CONTRALORÍA
GENERAL DE BOYACÁ

POLÍTICA INSTITUCIONAL DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

LINEAMIENTOS PARA LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN —MSPI—

Tunja, Boyacá

2026

FIRMA		FIRMA		FIRMA	
ELABORÓ	*Wilinthon Alonso Buitrago Rodriguez*	REVISÓ	*Comité Institucional de Gestión y Desempeño*	APROBÓ	Carlos Andrés Aranda
CARGO	*Director Técnico de Sistemas*	CARGO		CARGO	*Contralor General de Boyacá.*

CONTROL DE CAMBIOS

No.	Versión	Descripción del cambio	Fecha
1	01	Elaboración inicial del documento denominado **"Modelo de Seguridad y Privacidad de la Información – Políticas de Seguridad Informáticas"**.	23/11/2023
2	02	Actualización integral del documento y cambio de denominación a **"Política Institucional de Seguridad Digital y Privacidad de la Información"**. Se incorporan los lineamientos de la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información —MSPI—, el artículo 6 y el Anexo 3 de la Resolución MinTIC 1519 de 2020, así como disposiciones relacionadas con gestión de activos de información, riesgos, accesos, infraestructura tecnológica, servicios digitales, proveedores, incidentes de seguridad, continuidad de la operación, seguimiento y mejora continua.	Julio de 2026

I. CLÁUSULA DE SUSTITUCIÓN DOCUMENTAL

La presente **Política Institucional de Seguridad Digital y Privacidad de la Información, versión 02**, sustituye integralmente el documento denominado **"Modelo de Seguridad y Privacidad de la Información – Políticas de Seguridad Informáticas", versión 01 de 2023**.

Los lineamientos técnicos y operativos que continúen siendo aplicables deberán incorporarse o mantenerse en los planes, procedimientos, manuales, instructivos y demás documentos complementarios de la Contraloría General de Boyacá, siempre que sean compatibles con la presente política.

II. CLÁUSULA DE ADOPCIÓN DEL MSPI

La Contraloría General de Boyacá adopta e implementa progresivamente el **Modelo de Seguridad y Privacidad de la Información —MSPI—** como marco institucional para la gestión de la seguridad digital, la seguridad de la información y la privacidad, bajo un enfoque basado en riesgos, mejora continua y proporcionalidad institucional.

La implementación del MSPI se desarrollará mediante políticas, planes, procedimientos, controles, instrumentos de gestión, actividades de seguimiento y evidencias que permitan demostrar su aplicación y fortalecimiento continuo.

III. CLÁUSULA DE OBLIGATORIEDAD

Las disposiciones de la presente política son de obligatorio cumplimiento para todos los servidores públicos, contratistas, practicantes, proveedores, terceros y demás personas que, en ejercicio de sus funciones, actividades u obligaciones, accedan, administren, procesen, custodien, almacenen, transmitan o utilicen información o recursos tecnológicos de la Contraloría General de Boyacá.

El desconocimiento de la presente política no exime de responsabilidad frente a su cumplimiento.

IV. CLÁUSULA DE RESPONSABILIDAD INSTITUCIONAL

La seguridad digital y la privacidad de la información son responsabilidades compartidas por todos los niveles de la Contraloría General de Boyacá.

La Dirección Técnica de Sistemas liderará técnicamente su implementación; los responsables de proceso deberán garantizar su aplicación en sus dependencias; y el Comité Institucional de Gestión y Desempeño realizará el seguimiento institucional correspondiente.

PRESENTACIÓN INSTITUCIONAL

La Contraloría General de Boyacá reconoce la información como un activo esencial para el cumplimiento de su misión constitucional y legal, el ejercicio del control fiscal, la gestión administrativa, la atención a la ciudadanía y la prestación de sus servicios institucionales.

En desarrollo de este compromiso, adopta la presente **Política Institucional de Seguridad Digital y Privacidad de la Información** como instrumento rector para orientar la protección de la información, los activos tecnológicos, los sistemas, la infraestructura y los servicios digitales de la Entidad.

La política establece los principios, responsabilidades y lineamientos de obligatorio cumplimiento para los servidores públicos, contratistas, practicantes, proveedores y demás terceros que accedan, administren, custodien, procesen, almacenen, transmitan o utilicen información o recursos tecnológicos institucionales.

Su implementación se desarrollará de manera progresiva, articulada con la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información —MSPI— y los instrumentos institucionales de planeación, gestión de riesgos, continuidad, protección de datos personales y mejora continua.

Con esta política, la Contraloría General de Boyacá reafirma su compromiso con la protección de la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y privacidad de la información, así como con el fortalecimiento de una cultura institucional de seguridad digital.

Contenido

1. INTRODUCCIÓN

La Contraloría General de Boyacá reconoce que la información constituye uno de sus activos más importantes para el cumplimiento de su misión constitucional y legal. Su protección resulta esencial para garantizar la continuidad de los procesos, la confianza de la ciudadanía, la adecuada gestión institucional y el cumplimiento de las obligaciones legales y regulatorias aplicables.

El uso creciente de sistemas de información, plataformas tecnológicas, servicios digitales, redes de comunicaciones, infraestructura informática, servicios en la nube y mecanismos de almacenamiento e intercambio ha fortalecido la capacidad operativa de la Entidad. Sin embargo, también ha incrementado la exposición a amenazas internas y externas que pueden afectar la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y privacidad de la información.

En este contexto, la seguridad digital y la privacidad deberán gestionarse de manera integral, preventiva y permanente, mediante la identificación de activos, la administración de riesgos, la implementación de controles, la gestión de accesos, la protección de la infraestructura, la atención de incidentes, la continuidad de la operación y el seguimiento a la efectividad de las medidas adoptadas.

La presente política establece el marco institucional de principios, responsabilidades y lineamientos aplicables a todas las dependencias, procesos y personas que accedan, administren, custodien, procesen, almacenen, transmitan o utilicen información o recursos tecnológicos de la Contraloría General de Boyacá.

La política desarrolla el habilitador transversal de Seguridad y Privacidad de la Información de la Política de Gobierno Digital y adopta los lineamientos del Modelo de Seguridad y Privacidad de la Información —MSPI—, bajo un enfoque basado en riesgos, mejora continua y proporcionalidad institucional.

Asimismo, orienta el cumplimiento de las condiciones técnicas y de seguridad digital aplicables a la Entidad y la protección de la información pública, pública clasificada, pública reservada, personal y sensible, independientemente del medio en que sea tratada.

Su implementación se articulará con los planes, procedimientos, controles e instrumentos institucionales correspondientes, procurando fortalecer la capacidad de la Entidad para prevenir, detectar, responder y recuperarse frente a eventos que puedan afectar la información y los servicios tecnológicos.

2. OBJETIVOS

2.1. Objetivo General:

Establecer el marco institucional para la gestión de la seguridad digital, la seguridad de la información y la privacidad en la Contraloría General de Boyacá, mediante la implementación progresiva del Modelo de Seguridad y Privacidad de la Información —MSPI—, la gestión de riesgos y la aplicación de controles administrativos, humanos, físicos y tecnológicos orientados a proteger la información, los activos tecnológicos, la infraestructura y los servicios institucionales.

2.2. Objetivos específicos

- Proteger la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y privacidad de la información institucional, independientemente de su formato, ubicación o medio de tratamiento.
- Fortalecer la implementación y mejora continua del Modelo de Seguridad y Privacidad de la Información —MSPI—, en articulación con la Política de Gobierno Digital y los instrumentos de planeación institucional.
- Identificar, valorar, tratar y monitorear los riesgos que puedan afectar la información, los procesos, los activos, la infraestructura y los servicios tecnológicos de la Entidad.
- Establecer responsabilidades y controles para la adecuada gestión de activos, accesos, credenciales, sistemas, servicios digitales, proveedores y demás recursos tecnológicos.
- Fortalecer la capacidad institucional para prevenir, detectar, atender y recuperarse frente a incidentes, fallas, interrupciones y violaciones de datos personales.
- Promover una cultura institucional de seguridad digital y privacidad, mediante acciones de sensibilización, formación, seguimiento, evaluación y mejora continua.

3. ALCANCE

La presente **Política Institucional de Seguridad Digital y Privacidad de la Información** aplica a todas las dependencias y procesos estratégicos, misionales, de apoyo, evaluación y control de la Contraloría General de Boyacá.

Es de obligatorio cumplimiento para los servidores públicos, contratistas, practicantes, proveedores, terceros y demás personas que, en desarrollo de sus funciones, actividades u obligaciones, accedan, administren, custodien, procesen, almacenen, transmitan, intercambien, publiquen o utilicen información o recursos tecnológicos de la Entidad.

Su aplicación comprende toda la información institucional, independientemente de su formato, ubicación, medio o soporte, incluyendo documentos físicos y electrónicos, bases de datos, correos electrónicos, archivos audiovisuales, registros administrativos e información misional, financiera, contractual, jurídica, documental y tecnológica.

También comprende la información pública, pública clasificada, pública reservada, los datos personales, los datos sensibles y demás contenidos sujetos a condiciones especiales de acceso, reserva, confidencialidad, conservación o protección.

La política aplica a los activos y servicios tecnológicos que soportan la operación institucional, entre ellos:

- sistemas de información, aplicaciones y plataformas institucionales;
- servidores físicos y virtuales, bases de datos y sistemas de almacenamiento;
- equipos de cómputo, dispositivos portátiles, periféricos y medios removibles;
- redes de datos, equipos de comunicaciones y servicios de conectividad;
- portal web, subdominios, formularios electrónicos y demás canales digitales;
- correo institucional, herramientas de comunicación y colaboración;
- copias de seguridad, servicios de alojamiento, nube, soporte y mantenimiento;
- servicios tecnológicos administrados total o parcialmente por proveedores o terceros.

La política será aplicable tanto en las instalaciones físicas de la Contraloría General de Boyacá como en escenarios de trabajo remoto, acceso externo, operación móvil, prestación de servicios por terceros y uso de plataformas tecnológicas externas autorizadas.

Los contratos, convenios, órdenes de servicio, acuerdos de confidencialidad y demás instrumentos que impliquen acceso, tratamiento, custodia, almacenamiento

o administración de información institucional deberán incorporar y observar los lineamientos establecidos en esta política.

Su implementación se desarrollará de manera proporcional a la naturaleza de la información, la criticidad de los activos, el nivel de riesgo, las obligaciones legales y las capacidades institucionales, sin limitar el deber general de protección, cumplimiento y mejora continua.

4. MARCO NORMATIVO Y TÉCNICO

La presente **Política Institucional de Seguridad Digital y Privacidad de la Información** se fundamenta en las disposiciones constitucionales, legales, reglamentarias y técnicas aplicables a la Contraloría General de Boyacá en materia de seguridad digital, seguridad de la información, privacidad, protección de datos personales, transparencia, gestión documental, continuidad de la operación y Gobierno Digital.

Las normas y referentes señalados deberán interpretarse junto con las disposiciones que los modifiquen, adicionen, sustituyan o reglamenten.

