RESOLUCIÓN 0289 DE 25 MAY 2026

"Por medio de la cual se actualiza la Política del Sistema de Gestión de Seguridad de la Información en el Ministerio de Vivienda, Ciudad y Territorio"

LA MINISTRA DE VIVIENDA, CIUDAD Y TERRITORIO (E)

En ejercicio de sus facultades constitucionales y legales y en especial las conferidas en el numeral 11 del artículo 6 del Decreto Ley 3571 de 2011, el artículo 2.2.9.1.1.2 del Decreto 1078 de 2015 subrogado por el Decreto 1008 de 2018, y

CONSIDERANDO

Que el artículo 15 de la Constitución Política consagra el derecho de todas las personas a su intimidad personal y familiar, a su buen nombre, y a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bancos de datos y archivos de entidades públicas y privadas.

Que la Ley 1341 de 2009, "*Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones*", estableció el marco general del sector de las Tecnologías de la Información y las Comunicaciones, e indicó que, estas deben servir al interés general, siendo deber del Estado promover su acceso eficiente y en igualdad de oportunidades para todos los habitantes del territorio nacional.

Que el artículo 4 de la Ley 1341 de 2009 establece que, el Estado intervendrá en el sector de las Tecnologías de la Información y las Comunicaciones, entre otros fines, para promover condiciones de seguridad del servicio al usuario final e incentivar acciones preventivas y de seguridad informática y de redes para el desarrollo del sector.

Que el Decreto Ley 019 de 2012 "*Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública*", establece en su artículo 4 que, las autoridades deben incentivar el uso de las tecnologías de la información y las comunicaciones, con el fin que, los procesos administrativos se adelanten con diligencia, dentro de los términos legales y sin dilaciones injustificadas.

Que la Ley Estatutaria 1581 de 2012 "*Por la cual se dictan disposiciones generales para la protección de datos personales*" y el artículo 2.2.2.25.3.1 del Decreto 1074 de 2015, Único Reglamentario del Sector Comercio, Industria y Turismo, prevén la necesidad de garantizar de forma integral la protección del derecho fundamental de habeas data y establecen dentro de los deberes de los responsables del tratamiento de datos personales, el desarrollo de políticas para garantizar dicho derecho.

Que la Ley 1712 de 2014, "*Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional*", así como lo dispuesto en el Libro 2, Parte 8, Título 4 del Decreto 1080 de 2015, relacionado con la gestión de la información clasificada y reservada, establecen directrices e instrumentos para la adecuada gestión de la información pública.

RESOLUCIÓN 0289 DE 25 MAY 2026

Que el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, modificado por el Decreto 1499 de 2017, consagra el Modelo Integrado de Planeación y Gestión - MIPG, el cual articula el Sistema de Gestión con el Sistema de Control Interno.

Que el artículo 2.2.22.2.1 del Decreto 1083 de 2015 señala las políticas de Gestión y Desempeño Institucional, entre las cuales se encuentran las de Gobierno Digital y Seguridad Digital.

Que el Decreto 1078 de 2015, Único Reglamentario del Sector TIC, compiló los lineamientos de la Política de Gobierno Digital. Así mismo el artículo 2.2.9.1.2.1 del citado decreto, subrogado por el artículo 1 del Decreto 767 de 2022, estableció como uno de los habilitadores de esta política la Seguridad y Privacidad de la Información, orientada al fortalecimiento de las capacidades institucionales para garantizar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Que, mediante la Resolución 500 de 2021, el Ministerio de Tecnologías de la Información y las Comunicaciones estableció los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la información, el procedimiento para la gestión de incidentes de seguridad digital y los lineamientos y estándares para la estrategia de seguridad digital de los sujetos obligados.

Que mediante la Resolución 02277 del 03 de junio de 2025 el Ministerio de Tecnologías de la Información y las Comunicaciones actualizó el Anexo 1 de la Resolución 500 de 2021, relativo al Modelo de Seguridad y Privacidad de la Información - MSPI y derogó las disposiciones que le sean contrarias o que regulen de manera incompatible la misma materia.

