, estructura organizacional o normatividad aplicable. Las revisiones podrán ser solicitadas por la Alta Dirección, el Oficial de Seguridad de la Información, la Oficina de Planeación y Sistemas o como resultado de auditorías internas y externas.

Las políticas contenidas en este manual podrán ser ajustadas por recomendación del Oficial de Seguridad de la Información y deberán conservar su alineación con el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC y la norma NTC ISO/IEC 27001:2022.

La mejora continua del SGSI se materializa a través del ciclo PHVA (Planear-Hacer-Verificar-Actuar), con base en los resultados del monitoreo, las auditorías, las revisiones por la Dirección, los incidentes registrados y las acciones correctivas y preventivas implementadas.

7. APROBACIÓN Y RESPONSABLES DEL DOCUMENTO

El presente Manual de Políticas de Seguridad y Privacidad de la Información de la Cámara de Representantes ha sido elaborado, revisado y aprobado por las instancias institucionales que se relacionan a continuación, en concordancia con el Sistema Integrado de Gestión y los procedimientos institucionales para la formalización de documentos del Sistema de Gestión de Seguridad de la Información (SGSI).

Responsables permanentes del documento:

- Propietario del documento: Oficina de Planeación y Sistemas.
- Custodio técnico: Oficial de Seguridad de la Información (OSI).
- Responsable de actualización: Oficial de Seguridad de la Información en coordinación con los líderes de proceso.
- Responsable de divulgación: Oficina de Planeación y Sistemas, con apoyo de la División de Personal y la Oficina de Comunicaciones.

8. CONTROL DE CAMBIOS

Fecha	Versión	Descripción de los cambios
01/04/2024	01	Versión inicial del Manual de Políticas de Seguridad y Privacidad de la Información de la Cámara de Representantes.
28/05/2026	02	Actualización integral del manual conforme a la NTC ISO/IEC 27001:2022, el MSPI Versión 5 (Resolución 02277 de 2025 del MinTIC) y las disposiciones normativas vigentes en materia de seguridad y privacidad de la información. Reestructuración por dominios de control del Anexo A: organizacionales, de personas, físicos y tecnológicos. Incorporación de 31 políticas específicas (PA01–PA31).

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