4.1. Constitución Política de Colombia

- **Artículo 15:** reconoce los derechos a la intimidad, al buen nombre y al habeas data.
- **Artículo 20:** garantiza el derecho a informar y recibir información veraz e imparcial.
- **Artículo 74:** reconoce el derecho de acceso a los documentos públicos, salvo las excepciones legales.
- **Artículo 209:** establece los principios que orientan la función administrativa.

4.2. Leyes

- **Ley 527 de 1999:** regula los mensajes de datos, el comercio electrónico y las firmas digitales.
- **Ley 594 de 2000:** establece las disposiciones generales sobre gestión y conservación documental.
- **Ley 1266 de 2008:** regula el habeas data financiero, crediticio, comercial y de servicios, cuando resulte aplicable.
- **Ley 1273 de 2009:** protege la información y los datos y tipifica conductas relacionadas con delitos informáticos.

- **Ley 1341 de 2009:** establece principios sobre la sociedad de la información y las tecnologías de la información y las comunicaciones.
- **Ley 1437 de 2011:** regula las actuaciones, documentos, expedientes y medios electrónicos en la administración pública.
- **Ley 1581 de 2012:** establece el régimen general de protección de datos personales.
- **Ley 1712 de 2014:** regula la transparencia, el acceso a la información pública y las categorías de información pública, clasificada y reservada.
- **Ley 1755 de 2015:** regula el derecho fundamental de petición y el tratamiento de la información asociada.
- **Ley 2052 de 2020:** establece disposiciones sobre racionalización, digitalización y automatización de trámites.

4.3. Decretos

- **Decreto 1074 de 2015:** compila las disposiciones reglamentarias sobre protección de datos personales.
- **Decreto 1078 de 2015:** compila la regulación del sector TIC e incorpora la Política de Gobierno Digital.
- **Decreto 1081 de 2015:** reglamenta aspectos relacionados con transparencia y acceso a la información pública.
- **Decreto 1083 de 2015:** regula la planeación y gestión institucional en el sector público.
- **Decreto 612 de 2018:** integra los planes institucionales y estratégicos al Plan de Acción.
- **Decreto 2106 de 2019:** establece medidas para la simplificación, digitalización y automatización administrativa.
- **Decreto 620 de 2020:** establece lineamientos para el uso y operación de los servicios ciudadanos digitales.
- **Decreto 88 de 2022:** desarrolla disposiciones sobre digitalización y automatización de trámites.
- **Decreto 338 de 2022:** fortalece la gobernanza de la seguridad digital y la coordinación de respuesta a incidentes.

- **Decreto 767 de 2022:** actualiza la Política de Gobierno Digital y reconoce la seguridad y privacidad de la información como habilitador transversal.
- **Decreto 1263 de 2022:** establece lineamientos aplicables a la transformación digital pública.

4.4. Resoluciones y lineamientos sectoriales

- **Resolución MinTIC 1519 de 2020:** establece estándares de publicación, accesibilidad web, seguridad digital y datos abiertos, incluyendo las condiciones mínimas técnicas y de seguridad digital de su Anexo 3.
- **Resolución MinTIC 500 de 2021:** establece lineamientos para la implementación del MSPI, la gestión de riesgos y la gestión de incidentes de seguridad digital.
- **Resolución MinTIC 460 de 2022:** adopta el Plan Nacional de Infraestructura de Datos.
- **Resolución MinTIC 746 de 2022:** fortalece los lineamientos de implementación del MSPI.
- **Resolución MinTIC 2277 de 2025:** actualiza el Anexo 1 de la Resolución 500 de 2021 y fortalece los lineamientos del MSPI.
- Guías, manuales, instrumentos de autodiagnóstico y demás documentos técnicos expedidos por MinTIC para la implementación de Gobierno Digital y del MSPI.

4.5. Documentos de política pública

- **CONPES 3854 de 2016:** Política Nacional de Seguridad Digital.
- **CONPES 3975 de 2019:** Política Nacional para la Transformación Digital e Inteligencia Artificial.
- **CONPES 3995 de 2020:** Política Nacional de Confianza y Seguridad Digital.

4.6. Referentes técnicos

La Contraloría General de Boyacá podrá adoptar como referentes técnicos, de acuerdo con su aplicabilidad, nivel de riesgo y capacidad institucional:

- ISO/IEC 27001:2022, sobre sistemas de gestión de seguridad de la información.
- ISO/IEC 27002:2022, sobre controles de seguridad de la información.

- ISO/IEC 27005, sobre gestión de riesgos de seguridad de la información.
- ISO 22301, sobre continuidad.
- Modelo de Seguridad y Privacidad de la Información —MSPI—.
- Manual de Gobierno Digital.
- Guías para la administración del riesgo y el diseño de controles en entidades públicas.
- Buenas prácticas del NIST, CSIRT Gobierno y demás organismos competentes.

4.7. Aplicación institucional

Las disposiciones y referentes señalados se aplicarán de acuerdo con las competencias de la Contraloría General de Boyacá, la naturaleza de la información, la criticidad de los activos, los riesgos identificados y los recursos institucionales disponibles.

La aplicación del marco normativo y técnico se desarrollará mediante esta política y los planes, procedimientos, controles e instrumentos institucionales que la complementen.

5. DEFINICIONES

Para efectos de la presente **Política Institucional de Seguridad Digital y Privacidad de la Información**, se adoptan las siguientes definiciones:

Activo de información: Recurso que contiene, procesa, almacena, transmite o soporta información y que tiene valor para la Contraloría General de Boyacá. Comprende información, documentos, bases de datos, sistemas, aplicaciones, infraestructura, servicios tecnológicos y conocimiento institucional.

Amenaza: Causa o situación potencial que puede aprovechar una vulnerabilidad y afectar la seguridad o privacidad de la información.

Autenticación: Proceso mediante el cual se verifica la identidad de una persona, dispositivo, aplicación o sistema antes de permitir su acceso.

Autenticidad: Propiedad que permite comprobar que la información, comunicación o transacción proviene de la fuente declarada.

Autorización: Permiso otorgado para acceder a información, sistemas, funciones o recursos, de acuerdo con las responsabilidades asignadas.

Clasificación de la información: Proceso mediante el cual la información se categoriza según su naturaleza, sensibilidad, valor, criticidad, requisitos legales y nivel de protección requerido.

Confidencialidad: Propiedad que garantiza que la información solo sea conocida o utilizada por personas, procesos o sistemas autorizados.

Control: Medida administrativa, humana, física o tecnológica implementada para prevenir, reducir, detectar, corregir o responder frente a un riesgo.

Copia de seguridad: Reproducción de información, configuraciones o sistemas realizada para permitir su recuperación ante pérdida, daño, alteración o indisponibilidad.

Custodio del activo: Persona, dependencia o tercero responsable de administrar, almacenar, operar o proteger un activo de acuerdo con las instrucciones de su propietario.

Dato personal: Información vinculada o que pueda asociarse con una persona natural determinada o determinable.

Dato sensible: Dato cuyo uso indebido puede afectar la intimidad del titular o generar discriminación, de acuerdo con la normativa aplicable.

Disponibilidad: Propiedad que garantiza que la información, los sistemas y los servicios estén accesibles y utilizables oportunamente por las personas autorizadas.

Encargado del tratamiento: Persona natural o jurídica que realiza el tratamiento de datos personales por cuenta del responsable.

Incidente de seguridad digital: Evento o serie de eventos que compromete o amenaza la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad o privacidad de la información.

Información pública: Información generada, obtenida, adquirida o controlada por la Entidad cuyo acceso puede ser consultado por cualquier persona, salvo las excepciones legales.

Información pública clasificada: Información cuyo acceso puede limitarse por pertenecer al ámbito privado o semiprivado de una persona natural o jurídica, conforme con la ley.

Información pública reservada: Información cuyo acceso se encuentra restringido por disposición legal para proteger intereses públicos.

Integridad: Propiedad que garantiza que la información sea exacta, completa y no haya sido modificada o destruida sin autorización.

Mínimo privilegio: Principio según el cual cada usuario, proceso o sistema recibe únicamente los permisos necesarios para cumplir sus funciones.

Modelo de Seguridad y Privacidad de la Información —MSPI—: Marco definido por MinTIC para orientar la implementación, fortalecimiento y mejora continua de la seguridad y privacidad de la información en las entidades públicas.

Necesidad de conocer: Principio que limita el acceso a la información a quienes lo requieren para cumplir sus funciones, actividades u obligaciones.

Privacidad de la información: Protección de los derechos de las personas frente al tratamiento de sus datos personales.

Propietario del activo: Dependencia o responsable con autoridad para definir la clasificación, uso, acceso y protección de un activo de información.

Responsable del tratamiento: Persona natural o jurídica que decide sobre las bases de datos y las finalidades del tratamiento de los datos personales.

Riesgo de seguridad digital: Posibilidad de que una amenaza aproveche una vulnerabilidad y afecte la información, los procesos, los sistemas o los servicios institucionales.

Riesgo inherente: Nivel de riesgo existente antes de aplicar controles.

Riesgo residual: Nivel de riesgo que permanece después de aplicar y evaluar los controles existentes.

Segregación de funciones: Distribución de responsabilidades y privilegios entre diferentes personas o roles para reducir errores, fraude o abuso de acceso.

Seguridad de la información: Conjunto de principios, procesos y controles orientados a preservar la confidencialidad, integridad y disponibilidad de la información, así como su autenticidad, trazabilidad y privacidad.

Seguridad digital: Condición resultante de la gestión de riesgos y de la aplicación de medidas para proteger la información, los sistemas, la infraestructura y los servicios en el entorno digital.

Trazabilidad: Capacidad de identificar y reconstruir las acciones realizadas sobre la información, los sistemas o los servicios.

Tratamiento de datos personales: Cualquier operación realizada sobre datos personales, como recolección, almacenamiento, uso, circulación, transmisión, transferencia, consulta, actualización o eliminación.

Violación de datos personales: Incidente que ocasiona destrucción, pérdida, alteración, divulgación o acceso no autorizado a datos personales.

Vulnerabilidad: Debilidad de un activo, proceso, control, configuración, sistema o servicio que puede ser aprovechada por una amenaza.

6. ARTICULACIÓN CON LA POLÍTICA DE GOBIERNO DIGITAL, ADOPCIÓN DEL MSPI Y PRINCIPIOS INSTITUCIONALES

La **Política Institucional de Seguridad Digital y Privacidad de la Información** desarrolla el habilitador transversal de Seguridad y Privacidad de la Información de la Política de Gobierno Digital y constituye el marco institucional para orientar la protección de la información, los activos tecnológicos y los servicios digitales de la Contraloría General de Boyacá.

En este contexto, la Entidad adopta e implementa progresivamente el **Modelo de Seguridad y Privacidad de la Información —MSPI—**, de acuerdo con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones. Su aplicación se desarrollará bajo un enfoque basado en riesgos, proporcional a las capacidades institucionales, articulado con la planeación y orientado a la mejora continua.

La política se implementará mediante planes, procedimientos, controles e instrumentos de gestión que permitan demostrar su aplicación efectiva. El detalle técnico y operativo será desarrollado en los documentos complementarios de la Entidad, evitando incorporar en esta política actividades, frecuencias o instrucciones que correspondan a procedimientos específicos.