Que el artículo 5 de la Resolución 500 de 2021 dispone que, los sujetos obligados deben adoptar una estrategia de seguridad digital integrada por principios, políticas, procedimientos, guías, manuales, formatos y lineamientos, la cual debe incorporarse al Plan de Seguridad y Privacidad de la Información y articularse con el Modelo de Seguridad y Privacidad de la Información - MSPI como habilitador de la Política de Gobierno Digital.

Que el Documento CONPES 3854 de 2016 estableció la Política Nacional de Seguridad Digital y el Documento CONPES 3995 de 2020 formuló la Política Nacional de Confianza y Seguridad Digital, orientadas al fortalecimiento de capacidades para identificar, gestionar, tratar y mitigar riesgos de seguridad digital en el entorno digital.

Que el parágrafo del artículo 16 del Decreto 2106 de 2019 dispone que las autoridades que realicen trámites, procesos y procedimientos por medios digitales deberán contar con una estrategia de seguridad digital, de conformidad con los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

RESOLUCIÓN 0289 DE 25 MAY 2026

Que el Ministerio de Vivienda, Ciudad y Territorio, en desarrollo de sus funciones y en cumplimiento de las disposiciones legales y reglamentarias que regulan la gestión de la información, la seguridad digital, la protección de datos personales, la continuidad de la operación y el uso de medios digitales, requiere actualizar su política de seguridad de la información para fortalecer la protección de sus activos de información, la gestión de riesgos y la prestación continua y segura de sus servicios.

Que mediante la Resolución 0331 de 2021, el "*Por la cual se actualiza la Política del Sistema de Gestión de Seguridad de la Información en el Ministerio de Vivienda, Ciudad y Territorio*".

Que, por lo anterior, se hace necesario derogar la Resolución 0331 de 2021, de igual manera definir los objetivos y el ámbito de aplicación del Sistema de Seguridad de la Información en el Ministerio de Vivienda, Ciudad y Territorio, en el marco de la estrategia del Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información formulados por el Ministerio de Tecnología de Información y Comunicaciones.

Qué, en mérito de lo expuesto,

RESUELVE

Artículo 1. Objetivo. Establecer los lineamientos y directrices definidos por la Alta Dirección del Ministerio de Vivienda, Ciudad y Territorio –MVCT– en materia de seguridad y privacidad de la información, seguridad digital y la continuidad de la operación de los servicios tecnológicos, en concordancia con el Modelo de Seguridad y Privacidad de la Información –MSPI–, las políticas de Seguridad Digital y de Gobierno Digital, los requisitos legales y reglamentarios aplicables y las necesidades de las partes interesadas, con el propósito de salvaguardar la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y privacidad de la información y garantizar la prestación oportuna y confiable de los servicios a la ciudadanía, así como garantizar la prestación oportuna, continua y confiable de los servicios a la ciudadanía.

Artículo 2 – Definiciones.

- **Activo de información:** Cualquier información, sistema, servicio, infraestructura, soporte o persona que tiene valor para la organización y participa en el tratamiento de datos.
- **Autenticidad:** Propiedad que garantiza que una entidad, dato o transacción es genuina y que su origen es verificable.
- **Brecha de seguridad:** Materialización de una vulnerabilidad que provoca acceso, uso, divulgación, modificación o destrucción no autorizada de información o interrupción de servicios.
- **Cloud Computing (Computación en la nube):** Uso de servicios informáticos (servidores, almacenamiento, software) a través de internet, sin necesidad de infraestructura propia.
- **Confidencialidad:** Propiedad de la información por la cual se garantiza que solo es accesible a personas, procesos o sistemas debidamente autorizados.