Figura 1: Articulación de la Política de Gobierno Digital, el MSPI y los instrumentos institucionales
Fuente: elaboración propia

6.1. Articulación con los instrumentos institucionales

La implementación de esta política se articulará con el Plan Estratégico de Tecnologías de la Información —PETI—, el Plan de Seguridad y Privacidad de la Información, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, el Plan de Mantenimiento de Servicios Tecnológicos, la Política de Administración del Riesgo, la Política de Tratamiento y Protección de Datos Personales y los instrumentos de gestión documental, continuidad, contratación, control interno y planeación institucional.

Estos instrumentos deberán desarrollar las actividades, responsables, recursos, cronogramas, indicadores y evidencias requeridos para la aplicación progresiva del MSPI. Cuando un asunto se encuentre regulado en un procedimiento o plan especializado, esta política establecerá únicamente el lineamiento general y se remitirá al documento correspondiente.

La articulación institucional deberá evitar la creación de controles aislados o duplicados y procurar que las decisiones relacionadas con seguridad digital respondan a los riesgos, necesidades y prioridades de la Contraloría General de Boyacá.

6.2. Implementación progresiva del MSPI

La implementación del MSPI se desarrollará como un proceso continuo que comprenda la identificación del estado actual, la definición de acciones, la implementación de controles, la evaluación de resultados y la adopción de mejoras. El diagnóstico permitirá reconocer brechas, riesgos, activos, controles existentes y capacidades institucionales. Con base en sus resultados se establecerán prioridades y acciones en los planes correspondientes. La ejecución deberá orientarse a fortalecer los controles administrativos, humanos, físicos y tecnológicos, mientras que el seguimiento permitirá determinar su cumplimiento y efectividad.

Las acciones de mejora se definirán a partir de los resultados de auditorías, incidentes, análisis de riesgos, pruebas, cambios tecnológicos y modificaciones normativas. El seguimiento general a la política y a sus instrumentos se desarrollará en el capítulo correspondiente a medición y mejora continua, evitando repetir en este punto indicadores, evidencias y mecanismos de evaluación.

6.3. Principios institucionales

La gestión de la seguridad digital y la privacidad de la información deberá observar principios que orienten las decisiones, la asignación de responsabilidades y la implementación de controles durante todo el ciclo de vida de la información y de los servicios tecnológicos.

Para facilitar su comprensión y evitar una enumeración excesiva, los principios se organizan en cuatro grupos complementarios.

Figura 2: Principios institucionales de seguridad digital y privacidad de la información
Fuente: elaboración propia

- **Protección de la información:** La Contraloría General de Boyacá deberá preservar la **confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad** de la información. La confidencialidad exige que solo accedan quienes se encuentren autorizados; la integridad procura que la información permanezca completa y sin modificaciones indebidas; y la disponibilidad garantiza su acceso oportuno por parte de los usuarios autorizados.
  La autenticidad permitirá comprobar la identidad de las personas, sistemas o fuentes que generan información, mientras que la trazabilidad deberá facilitar la identificación y reconstrucción de las actividades relevantes realizadas sobre los activos institucionales.
- **Acceso, control y legalidad:** El tratamiento de la información y el uso de los recursos tecnológicos deberán realizarse de conformidad con la normativa vigente, las finalidades institucionales y las autorizaciones establecidas.
  Los accesos deberán regirse por los principios de **necesidad de conocer, mínimo privilegio y segregación de funciones**, de manera que cada persona o sistema cuente únicamente con los permisos indispensables y se evite la concentración de actividades incompatibles.
  Las decisiones de seguridad deberán sustentarse en la gestión de riesgos y en la criticidad de la información, procurando que los controles aplicados

sean proporcionales, verificables y adecuados a las obligaciones de la Entidad.

- **Diseño, prevención y resiliencia:** La seguridad y la privacidad deberán incorporarse desde la planeación de los procesos, proyectos, contratos, sistemas, formularios y servicios digitales, y no únicamente después de su implementación.
  La Entidad aplicará medidas preventivas y un enfoque de defensa en profundidad, combinando controles administrativos, humanos, físicos y tecnológicos. La falla de una medida no deberá ocasionar automáticamente la pérdida o exposición de la información.
  La continuidad y la resiliencia orientarán la preparación institucional para mantener o recuperar los procesos y servicios críticos frente a fallas, incidentes, ataques, desastres o interrupciones.

- **Cultura y mejora continua:** La seguridad digital y la privacidad son responsabilidades compartidas por todos los niveles de la Entidad y por las personas que accedan, administren, custodien o utilicen información institucional.
  La Contraloría promoverá la formación, la sensibilización y el reporte oportuno de eventos de seguridad. Asimismo, conservará evidencias que permitan demostrar la gestión de riesgos, la ejecución de controles y la atención de incidentes.
  Los controles y lineamientos deberán revisarse y mejorarse de acuerdo con los resultados obtenidos, los cambios tecnológicos, los riesgos emergentes y las necesidades institucionales.

7. GOBIERNO, ROLES Y RESPONSABILIDADES

La seguridad digital y la privacidad de la información requieren la participación coordinada de la alta dirección, los responsables de proceso, la Dirección Técnica de Sistemas, las dependencias de apoyo, los usuarios y los terceros vinculados con la Contraloría General de Boyacá.

Las responsabilidades se asignarán de acuerdo con las competencias institucionales, la propiedad y custodia de los activos de información, el nivel de acceso y la capacidad de decisión de cada actor. La Dirección Técnica de Sistemas liderará técnicamente la implementación de esta política, sin que ello implique

asumir de manera exclusiva la responsabilidad sobre la información administrada por los demás procesos.

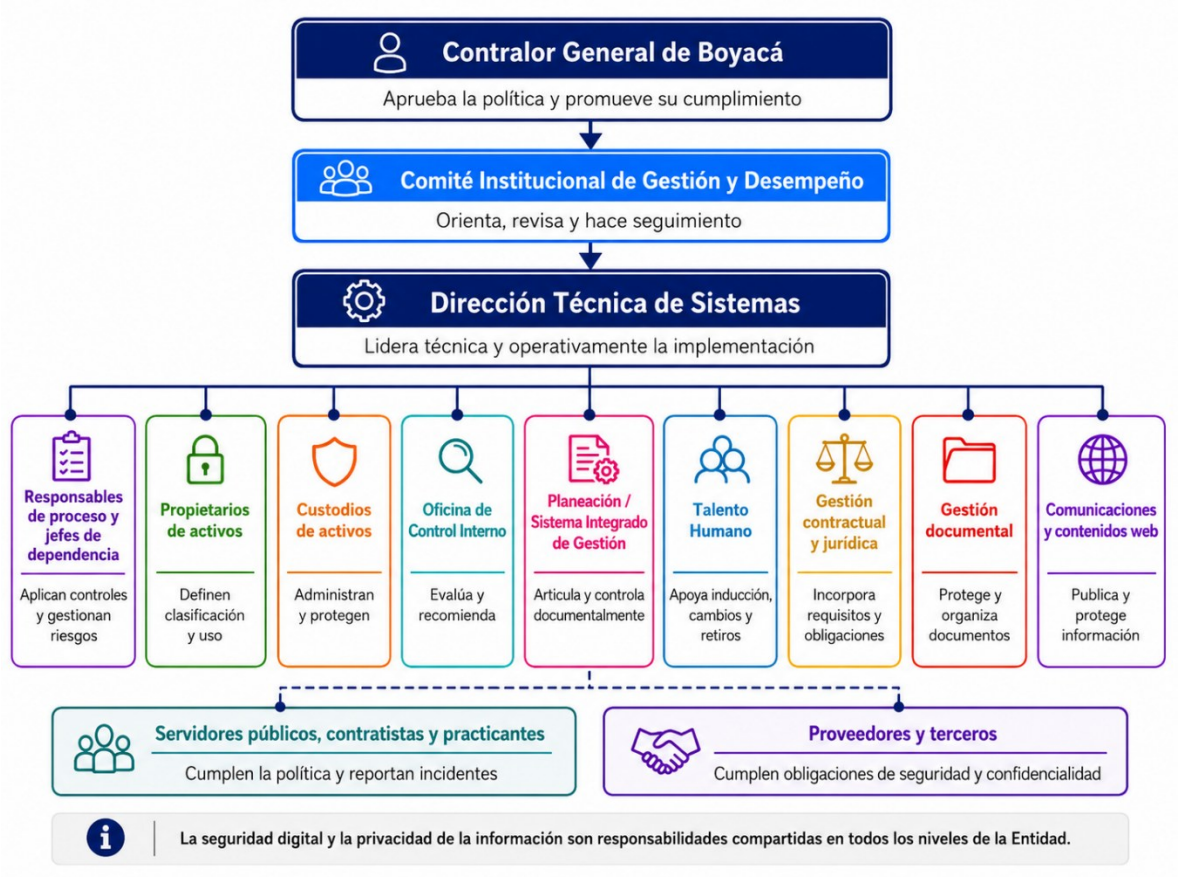

Figura 3: Gobierno, roles y responsabilidades en seguridad digital y privacidad de la información.
Fuente: elaboración propia

7.1. Alta dirección y gobierno institucional

El Contralor General de Boyacá aprobará la política, promoverá su cumplimiento y respaldará la asignación de los recursos necesarios para su implementación, de acuerdo con los riesgos, prioridades y capacidades institucionales.

El Comité Institucional de Gestión y Desempeño orientará la aplicación de la Política de Gobierno Digital y del Modelo de Seguridad y Privacidad de la Información —MSPI—, conocerá los avances, riesgos e incidentes relevantes y realizará seguimiento a las acciones que requieran coordinación institucional.

La dependencia responsable de planeación apoyará la articulación de esta política con el Sistema Integrado de Gestión, la planeación institucional, la administración del riesgo y los mecanismos de seguimiento y mejora.

7.2. Liderazgo técnico y evaluación independiente

La Dirección Técnica de Sistemas liderará la implementación técnica del MSPI y administrará los controles tecnológicos bajo su competencia. Asimismo, orientará a los procesos en la protección de los activos de información, la gestión de riesgos, el control de accesos, la atención de incidentes y la continuidad de los servicios tecnológicos.

También será responsable de formular y mantener los planes, procedimientos y lineamientos técnicos necesarios para desarrollar esta política, así como de coordinar el seguimiento a las acciones de seguridad digital que se encuentren bajo su responsabilidad.

La Oficina de Control Interno evaluará de manera independiente la existencia, aplicación y efectividad de los controles, formulará recomendaciones y realizará seguimiento a las acciones de mejora, sin asumir responsabilidades operativas sobre su implementación.

7.3. Responsables de procesos, propietarios y custodios

Los responsables de proceso deberán identificar la información y los activos utilizados en sus dependencias, gestionar los riesgos asociados, autorizar los accesos requeridos y promover el cumplimiento de esta política dentro de su ámbito de competencia.

Los propietarios de los activos deberán definir su clasificación, condiciones de acceso, uso autorizado y nivel de protección. Los custodios deberán aplicar los controles de administración, almacenamiento, conservación, respaldo y protección establecidos por la Entidad y por el propietario correspondiente.

La información producida o administrada por servidores públicos, contratistas o proveedores en cumplimiento de sus funciones u obligaciones continuará siendo propiedad de la Contraloría General de Boyacá, salvo las excepciones legal o contractualmente establecidas.

7.4. Dependencias de apoyo institucional

Talento Humano deberá incorporar los deberes de seguridad digital y privacidad en los procesos de inducción, reinducción, cambios de funciones y retiro, y comunicar

oportunamente las novedades que puedan requerir la creación, modificación o revocación de accesos.

Las dependencias responsables de contratación y asuntos jurídicos deberán incorporar en los contratos y demás instrumentos aplicables las obligaciones de confidencialidad, seguridad, protección de datos, continuidad, propiedad, entrega y eliminación de información.

Gestión Documental orientará la organización, conservación, acceso, transferencia y disposición de la información documental. Las dependencias responsables de comunicaciones y publicación web deberán garantizar que los contenidos difundidos sean autorizados, íntegros y acordes con las disposiciones sobre transparencia, reserva y protección de datos personales.

7.5. Usuarios, contratistas, practicantes y terceros

Toda persona que acceda a información o recursos tecnológicos deberá utilizar únicamente los activos y permisos autorizados, proteger sus credenciales, cumplir los controles establecidos y reportar oportunamente cualquier pérdida, anomalía, vulnerabilidad o posible incidente.

Los usuarios serán responsables de las actividades realizadas mediante las cuentas y recursos que les sean asignados. Las obligaciones de confidencialidad y protección de la información se mantendrán incluso después de finalizar la relación laboral, contractual, académica o comercial con la Entidad.

Los proveedores y terceros deberán cumplir las condiciones de seguridad establecidas contractualmente, limitar sus actuaciones al alcance autorizado y devolver o eliminar la información institucional cuando finalice la relación con la Contraloría General de Boyacá.

Las responsabilidades establecidas en este capítulo deberán ejercerse de manera coordinada. Cuando una actividad involucre varias dependencias, deberá identificarse quién autoriza, quién ejecuta y quién verifica el control correspondiente. Su cumplimiento deberá respaldarse mediante los registros, autorizaciones, actas, informes o soportes que resulten aplicables, sin perjuicio del deber general de todas las personas de proteger la información institucional.

8. GESTIÓN DE ACTIVOS, CLASIFICACIÓN Y TRATAMIENTO DE LA INFORMACIÓN

La Contraloría General de Boyacá deberá identificar, registrar, clasificar y proteger los activos de información necesarios para el cumplimiento de sus funciones, independientemente de su formato, ubicación, soporte tecnológico o dependencia responsable.

La gestión de activos permitirá establecer qué información posee la Entidad, dónde se encuentra, quién responde por ella, qué nivel de protección requiere y cuáles controles deben aplicarse durante su uso, almacenamiento, intercambio y disposición final.

Los responsables de proceso deberán participar en la identificación y actualización de los activos bajo su competencia, con el acompañamiento técnico de la Dirección Técnica de Sistemas y de las demás dependencias que intervengan según la naturaleza de la información.

Figura 4: Proceso institucional de gestión de activos de información.
Fuente: elaboración propia

8.1. Identificación e inventario

Los activos de información deberán identificarse y registrarse en los instrumentos institucionales definidos para tal fin. El inventario deberá incluir, según corresponda, información documental, bases de datos, sistemas, aplicaciones, infraestructura tecnológica, equipos, redes, servicios digitales, medios de almacenamiento, conocimiento institucional y servicios administrados por terceros.

El registro deberá contener información suficiente para reconocer el activo, su ubicación, dependencia responsable, propietario, custodio, clasificación, nivel de criticidad y relación con los procesos institucionales.

Los inventarios deberán mantenerse actualizados cuando se creen, adquieran, modifiquen, trasladen, integren, sustituyan o retiren activos. La actualización será responsabilidad compartida entre el proceso que utiliza o genera la información y la dependencia que administra el recurso tecnológico o documental correspondiente.

8.2. Clasificación, criticidad, propiedad y custodia

La información deberá clasificarse de acuerdo con su naturaleza, sensibilidad, valor institucional, requisitos legales y posibles consecuencias derivadas de su pérdida, alteración, divulgación o indisponibilidad.

Para efectos de acceso y divulgación, la clasificación deberá considerar las categorías de información pública, pública clasificada y pública reservada, así como los datos personales, sensibles y demás contenidos sujetos a protección especial. La criticidad deberá valorar el impacto que tendría la afectación de la confidencialidad, integridad o disponibilidad del activo sobre los procesos y servicios institucionales.

Figura 5: Clasificación y criticidad de los activos de información.
Fuente: elaboración propia

Todo activo deberá contar con un propietario y, cuando corresponda, con un custodio. El propietario definirá la clasificación, condiciones de acceso, uso autorizado y nivel de protección requerido. El custodio aplicará los controles de administración, almacenamiento, conservación y protección establecidos por la Entidad.

La asignación de propietario o custodio no modifica la titularidad institucional de la información ni libera a los usuarios del deber de proteger los activos a los que tengan acceso.

8.3. Uso, almacenamiento, transferencia y protección

Los activos deberán utilizarse exclusivamente para las finalidades institucionales autorizadas y de acuerdo con su clasificación, criticidad y condiciones de acceso. Los usuarios deberán evitar su copia, modificación, divulgación o traslado sin autorización.

La información deberá almacenarse en repositorios, sistemas, equipos y servicios previamente autorizados por la Contraloría General de Boyacá. Cuando se requiera utilizar medios removibles, dispositivos externos o servicios administrados por terceros, deberán aplicarse controles acordes con el riesgo y con la sensibilidad de la información.

La transferencia o intercambio deberá realizarse mediante canales seguros, con destinatarios autorizados y bajo condiciones que permitan preservar la confidencialidad, integridad y trazabilidad. Cuando la naturaleza de la información lo exija, deberán emplearse mecanismos de cifrado, protección de archivos, acuerdos de confidencialidad o confirmación de entrega.

Los activos administrados por proveedores o terceros estarán sujetos a las mismas condiciones de clasificación y protección establecidas por la Entidad. Las obligaciones contractuales correspondientes se desarrollarán en el capítulo de gestión de proveedores.

Los respaldos, mantenimientos, accesos y controles técnicos deberán aplicarse de acuerdo con los capítulos especializados de esta política, evitando duplicar aquí su desarrollo operativo.

8.4. Retención, revisión y disposición final

La conservación de la información deberá responder a las necesidades institucionales, los requisitos legales, las tablas de retención documental, las obligaciones contractuales y las condiciones técnicas de los sistemas utilizados.

Los activos deberán revisarse periódicamente para verificar que su clasificación, propietario, custodio, ubicación y controles continúen vigentes. Los cambios identificados deberán actualizarse en el inventario y en los instrumentos asociados.

Cuando un activo deje de ser necesario o cumpla su periodo de conservación, deberá aplicarse una disposición final segura. Esta podrá incluir transferencia documental, archivo, anonimización, devolución, reutilización controlada, borrado seguro o destrucción, según la naturaleza del activo y las obligaciones aplicables.

Antes de reasignar, devolver, donar, retirar o disponer equipos y medios de almacenamiento, deberá verificarse la eliminación segura de la información. La disposición final deberá dejar evidencia cuando la criticidad, la clasificación o el riesgo del activo así lo requieran.

La gestión de activos deberá mantenerse articulada con la gestión documental, la administración del riesgo, el control de accesos, las copias de seguridad, la continuidad, la gestión contractual y la protección de datos personales.

9. GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

La Contraloría General de Boyacá gestionará los riesgos de seguridad digital y privacidad de la información de manera permanente, sistemática y articulada con la metodología institucional de administración del riesgo.

Esta gestión tendrá como propósito prevenir, reducir y controlar los eventos que puedan afectar la información, los activos tecnológicos, los procesos, los servicios institucionales y el cumplimiento de los objetivos de la Entidad.

La gestión de riesgos se desarrollará como un ciclo continuo de identificación, análisis, valoración, tratamiento, monitoreo y mejora, considerando la criticidad de los activos, las amenazas, las vulnerabilidades, los controles existentes y las consecuencias que podrían derivarse de su materialización.

Figura 6: Ciclo de gestión continua de riesgos de seguridad digital y privacidad de la información.
Fuente: elaboración propia

9.1. Identificación, análisis y valoración

Los riesgos deberán identificarse a partir de los activos, procesos y servicios institucionales que puedan resultar afectados. El análisis deberá considerar las amenazas internas y

externas, las vulnerabilidades administrativas, humanas, físicas y tecnológicas, las causas del evento y sus posibles consecuencias.

La valoración deberá permitir determinar el nivel de riesgo inherente y el riesgo residual resultante después de evaluar los controles existentes. Para ello se tendrá en cuenta la probabilidad de ocurrencia, el impacto sobre la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y privacidad, así como las consecuencias operativas, legales, financieras o reputacionales para la Entidad.

Los criterios y niveles de valoración se aplicarán conforme a la metodología institucional vigente y deberán guardar relación con la criticidad de los activos y la continuidad de los procesos.

9.2. Tratamiento y aceptación del riesgo residual

Con base en la valoración realizada, la Entidad podrá aceptar, reducir, evitar, compartir o transferir los riesgos, de acuerdo con los niveles de tolerancia definidos y con las competencias de las instancias responsables.

La reducción implicará implementar o fortalecer controles; la evitación podrá requerir modificar o suspender la actividad que origina el riesgo; y la transferencia o el compartimiento podrán realizarse mediante contratos, seguros, acuerdos de servicio u otros mecanismos, sin que ello implique trasladar la responsabilidad institucional sobre la información.

Los riesgos que requieran acciones adicionales deberán incorporarse al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, indicando responsables, plazos, recursos y resultados esperados.

La aceptación de riesgos residuales altos o extremos deberá estar justificada, contar con medidas de seguimiento y ser conocida por la instancia competente, de acuerdo con la metodología institucional.

9.3. Seguimiento, materialización y mejora

Los riesgos deberán revisarse con una frecuencia proporcional a su nivel, a la criticidad del activo y a los cambios que puedan afectar su valoración. La revisión deberá considerar modificaciones en sistemas, procesos, proveedores, infraestructura, normativa, amenazas, vulnerabilidades e incidentes ocurridos.

Cuando un riesgo se materialice, deberá registrarse el evento, evaluarse el impacto, revisarse la eficacia de los controles y definirse las acciones necesarias para evitar su repetición. Si el evento constituye un incidente, deberá activarse el procedimiento institucional correspondiente.

La materialización de riesgos, los resultados de auditorías y las debilidades identificadas deberán utilizarse como insumo para actualizar la matriz, fortalecer los controles y ajustar los planes institucionales.