- **Continuidad del negocio:** Capacidad de la entidad para mantener o restablecer sus procesos y servicios esenciales ante eventos disruptivos, mediante planes de continuidad y recuperación.
- **Disponibilidad:** Propiedad de la información y de los servicios que asegura su acceso y uso oportuno y fiable cuando es requerido por los usuarios autorizados.
- **Evento de seguridad de la información:** Ocurrencia identificable en sistemas, redes o servicios que puede indicar un posible incumplimiento de la política de seguridad o fallo de los controles.
- **Incidente de seguridad digital:** Violación o amenaza inminente a la confidencialidad, integridad o disponibilidad de sistemas de información o datos, que exige acciones de respuesta y recuperación.
- **Información personal (datos personales):** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables, cuyo tratamiento se sujeta a la normativa de protección de datos.
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud, protegiéndola contra modificaciones no autorizadas o no detectadas.
- **Modelo de Seguridad y Privacidad de la Información (MSPI):** Marco definido por MinTIC que establece lineamientos, fases y controles para gestionar la seguridad, privacidad de la información y seguridad digital en entidades públicas.
- **On Premise (En Local):** modelo donde los sistemas y datos se alojan y gestionan en la infraestructura física propia de la organización (servidores locales
- **Parte interesada:** Persona, grupo u organización que puede afectar, verse afectada o percibirse como afectada por las decisiones o resultados del SGSI y de la Política.
- **Política de seguridad de la información:** Directriz de alto nivel emitida por la Alta Dirección que define objetivos, principios, lineamientos y responsabilidades para proteger la información y sus activos asociados.
- **Riesgo de seguridad de la información:** Combinación de la probabilidad de que una amenaza explote una vulnerabilidad y de las consecuencias sobre los activos de información.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, incluyendo otras propiedades como autenticidad, trazabilidad y no repudio.
- **Seguridad digital:** Gestión de riesgos y medidas para proteger la información, los servicios y la infraestructura en entornos digitales, incluyendo ciberseguridad y protección de datos en línea.
- **Sistema de Gestión de Seguridad de la Información (SGSI):** Conjunto de políticas, procedimientos, recursos y procesos interrelacionados para gestionar de forma sistemática los riesgos de seguridad de la información en la organización.
- **Security/Privacy by Design (Seguridad y privacidad desde el diseño):** enfoque proactivo que integra medidas de protección de datos y ciberseguridad desde el diseño inicial de sistemas y procesos, no como algo añadido después.
- **Trazabilidad:** Capacidad de seguir el rastro de actividades, accesos y cambios realizados sobre la información y los sistemas, mediante registros y evidencias que permitan su análisis posterior.

- **Tratamiento de riesgos:** Proceso de seleccionar e implementar medidas para modificar el riesgo, ya sea mitigándolo, evitándolo, transfiriéndolo o aceptándolo de forma informada.
- **Vulnerabilidad:** Debilidad o fallo en procesos, personas, tecnologías o controles que puede ser explotada por una amenaza para afectar la seguridad de la información.
- **Zero Trust (Confianza Cero):** Enfoque de arquitectura de seguridad que asume que ninguna entidad es confiable por defecto y exige verificación continua y acceso con privilegios mínimos a recursos y servicios.

Artículo 3. Política general de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos. El Ministerio de Vivienda, Ciudad y Territorio –MVCT–, mediante la adopción, implementación, mantenimiento y mejora continua de su Sistema de Gestión de Seguridad de la Información (SGSI), articulado con el Sistema Integrado de Gestión (SIG) y alineado con el Modelo de Seguridad y Privacidad de la Información –MSPI– definido por el Ministerio de Tecnologías de la Información y las Comunicaciones , se compromete a proteger la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y privacidad de la información que gestiona en sus procesos, trámites y servicios. Así mismo, el Ministerio de Vivienda, Ciudad y Territorio –MVCT– promoverá una cultura de seguridad y protección de la información, gestionará los riesgos asociados a los activos de información y a los servicios tecnológicos, fortalecerá la seguridad digital y garantizará la continuidad de la operación institucional, en cumplimiento de la normativa aplicable con el fin de asegurar la prestación oportuna, confiable y segura de los servicios a la ciudadanía.
Con el firme propósito de garantizar la alta disponibilidad, continuidad y confiabilidad de sus servicios frente a la ciudadanía y grupos de interés, el Ministerio de Vivienda, Ciudad y Territorio – MVCT aplicará un enfoque integral para la gestión de los riesgos asociados a la seguridad y privacidad de la información, la seguridad digital y la continuidad de la operación. Para materializar este compromiso, el Ministerio:

- Establecerá controles organizacionales, administrativos, físicos y tecnológicos de vanguardia, proporcionales al riesgo, priorizando la redundancia y la tolerancia a fallos en la infraestructura crítica.
- Desarrollará planes de contingencia y recuperación ante desastres (DRP) probados periódicamente, asegurando la continuidad del negocio (BCP) ante cualquier incidente disruptivo.
- Fortalecerá las capacidades para prevenir, detectar y responder ágilmente a incidentes de ciberseguridad, minimizando cualquier impacto en la prestación de los servicios.
- Garantizará el estricto cumplimiento de los requisitos legales, reglamentarios, técnicos y contractuales vigentes aplicables al MVCT.
- Velará por la protección de los activos de información y la adecuada gestión de los servicios tecnológicos durante todo su ciclo de vida.

Artículo 3.1. Objetivos de la Política general de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos. La Política tendrá, los siguientes objetivos:

1. Definir y formalizar los lineamientos normativos y de gestión relacionados con la protección de la información y la seguridad digital en el MVCT.
2. Facilitar la gestión integral de los riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios del Ministerio.
3. Reducir la probabilidad e impacto de los incidentes de seguridad y privacidad de la información y de seguridad digital, mediante controles preventivos, detectivos y correctivos eficaces.
4. Establecer mecanismos de aseguramiento físico y digital que fortalezcan la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información institucional.
5. Definir lineamientos para el manejo de la información física y digital, articulados con la gestión documental y la normativa sobre transparencia, acceso a la información y archivos.
6. Impulsar un cambio organizacional mediante la concienciación y apropiación de la seguridad y privacidad de la información y la seguridad digital por parte de todos los colaboradores.
7. Garantizar el cumplimiento de los requisitos legales, reglamentarios, regulatorios, contractuales y de normas técnicas colombianas en materia de seguridad y privacidad de la información, seguridad digital y protección de datos personales.
8. Asegurar la integralidad de los atributos de seguridad de la información, mediante el establecimiento de mecanismos de seguridad desde el diseño y por defecto (Security/Privacy by Design) tanto en entornos físicos como tecnológicos —incluyendo infraestructuras híbridas y en la nube—, para garantizar la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y privacidad de los activos de información del MVCT.
9. Gestionar de manera segura el ciclo de vida del dato, definiendo e implementando directrices para el manejo seguro de la información desde su creación hasta su disposición final, garantizando su articulación armónica con los procesos de gestión documental, las políticas de transparencia activa, el acceso a la información pública y el cumplimiento estricto de la Ley de Protección de Datos Personales.

Artículo 4. Compromiso de la Alta Dirección. La Alta Dirección del Ministerio de Vivienda, Ciudad y Territorio se compromete a liderar, apoyar y promover el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI); así mismo, se compromete a revisar el avance de la implementación del SGSI de manera periódica y también garantizará los recursos suficientes (tecnológicos y talento humano calificado) para implementar y mantener el sistema, así mismo, incluirá dentro de las decisiones estratégicas, la seguridad de la información.