9.4. Responsabilidades y evidencias

Los responsables de proceso deberán identificar y gestionar los riesgos asociados con sus actividades y activos de información. La Dirección Técnica de Sistemas brindará acompañamiento técnico y gestionará los riesgos tecnológicos bajo su competencia,

mientras que la dependencia encargada de planeación o administración del riesgo orientará la aplicación de la metodología institucional.
El Comité Institucional de Gestión y Desempeño conocerá los riesgos relevantes y realizará seguimiento a las acciones que requieran coordinación institucional. La Oficina de Control Interno evaluará de manera independiente el diseño y funcionamiento de los controles, sin asumir su ejecución.
La Entidad deberá conservar evidencias suficientes de la identificación, valoración, tratamiento, aceptación y seguimiento de los riesgos. Estas podrán estar contenidas en matrices, planes, actas, informes, registros de incidentes, resultados de pruebas y demás soportes institucionales.
La gestión de riesgos deberá articularse con la gestión de activos, el control de accesos, la seguridad de las operaciones, la gestión de incidentes, la continuidad, la contratación y los demás instrumentos relacionados con la protección de la información.

10. GESTIÓN DE IDENTIDADES Y CONTROL DE ACCESOS

La Contraloría General de Boyacá deberá administrar de manera controlada el acceso a la información, los sistemas, aplicaciones, redes, equipos y servicios tecnológicos, garantizando que cada persona disponga únicamente de los permisos necesarios para cumplir sus funciones u obligaciones.

La gestión de accesos se fundamentará en los principios de necesidad de conocer, mínimo privilegio, segregación de funciones, trazabilidad y responsabilidad individual. Toda cuenta deberá estar asociada con una persona identificable, un rol definido y una necesidad institucional autorizada.

Los accesos deberán gestionarse durante todo su ciclo de vida, desde la solicitud y creación hasta su modificación, revisión, suspensión o eliminación.

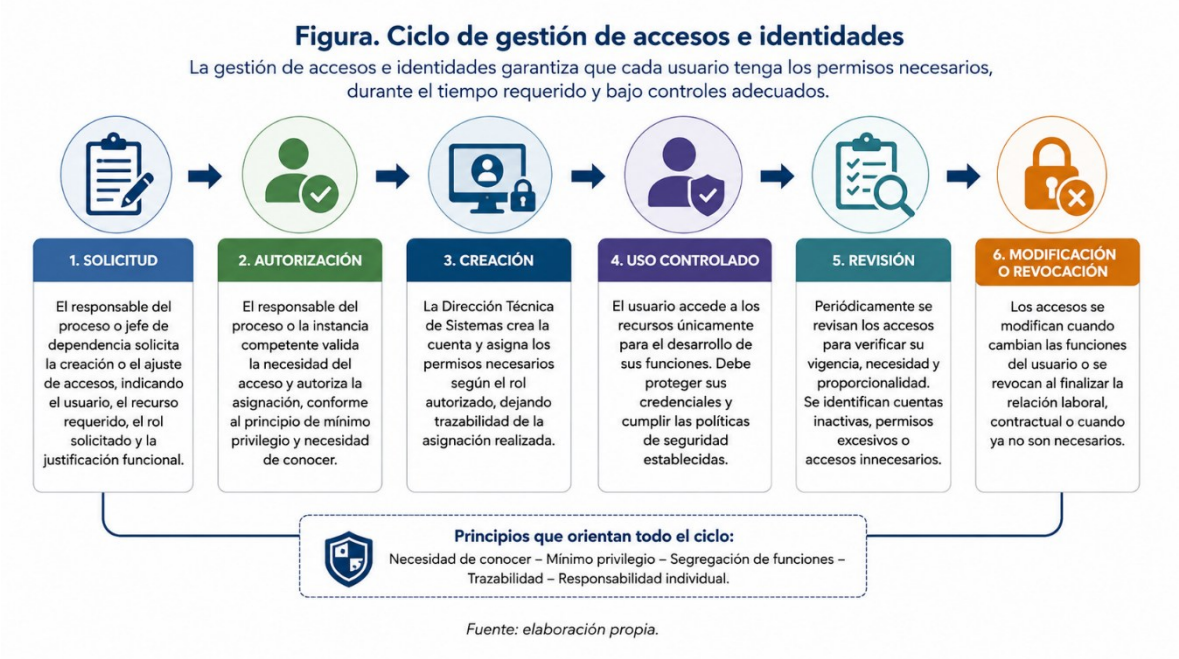

Figura 7: Ciclo de gestión de accesos e identidades.
Fuente: elaboración propia

10.1. Autorización y ciclo de vida de las cuentas

La creación de cuentas y asignación de permisos deberá contar con solicitud y autorización del responsable de proceso o jefe de dependencia correspondiente. Los accesos otorgados deberán responder al cargo, las funciones, las obligaciones contractuales o las actividades autorizadas.

Las dependencias responsables de Talento Humano y de la gestión contractual deberán informar oportunamente los ingresos, cambios de funciones, traslados, suspensiones y terminaciones que requieran crear, modificar o revocar accesos.

Cuando cambien las responsabilidades de un usuario, sus permisos deberán revisarse y ajustarse. Al finalizar la vinculación laboral, contractual o académica, las cuentas deberán desactivarse y los accesos revocarse oportunamente.

Los accesos temporales deberán contar con una vigencia definida y retirarse una vez finalice la necesidad que justificó su creación.

10.2. Credenciales, autenticación y accesos privilegiados

Las credenciales son personales, confidenciales e intransferibles. Cada usuario será responsable de protegerlas y de reportar inmediatamente cualquier sospecha de pérdida, exposición, suplantación o uso no autorizado.

Las contraseñas y demás mecanismos de autenticación deberán cumplir las condiciones técnicas definidas por la Entidad. Cuando la plataforma lo permita y el nivel de riesgo lo justifique, deberá implementarse autenticación multifactor, especialmente para cuentas administrativas, accesos remotos, correo institucional, servicios en la nube y sistemas críticos.

Las cuentas con privilegios administrativos deberán asignarse exclusivamente a personal autorizado y utilizarse solo para las tareas técnicas que requieran dicho nivel de acceso. Cuando sea posible, deberán mantenerse separadas de las cuentas utilizadas para actividades ordinarias.

Las cuentas genéricas o compartidas deberán evitarse. Cuando resulten indispensables por limitaciones técnicas, deberán contar con justificación, autorización y mecanismos que permitan identificar a las personas que las utilizan.

10.3. Acceso remoto, dispositivos personales y terceros

El acceso remoto deberá realizarse únicamente mediante mecanismos institucionales autorizados y bajo condiciones de autenticación, protección y registro acordes con el riesgo. Los usuarios deberán evitar conexiones desde equipos públicos, compartidos o redes que no ofrezcan condiciones razonables de seguridad.

El uso de dispositivos personales para acceder a información o servicios institucionales requerirá autorización y cumplimiento de las condiciones técnicas establecidas por la Entidad. La información institucional no deberá almacenarse permanentemente en estos equipos, salvo que exista autorización y se apliquen los controles correspondientes.

Los accesos otorgados a proveedores y terceros deberán estar asociados con un responsable interno, limitarse a los recursos y periodos necesarios y deshabilitarse al finalizar la actividad. Las obligaciones contractuales, de supervisión y terminación se desarrollarán en el capítulo de gestión de proveedores y terceros.

La pérdida, hurto o compromiso de un dispositivo utilizado para acceder a recursos institucionales deberá reportarse inmediatamente para restringir las cuentas, proteger la información y activar la gestión de incidentes cuando corresponda.

10.4. Revisión, segregación y trazabilidad

Los responsables de proceso y propietarios de activos deberán revisar periódicamente los accesos bajo su competencia para verificar su vigencia, necesidad y proporcionalidad. La revisión deberá permitir identificar cuentas

inactivas, permisos excesivos, privilegios incompatibles, accesos temporales vencidos y usuarios sin relación vigente con la Entidad.

La asignación de roles deberá evitar que una sola persona concentre funciones incompatibles que faciliten errores, fraude, alteración indebida o aprobación sin control independiente. Cuando la separación completa no sea posible, deberán implementarse controles compensatorios, como revisión posterior, doble aprobación o monitoreo reforzado.

Los sistemas deberán conservar registros suficientes para identificar accesos, intentos fallidos, cambios de permisos y uso de cuentas privilegiadas, de acuerdo con su criticidad y con las capacidades institucionales.

Cuando se detecten accesos no autorizados, uso indebido de credenciales o permisos incompatibles, la Entidad podrá restringir o suspender preventivamente la cuenta, preservar los registros y activar el procedimiento de gestión de incidentes.

11. USO ACEPTABLE DE LA INFORMACIÓN Y DE LOS RECURSOS TECNOLÓGICOS

La información, los equipos, sistemas, aplicaciones, redes, cuentas, servicios digitales y demás recursos tecnológicos de la Contraloría General de Boyacá deberán utilizarse exclusivamente para el cumplimiento de las funciones institucionales y de las obligaciones autorizadas.

Toda persona que acceda a estos recursos deberá emplearlos de manera responsable, segura y conforme con la normativa vigente, las condiciones de acceso asignadas y los lineamientos establecidos por la Entidad.

El uso autorizado no implica expectativa absoluta de privacidad sobre la información almacenada, transmitida o procesada mediante recursos institucionales. La Entidad podrá realizar actividades de administración, registro, supervisión y control, respetando las disposiciones legales aplicables.

PRINCIPIO	¿QUÉ IMPLICA?	USO ADECUADO (Ejemplos)	USO INADECUADO (Ejemplos)
1. USO INSTITUCIONAL	Los recursos tecnológicos e información institucional deben utilizarse exclusivamente para el cumplimiento de las funciones, procesos y actividades autorizadas por la Entidad.	✓ Usar equipos y sistemas para actividades laborales. ✓ Acceder solo a la información necesaria para el desarrollo de las funciones.	✗ Utilizar recursos institucionales para fines personales o ajenos a la Entidad. ✗ Realizar actividades ilegales, comerciales no autorizadas o proselitismo.
2. PROTECCIÓN DE CREDENCIALES	Cada usuario es responsable de la confidencialidad de sus credenciales y del uso seguro de las cuentas asignadas.	✓ Mantener contraseñas seguras y personales. ✓ Cerrar sesión al finalizar el trabajo y reportar credenciales comprometidas.	✗ Compartir usuarios o contraseñas. ✗ Dejar sesiones abiertas o anotadas en lugares visibles.
3. SOFTWARE AUTORIZADO	Solo se debe utilizar software, aplicaciones y servicios autorizados por la Entidad, que cuenten con licencias y cumplan las condiciones de seguridad establecidas.	✓ Usar programas y servicios aprobados por la Entidad. ✓ Permitir actualizaciones y controles de seguridad.	✗ Instalar o usar software no autorizado. ✗ Desactivar antivirus, cortafuegos o controles de seguridad.
4. ALMACENAMIENTO SEGURO	La información institucional debe almacenarse en repositorios, sistemas y medios autorizados, según su clasificación y nivel de protección.	✓ Guardar información en carpetas y sistemas institucionales. ✓ Usar medios removibles solo cuando sea necesario y con autorización.	✗ Almacenar información en dispositivos personales o servicios no autorizados. ✗ Transferir información institucional a cuentas personales o externas sin autorización.
5. COMUNICACIÓN RESPONSABLE	El correo institucional, internet y las herramientas de colaboración deben usarse con responsabilidad, verificando destinatarios, archivos y contenidos.	✓ Verificar destinatarios y archivos antes de enviar información. ✓ Reportar correos sospechosos o mensajes inusuales.	✗ Abrir enlaces, archivos o mensajes sospechosos. ✗ Publicar información institucional en redes sociales sin autorización.
6. REPORTE OPORTUNO	Todos los usuarios deben reportar situaciones que puedan afectar la seguridad digital, la privacidad o la disponibilidad de la información.	✓ Informar pérdida de equipos, accesos no autorizados o incidentes de seguridad. ✓ Reportar vulnerabilidades o fallas en los sistemas.	✗ No reportar incidentes o eventos sospechosos. ✗ Ignorar pérdidas, fallas o situaciones que puedan afectar la seguridad.

Figura 8: Principios de uso aceptable de la información y de los recursos tecnológicos.
Fuente: elaboración propia

11.1. Equipos, software y servicios tecnológicos

Los equipos y servicios tecnológicos deberán utilizarse conforme a su finalidad institucional, configuración autorizada y condiciones de seguridad. Los usuarios deberán protegerlos contra pérdida, daño, acceso no autorizado y uso por personas diferentes a las autorizadas.

La instalación, modificación o eliminación de software deberá realizarse únicamente con autorización de la Dirección Técnica de Sistemas. No se permitirá el uso de aplicaciones, licencias o servicios que vulneren derechos de autor, introduzcan riesgos o dificulten la administración de los recursos institucionales.

Las configuraciones de seguridad no deberán desactivarse, alterarse o evadirse sin autorización. Los usuarios deberán permitir la aplicación de actualizaciones, mantenimientos, controles y demás medidas requeridas para proteger los equipos y servicios.

Los recursos institucionales no deberán utilizarse para actividades ilícitas, comerciales no autorizadas, proselitismo, contenidos ofensivos o actuaciones ajenas a las funciones y obligaciones asignadas.

11.2. Correo electrónico, internet y herramientas de colaboración

El correo institucional, el acceso a internet y las herramientas de colaboración deberán utilizarse con criterios de responsabilidad, confidencialidad y necesidad institucional.

Los usuarios deberán verificar los destinatarios, archivos adjuntos y contenido antes de enviar información, especialmente cuando se trate de datos personales, información clasificada, reservada o sujeta a restricciones de divulgación.

No deberán abrirse enlaces, mensajes o archivos sospechosos. Cualquier comunicación que pueda constituir fraude, suplantación, código malicioso o intento de obtención de credenciales deberá reportarse de manera inmediata.

La publicación de información en páginas web, redes sociales, plataformas colaborativas o servicios externos deberá contar con autorización y respetar las disposiciones sobre transparencia, reserva, propiedad intelectual y protección de datos personales.

11.3. Almacenamiento, medios removibles e inteligencia artificial

La información institucional deberá almacenarse en repositorios, sistemas, carpetas y servicios autorizados por la Entidad. Los usuarios deberán evitar conservar información exclusivamente en discos locales, cuentas personales o plataformas no aprobadas.

El uso de memorias USB, discos externos y otros medios removibles deberá limitarse a necesidades justificadas y realizarse bajo condiciones de protección acordes con la clasificación de la información y el nivel de riesgo.

La información institucional no deberá transferirse a cuentas personales de correo, servicios privados de almacenamiento o aplicaciones no autorizadas, salvo autorización expresa y aplicación de los controles correspondientes.

El uso de herramientas de inteligencia artificial deberá realizarse de manera responsable. No deberá incorporarse en ellas información reservada, clasificada, datos personales sensibles, credenciales, documentos internos o contenidos cuya divulgación no esté autorizada.

Los resultados generados mediante inteligencia artificial deberán ser revisados antes de su utilización, publicación o incorporación en documentos institucionales. La responsabilidad sobre su exactitud, legalidad y pertinencia continuará en cabeza de la persona que los utilice.

11.4. Conductas prohibidas, monitoreo y reporte

Se prohíbe acceder, copiar, modificar, divulgar, eliminar o utilizar información sin autorización; compartir credenciales; suplantar identidades; evadir controles de seguridad; realizar pruebas no autorizadas; introducir software malicioso o interferir con la disponibilidad de los servicios institucionales.

También se prohíbe conectar equipos, aplicaciones, redes, dispositivos o servicios externos sin autorización cuando puedan generar riesgos para la infraestructura o la información de la Entidad.

La Contraloría General de Boyacá podrá registrar y monitorear el uso de sus recursos tecnológicos para fines de seguridad, administración, continuidad, auditoría y cumplimiento, de acuerdo con sus capacidades y con la normativa aplicable.

Los usuarios deberán reportar oportunamente la pérdida de información, el extravío de equipos, la exposición de credenciales, los mensajes sospechosos, los accesos no autorizados y cualquier situación que pueda comprometer la seguridad digital o la privacidad.

Las posibles infracciones se gestionarán conforme con el capítulo de incumplimientos y con los procedimientos institucionales aplicables.

12. SEGURIDAD FÍSICA, OPERACIÓN Y MANTENIMIENTO TECNOLÓGICO

La Contraloría General de Boyacá deberá proteger las instalaciones, los equipos, la infraestructura y los servicios tecnológicos frente al acceso no autorizado, el daño, la alteración, la pérdida y las condiciones ambientales que puedan afectar la información o la continuidad institucional.

La operación tecnológica deberá realizarse de manera controlada, documentada y por personal autorizado. Los equipos, redes, servidores, aplicaciones, bases de datos, servicios en la nube y demás componentes deberán administrarse de acuerdo con su criticidad, los riesgos identificados y las capacidades de la Entidad.

Las medidas de seguridad física y tecnológica deberán aplicarse de manera complementaria, procurando prevenir fallas, detectar situaciones anómalas y responder oportunamente ante eventos que puedan afectar los activos o servicios institucionales.

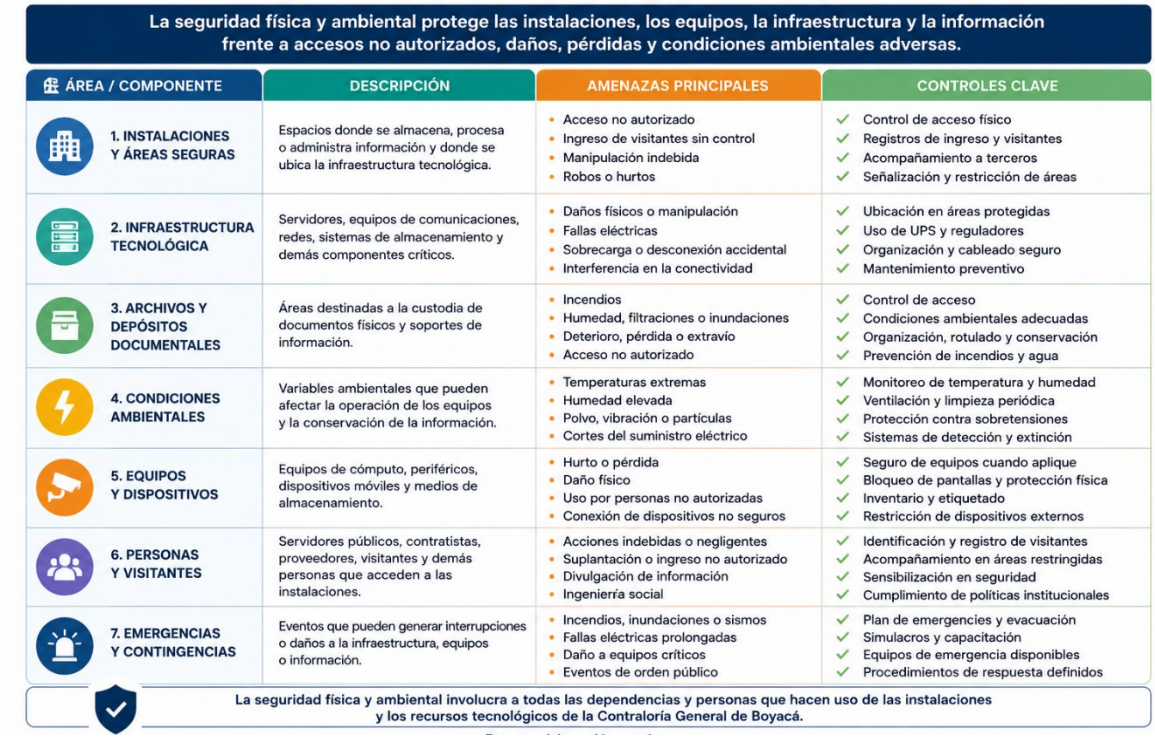

Figura 9: Componentes de la seguridad física y ambiental.
Fuente: elaboración propia

12.1. Áreas seguras y protección física

Las áreas donde se almacene, procese o administre información sensible o infraestructura crítica deberán contar con controles de acceso acordes con su nivel de riesgo. El ingreso deberá limitarse al personal autorizado y, cuando corresponda, conservar registros de visitantes, proveedores e intervenciones realizadas.

Los centros de procesamiento, áreas de comunicaciones, archivos, depósitos documentales y demás espacios de acceso restringido deberán protegerse frente a incendios, humedad, filtraciones, fallas eléctricas, alteraciones de temperatura, ingreso no autorizado y otros eventos que puedan afectar los activos.

Los visitantes y proveedores deberán permanecer acompañados cuando accedan a áreas restringidas y cumplir las condiciones de seguridad definidas por la Entidad.

Las llaves, tarjetas, códigos y demás mecanismos de ingreso deberán asignarse y controlarse de manera individual. Su pérdida, préstamo, deterioro o utilización indebida deberá reportarse oportunamente.

12.2. Protección y mantenimiento de los equipos

Los equipos tecnológicos deberán instalarse y ubicarse en condiciones que reduzcan los riesgos de daño, manipulación no autorizada, desconexión accidental, hurto y afectación ambiental.

Su traslado, retiro, reparación o intervención deberá ser autorizado y quedar registrado cuando corresponda. Antes de entregar equipos a terceros o retirarlos de las instalaciones, deberá protegerse la información almacenada y verificarse el cumplimiento de las condiciones de confidencialidad aplicables.

La Entidad deberá mantener los equipos y componentes tecnológicos mediante actividades preventivas y correctivas acordes con su estado, criticidad y disponibilidad de recursos. Estas actividades deberán ejecutarse por personal autorizado y conforme al Plan de Mantenimiento de Servicios Tecnológicos.

Los usuarios deberán cuidar los equipos asignados y reportar oportunamente daños, fallas, pérdidas o condiciones que puedan afectar su funcionamiento. No deberán realizar reparaciones, conexiones o cambios de configuración sin autorización.

12.3. Operación, configuración y gestión de cambios

La infraestructura, las plataformas y los servicios tecnológicos deberán operar bajo configuraciones autorizadas, actualizadas y acordes con los riesgos identificados. La administración deberá incluir, según corresponda, protección contra código malicioso, aplicación de actualizaciones, revisión de capacidad, gestión de vulnerabilidades y control de componentes conectados a la red.