Artículo 5. Alcance. El alcance de la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios Tecnológicos del Ministerio de Vivienda, Ciudad y Territorio - MVCT es de estricto cumplimiento y aplicación, abarcando de manera integral, los siguientes ámbitos:

RESOLUCIÓN 0289 DE 25 MAY 2026

1. **Gestión Integral de la Información:** La protección y aseguramiento de la seguridad y privacidad de la información generada, procesada, almacenada o transmitida en el marco de la totalidad de los procesos estratégicos, misionales, de apoyo y de evaluación y control de la Entidad.
2. **Seguridad Digital y Tecnológica:** La salvaguarda y aseguramiento cibernético de los servicios digitales, sistemas de información, redes, infraestructura tecnológica (On Premise) y plataformas de servicios en la nube (Cloud Computing) que soportan la operación y la prestación de servicios institucionales.
3. **Continuidad Operativa y Disponibilidad:** La formulación, implementación y mantenimiento de los mecanismos tecnológicos, organizacionales y procedimentales requeridos para garantizar la continuidad del negocio y la alta disponibilidad de los servicios críticos del MVCT frente a incidentes cibernéticos, fallas de infraestructura o eventos disruptivos, asegurando la oportuna recuperación de las operaciones.
4. **Grupos de Interés:** La presente política es de obligatorio cumplimiento para todos los servidores públicos, contratistas, practicantes, terceros, proveedores y demás partes interesadas que tengan acceso, administren o gestionen activos de información o recursos tecnológicos propiedad del MVCT o bajo su custodia.

Artículo 6. Aplicabilidad. La presente Política General de Seguridad y Privacidad de la Información, Seguridad Digital del Ministerio de Vivienda, Ciudad y Territorio, así como sus objetivos, además de los manuales, procedimientos y demás documentos derivados o complementarios son de obligatorio cumplimiento y aplicación para todas las dependencias de este Ministerio, incluyendo a servidores públicos, contratistas, proveedores, terceros y demás partes interesadas que, en ejercicio de sus funciones u obligaciones, accedan, gestionen, procesen, custodien o administren información y servicios tecnológicos de la Entidad.

El incumplimiento de la presente Política general de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos o de sus lineamientos derivados, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad.

Artículo 7. Roles y responsabilidades frente a la Política general de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos:

Comité Institucional de Gestión y Desempeño:

- Orientar la implementación, seguimiento y mejora del SGSI y de la presente Política, en concordancia con el Modelo Integrado de Planeación y Gestión –MIPG–.
- Aprobar y hacer seguimiento a planes, programas, proyectos y estrategias de seguridad y privacidad de la información.

Oficina de Tecnologías de la Información y las Comunicaciones (OTIC):

- Liderar la implementación, operación, seguimiento y mejora del SGSI, así como la estrategia de seguridad digital del MVCT, en articulación con los

- grupos internos de trabajo creados mediante la Resolución 0672 de 2025, o aquella que la modifique, actualice o derogue.

Oficial de Seguridad y Privacidad de la Información:

- Liderar y gestionar la implementación y mantenimiento del Modelo de Seguridad y Privacidad de la Información (MSPI) en la Entidad.
- Definir y gestionar la normativa de seguridad y privacidad de la información y de seguridad digital.
- Promover la concientización, capacitación y mejora continua en seguridad y privacidad de la información.
- Definir, socializar e implementar los procedimientos de gestión de seguridad y privacidad de la información.
- Asesorar y acompañar a las áreas en la gestión de activos de información, riesgos, controles y planes de tratamiento.

Funcionarios, contratistas y practicantes:

- Aplicar las políticas y procedimientos de seguridad de la información.
- Cumplir los roles y responsabilidades asignados en materia de seguridad y privacidad.
- Gestionar los riesgos de seguridad y privacidad de la información inherentes a sus procesos.
- Participar activamente en programas de capacitación y sensibilización sobre seguridad de la información.
- Identificar y clasificar los activos de información bajo su responsabilidad.
- Actuar como propietarios o custodios de la información, garantizando la protección de los activos.

Oficina Asesora Jurídica:

- Asesorar a los procesos en temas jurídicos y legales relacionados con seguridad y privacidad de la información.
- Asesorar sobre obligaciones legales y requisitos de cumplimiento en seguridad y protección de la información.
- Apoyar lineamientos de seguridad para la gestión con proveedores.
- Verificar que políticas y procedimientos del MSPI se ajusten a la normativa vigente.