Los cambios que puedan afectar sistemas, aplicaciones, redes, servidores o servicios deberán evaluarse, autorizarse y documentarse antes de su implementación. Cuando el nivel de riesgo lo requiera, deberán contemplarse pruebas, respaldo previo, comunicación a los usuarios y mecanismos de reversión.

Los ambientes de desarrollo, pruebas y producción deberán mantenerse separados cuando las capacidades y características de las soluciones lo permitan. El acceso y traslado de información entre estos ambientes deberá estar controlado.

La gestión detallada de actualizaciones, mantenimiento, vulnerabilidades y cambios se desarrollará mediante los procedimientos, planes e instructivos técnicos correspondientes.

Figura 10: Gestión segura de la operación tecnológica.
Fuente: elaboración propia

12.4. Monitoreo, registros y controles criptográficos

La Entidad deberá realizar, conforme a sus capacidades y a la criticidad de los servicios, el monitoreo de la infraestructura tecnológica para identificar fallas, accesos inusuales, degradación del rendimiento, vulnerabilidades y eventos que puedan afectar la seguridad o disponibilidad.

Los sistemas y servicios críticos deberán generar y conservar registros que permitan verificar las actividades administrativas, los eventos de seguridad y los cambios relevantes. El acceso a estos registros deberá limitarse al personal autorizado y protegerse contra alteración o eliminación indebida.

Cuando la clasificación de la información, el canal utilizado o el nivel de riesgo lo requieran, deberán aplicarse mecanismos criptográficos para proteger la información almacenada o transmitida. Las claves, certificados y demás elementos utilizados deberán administrarse de manera segura durante su generación, asignación, almacenamiento, renovación, revocación y eliminación.

Los eventos físicos, ambientales o tecnológicos que puedan comprometer la información o los servicios deberán reportarse y gestionarse conforme al procedimiento institucional de incidentes. Cuando ocasionen interrupciones significativas, se activarán los mecanismos de continuidad y recuperación aplicables.

13. COPIAS DE SEGURIDAD, CONTINUIDAD Y RECUPERACIÓN

La Contraloría General de Boyacá deberá adoptar medidas que permitan proteger, recuperar y restablecer la información, los sistemas y los servicios tecnológicos ante fallas, incidentes, errores humanos, ataques, desastres o interrupciones.

Las copias de seguridad y la continuidad institucional deberán gestionarse de acuerdo con la criticidad de la información, los riesgos identificados, las necesidades de los procesos y las capacidades de la Entidad.

La recuperación deberá contemplar no solo la disponibilidad de los respaldos, sino también su integridad, protección y capacidad de restauración, así como el restablecimiento oportuno de los procesos y servicios prioritarios.

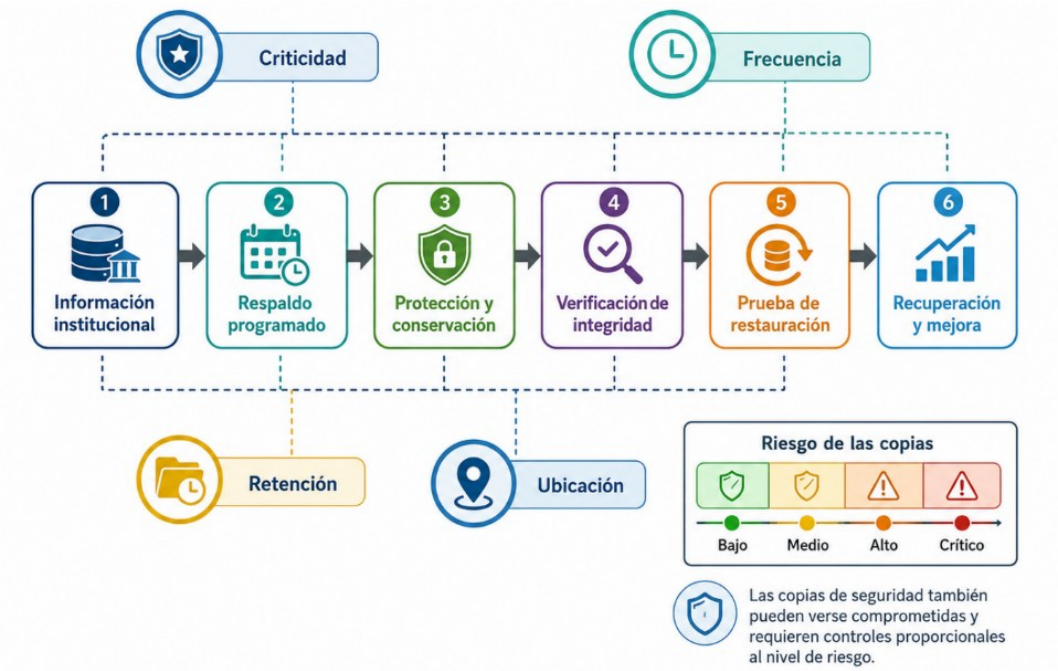

Figura 11: Copias de seguridad bajo riesgo.
Fuente: elaboración propia

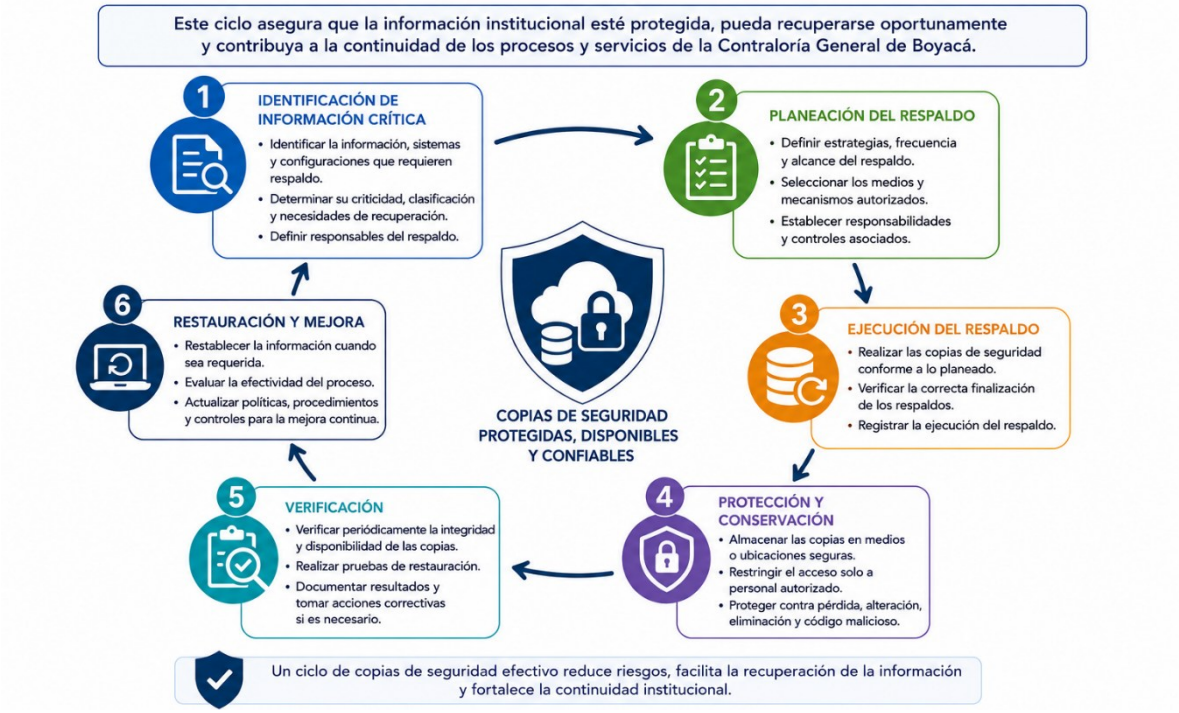

Figura 12: Ciclo institucional de gestión de copias de seguridad.
Fuente: elaboración propia

13.1. Planeación y protección de las copias de seguridad

Los responsables de proceso, propietarios de activos y administradores tecnológicos deberán identificar la información, los sistemas y las configuraciones que requieran respaldo, teniendo en cuenta su criticidad, clasificación y necesidad de recuperación.

Las copias deberán realizarse mediante mecanismos institucionales autorizados y almacenarse en condiciones que reduzcan el riesgo de pérdida simultánea con la información original. Cuando sea viable, deberán mantenerse copias separadas o ubicadas en medios o ambientes diferentes.

El acceso a los respaldos deberá restringirse al personal autorizado. Estos deberán protegerse contra alteración, eliminación, divulgación, código malicioso y acceso no autorizado.

Las frecuencias, periodos de conservación, medios utilizados, responsables y condiciones técnicas se definirán en los procedimientos e instrumentos institucionales correspondientes.

13.2. Verificación y restauración

La existencia de una copia de seguridad no será suficiente para considerar protegida la información. La Entidad deberá verificar que los respaldos se ejecuten correctamente y que puedan utilizarse cuando sean requeridos.

Las pruebas de restauración deberán realizarse de manera proporcional a la criticidad de los activos y permitir comprobar la integridad, disponibilidad y utilidad de la información respaldada.

Los errores o resultados no satisfactorios deberán documentarse y generar las acciones correctivas correspondientes. Las restauraciones deberán ser realizadas por personal autorizado y bajo condiciones que eviten la pérdida o alteración de información.

Cuando una restauración se origine en un incidente de seguridad, deberá coordinarse con el procedimiento institucional de gestión de incidentes y con la preservación de evidencias cuando corresponda.

13.3. Continuidad de procesos y servicios críticos

La Entidad deberá identificar los procesos, activos, sistemas, proveedores y servicios cuya interrupción pueda afectar de manera significativa el cumplimiento de sus funciones.

Con base en esta identificación, se definirán estrategias de continuidad y recuperación acordes con los riesgos, los recursos disponibles y las prioridades institucionales. Estas podrán incluir mecanismos alternos de operación, redundancia, respaldos, acuerdos con proveedores, recuperación tecnológica y procedimientos manuales temporales.

Las dependencias responsables deberán participar en la definición de las prioridades de recuperación y de los recursos mínimos requeridos para mantener o restablecer sus actividades.

Los terceros que soporten servicios críticos deberán cumplir las condiciones de continuidad establecidas contractualmente y suministrar la información necesaria para coordinar la recuperación.