Grupo del Talento Humano:

- Controlar y salvaguardar la información personal de los funcionarios, asegurando su tratamiento conforme a la normatividad.
- Gestionar vinculación, capacitación y desvinculación del personal cumpliendo controles de seguridad y privacidad de la información.
- Implementar procesos de selección con verificación de antecedentes y evaluaciones de confiabilidad.
- Garantizar la firma de acuerdos de confidencialidad y compromiso con la protección de datos desde la vinculación.
- Integrar la formación en seguridad de la información en los procesos de inducción y reinducción.

- Apoyar al Oficial de Seguridad y Privacidad de la Información en el plan de concientización y sensibilización.

Oficina de Control Disciplinario Interno:

- Incluir auditorías de seguridad de la información en el Plan Anual de Auditoría.
- Evaluar la efectividad de los controles y el cumplimiento normativo en seguridad de la información y protección de datos personales.
- Realizar auditorías internas de seguridad de la información e identificar no conformidades y oportunidades de mejora.
- Informar los resultados de las auditorías y coordinar actividades con otras áreas.
- Proporcionar una evaluación independiente y objetiva sobre la eficacia del sistema de gestión de seguridad de la información.

Grupo de Comunicaciones:

- Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la Entidad.

Grupo de Recursos Físicos:

- Implementar y operar los controles de acceso físico a sedes, pisos, salas técnicas, centros de datos, archivos y demás áreas donde se procesan o almacenan activos de información.
- Asegurar que los servicios de vigilancia ejecuten verificación de identidad, registro de visitantes, control de ingreso de equipos tecnológicos y acompañamiento a terceros en áreas sensibles.
- Mantener actualizados los registros de acceso físico (bitácoras/minutas, registros de visitas, reportes de novedades) y ponerlos a disposición del Oficial de Seguridad y Privacidad de la Información y de Oficina de Control Interno cuando se investiguen incidentes.
- Asegurar que las cámaras cubran accesos, pasillos y puntos sensibles de acuerdo con la matriz de riesgos de seguridad de la información y los criterios que defina el Oficial de Seguridad.
- Administrar la conservación, custodia y entrega de grabaciones, respetando tiempos de retención, cadena de custodia y restricciones de acceso, coordinado con la Oficina Asesora Jurídica y Seguridad de la Información.
- Reportar oportunamente al Oficial de Seguridad y al Grupo de Ciberseguridad cualquier anomalía física que pueda tener impacto lógico (por ejemplo, ingreso no autorizado al CPD, manipulación de racks, daño o desconexión de equipos).
- Incluir en los pliegos y contratos de vigilancia y CCTV requisitos de seguridad de la información: confidencialidad sobre lo observado, manejo de grabaciones, tratamiento de datos personales (imágenes), tiempos de respuesta ante incidentes y reportes.

Artículo 8. Solicitud y gestión de excepciones a la política y lineamientos de seguridad. Cuando, por razones operativas, técnicas, administrativas o misionales, un servidor público, contratista del Ministerio de Vivienda, Ciudad y Territorio- MVCT o un tercero requiera apartarse de lo establecido en la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Tecnológicos y continuidad de la operación de los servicios tecnológicos, deberá presentar una solicitud formal de excepción, debidamente justificada, ante su jefe inmediato y ante el jefe de la oficina de Tecnología de la Información y las Comunicaciones, utilizando los formatos, procedimientos y canales definidos por la Entidad.

Toda solicitud de excepción deberá: (i) describir claramente el requerimiento y la política o control sobre el cual se solicita la excepción; (ii) sustentar las razones misionales o técnicas que la motivan; (iii) identificar los activos de información y servicios impactados; y (iv) incluir un análisis de riesgos asociado, así como las medidas compensatorias propuestas para mitigar los riesgos adicionales que se puedan generar.

Las excepciones serán evaluadas por el responsable de Seguridad de la Información, con el apoyo de los lideres de los procesos y activos involucrados, quienes determinarán el nivel de riesgo y el periodo máximo de vigencia de la excepción. Cuando el riesgo sea alto o crítico, la decisión de aprobación, modificación o negación deberá ser elevada al Comité de Ciberseguridad de la Información o a la instancia que haga sus veces, para su validación y autorización expresa.

Las excepciones aprobadas deberán quedar documentadas, registradas y conservadas como soporte del Sistema de Gestión de Seguridad de la Información (SGSI), incluyendo su fecha de inicio y vencimiento, las condiciones bajo las cuales se otorgan y los controles compensatorios aplicables. Una vez cumplido el plazo autorizado, la excepción será revisada para decidir su cierre o, de manera excepcional, su renovación, previo nuevo análisis de riesgos.

La aprobación de una excepción no exonera al solicitante ni a los responsables del proceso de su deber de proteger la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y privacidad de la información, ni lo libera de las responsabilidades disciplinarias, contractuales o legales que puedan derivarse de un uso inadecuado o abuso de dicha excepción.

Artículo 9. Sanciones. Cualquier violación o incumplimiento de las políticas de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios tecnológicos del Ministerio de Vivienda, Ciudad y Territorio –MVCT–, por acción u omisión, será objeto de las medidas disciplinarias, administrativas, contractuales y/o penales a que haya lugar, de conformidad con el Reglamento Interno de Trabajo, el Código General Disciplinario, las normas laborales vigentes, la normativa sobre protección de datos personales y las leyes regulatorias de delitos informáticos en Colombia. Las sanciones se definirán y aplicarán atendiendo la gravedad de la falta, las consecuencias generadas sobre la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y privacidad de la información, el impacto en la continuidad de los servicios del MVCT y la intencionalidad o reincidencia en la conducta.

RESOLUCIÓN 0289 DE 25 MAY 2026

Artículo 10. Seguimiento, medición, análisis y evaluación del SGSI. El Ministerio de Vivienda, Ciudad y Territorio realizará revisiones periódicas al SGSI. Dichas revisiones estarán enfocadas en los siguientes aspectos:

- Revisión de indicadores definidos para el Sistema de Gestión de Seguridad de la Información.
- Revisión de avance en la implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio TIC.
- Revisión de avance de la Política de Seguridad Digital de acuerdo con lo solicitado por FURAG o la herramienta definida para tal fin.

Artículo 11. Aprobación y Revisiones a la Política. Esta Política será efectiva desde su aprobación por la Alta Dirección/Instancia. La revisión de esta política se hará en las siguientes condiciones:

- De forma anual, donde se deberá revisar la efectividad de la política y sus objetivos.
- Si se dan cambios estructurales en la Entidad (restructuración de áreas o procesos).
- Incidentes de seguridad de la información que requieran que la política requiera cambios.

Artículo 12. Vigencia. La presente Resolución rige a partir de la fecha de expedición y deroga la Resolución 0331 de 2021.

PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C., a los 25 de mayo de 2026

RUTH MARITZA QUEVEDO FIQUE
Ministra de Vivienda, Ciudad y Territorio (E)

Aprobó:
Luis Roberto Cruz Gonzalez
Secretario General

Revisó:
Jesus Fernando Sarria Lopez
Jefe Oficina TIC

Elaboró:
Kevin Leonardo Barrionuevo
Coordinador Grupo Ciberseguridad

Elaboró:
Jose Gregorio Rodriguez
Contratista Oficina TIC

Revisó:
Juan Manuel Cortes Isaza
Coordinador Grupo Infraestructura Tecnológica

Revisó:
Hector Mauricio Herrera Galarza
Coordinador Grupo Sistemas de Información

Revisó:
Leydi Dayan Falla Sepúlveda
Coordinador Estrategia y Gobierno de TI

Revisó:
Diana Paola Páez Lozano
Contratista Secretaría General