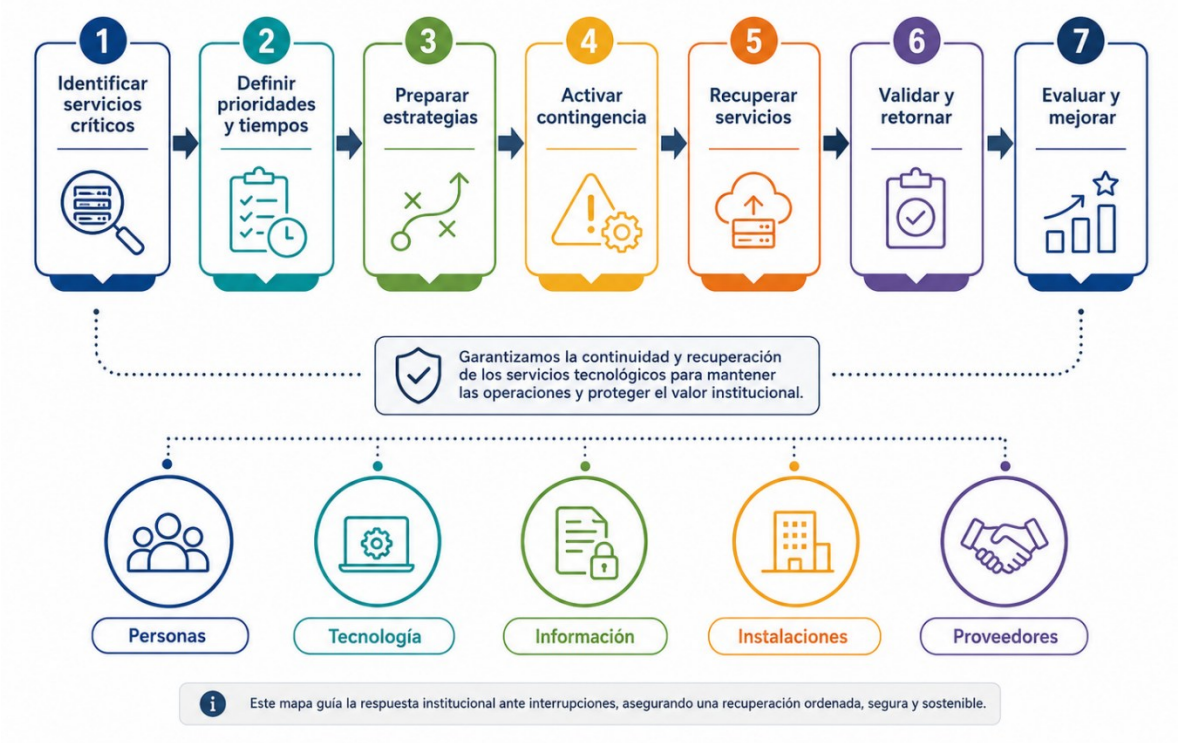

Figura 13: Gestión institucional de continuidad y recuperación.
Fuente: elaboración propia

13.4. Activación, recuperación y retorno a la operación

Los mecanismos de continuidad y recuperación deberán activarse cuando una interrupción supere la capacidad ordinaria de respuesta o amenace el cumplimiento de los procesos y servicios prioritarios.

La recuperación deberá ejecutarse de acuerdo con las prioridades institucionales, procurando restablecer primero los servicios de mayor criticidad para la operación.

Durante la contingencia deberán definirse responsables, canales de coordinación y mecanismos de comunicación. El retorno a la operación normal deberá realizarse de manera controlada, verificando la integridad de la información y la estabilidad de los servicios.

Cuando la interrupción se encuentre relacionada con un incidente de seguridad, las actividades de continuidad deberán articularse con la contención, investigación, recuperación y cierre del incidente.

13.5. Pruebas, revisión y mejora

Los mecanismos de respaldo, continuidad y recuperación deberán revisarse y probarse de acuerdo con la criticidad de los procesos y servicios.

Las pruebas podrán incluir restauración de información, simulaciones, ejercicios de escritorio, validación de contactos y pruebas técnicas de recuperación.

Los resultados deberán documentarse y utilizarse para corregir debilidades, actualizar responsables, ajustar estrategias y fortalecer la capacidad institucional de respuesta.

Los cambios en infraestructura, sistemas, procesos, proveedores, sedes, riesgos o normativa deberán considerarse para actualizar los mecanismos de continuidad y recuperación.

14. ADQUISICIÓN, DESARROLLO Y GESTIÓN SEGURA DE SERVICIOS DIGITALES

La Contraloría General de Boyacá deberá incorporar requisitos de seguridad digital, privacidad, continuidad y protección de datos desde la planeación de la adquisición, desarrollo, modificación o contratación de sistemas de información, aplicaciones, infraestructura y servicios tecnológicos.

Las soluciones deberán responder a las necesidades institucionales, los riesgos identificados, la clasificación de la información y los requisitos legales, técnicos y contractuales aplicables. La seguridad deberá considerarse durante todo el ciclo de vida, desde la definición de la necesidad hasta el retiro de la solución.

Las responsabilidades de la Entidad, los desarrolladores, proveedores, supervisores y administradores deberán establecerse de manera clara, procurando conservar el control institucional sobre la información, las cuentas administrativas, los dominios, la documentación y los componentes esenciales de las soluciones.

Figura 14: Ciclo de vida seguro de las soluciones tecnológicas.
Fuente: elaboración propia

14.1. Requisitos desde la planeación y la contratación

Las iniciativas tecnológicas deberán incluir requisitos de seguridad y privacidad acordes con la criticidad de la información, el nivel de exposición, la cantidad de usuarios, las integraciones previstas y las consecuencias de una posible falla o vulneración.

Los estudios, especificaciones y contratos deberán definir, cuando corresponda, condiciones sobre confidencialidad, protección de datos personales, control de accesos, respaldo, continuidad, registro de eventos, gestión de vulnerabilidades, atención de incidentes, propiedad intelectual, transferencia de conocimiento y devolución o eliminación de información.

La selección de soluciones y proveedores deberá considerar su capacidad para cumplir los requisitos institucionales y legales. La adquisición o contratación de un servicio no trasladará al proveedor la responsabilidad institucional sobre la información.

Las excepciones a los requisitos establecidos deberán estar justificadas, documentadas y acompañadas de controles compensatorios proporcionales al riesgo.

14.2. Desarrollo, pruebas y puesta en producción

El desarrollo o modificación de sistemas deberá realizarse aplicando prácticas de seguridad desde el diseño y protegiendo la información utilizada durante la construcción y prueba de las soluciones.

Los ambientes de desarrollo, pruebas y producción deberán mantenerse separados cuando resulte técnica e institucionalmente viable. El acceso a cada ambiente deberá limitarse al personal autorizado y la información real no deberá utilizarse en pruebas sin las medidas de protección correspondientes.

Antes de la puesta en producción, las soluciones deberán ser verificadas funcional y técnicamente para identificar errores, vulnerabilidades, configuraciones inseguras y posibles afectaciones a la información o a los servicios existentes.

La autorización de puesta en producción deberá confirmar que se cumplieron los requisitos definidos, se atendieron los hallazgos relevantes y existen mecanismos de respaldo, reversión, soporte y continuidad adecuados.

14.3. Operación, mantenimiento y retiro seguro

Las soluciones deberán mantenerse actualizadas, soportadas y protegidas durante su operación. Los cambios relevantes deberán evaluarse y gestionarse conforme con los lineamientos institucionales sobre mantenimiento, vulnerabilidades y control de cambios.

La documentación técnica y funcional necesaria deberá conservarse actualizada y permanecer disponible para la Entidad. Las cuentas maestras, certificados, dominios, repositorios, códigos, licencias y demás componentes esenciales deberán mantenerse bajo control institucional o contar con mecanismos que garanticen su recuperación.

Cuando una solución deje de ser necesaria, pierda soporte o represente un riesgo no aceptable, deberá planearse su actualización, sustitución o retiro. La información deberá migrarse, conservarse, devolverse o eliminarse de manera segura, según las obligaciones aplicables.

El retiro deberá incluir la revocación de accesos, cierre de integraciones, eliminación de credenciales y verificación de que los proveedores no conserven información institucional sin autorización.

14.4. Portal web, formularios y servicios digitales

El portal web institucional, los formularios electrónicos, las sedes digitales y demás canales tecnológicos dirigidos a la ciudadanía deberán administrarse bajo criterios de disponibilidad, integridad, autenticidad, accesibilidad, privacidad y seguridad.

La publicación o modificación de contenidos deberá ser realizada por personal autorizado y contar con aprobación de la dependencia responsable. La Dirección Técnica de Sistemas administrará los componentes tecnológicos bajo su competencia, mientras que cada dependencia responderá por la legalidad, exactitud, oportunidad y vigencia de la información que solicite publicar.

Los formularios y servicios que recopilen información deberán solicitar únicamente los datos necesarios, informar las finalidades del tratamiento y proteger la información durante su transmisión, almacenamiento y consulta.

Los dominios, certificados digitales, cuentas administrativas, servicios de alojamiento, copias de seguridad y mecanismos de recuperación deberán mantenerse bajo control institucional y revisarse de acuerdo con su criticidad.

Figura 15: Protección del portal web y de los servicios digitales institucionales.
Fuente: elaboración propia

15. GESTIÓN DE PROVEEDORES Y TERCEROS

La Contraloría General de Boyacá deberá gestionar los riesgos asociados con proveedores, contratistas, operadores tecnológicos, prestadores de servicios en la nube, personal de soporte y demás terceros que accedan, administren, almacenen, transmitan o procesen información institucional, o que intervengan en la operación de infraestructura, sistemas y servicios digitales.

La participación de terceros no disminuye la responsabilidad institucional sobre la protección de la información. Por esta razón, las condiciones de seguridad digital, privacidad, confidencialidad, continuidad y devolución de información deberán definirse desde la planeación contractual y mantenerse durante toda la relación con el proveedor.

Los requisitos aplicables deberán ser proporcionales al tipo de servicio, la información involucrada, los accesos requeridos, la dependencia tecnológica y los riesgos que puedan afectar a la Entidad.

15.1. Evaluación y requisitos contractuales

Antes de contratar servicios que involucren información o recursos tecnológicos, la Entidad deberá identificar los riesgos, activos, accesos, responsabilidades y controles requeridos.

Los estudios previos, contratos, convenios, órdenes de compra, acuerdos de servicio y demás instrumentos deberán incluir, cuando corresponda, obligaciones relacionadas con:

- confidencialidad y reserva de la información
- protección de datos personales
- control y revocación de accesos
- atención y reporte de incidentes
- continuidad y recuperación
- copias de seguridad
- propiedad y entrega de la información
- cumplimiento de niveles de servicio
- devolución, transferencia o eliminación segura de la información
- cumplimiento de los lineamientos institucionales.

Los proveedores deberán acreditar capacidad técnica y organizacional suficiente para cumplir las obligaciones asignadas. Cuando utilicen subcontratistas o integrantes de su cadena de suministro, deberán asegurar que estos cumplan condiciones de seguridad equivalentes.

La contratación de servicios en la nube, alojamiento, soporte, desarrollo o administración tecnológica deberá garantizar que la Contraloría conserve el control sobre la información, las cuentas administrativas, los dominios, las configuraciones esenciales y los mecanismos de recuperación.

15.2. Seguimiento y control del servicio

El supervisor o responsable institucional deberá verificar el cumplimiento de las obligaciones de seguridad durante la ejecución del contrato y coordinar con la Dirección Técnica de Sistemas los aspectos que requieran evaluación especializada.

Los accesos de proveedores deberán limitarse a los recursos, funciones y periodos estrictamente necesarios. Su autorización, administración y revocación se realizará conforme con el capítulo de gestión de identidades y control de accesos.

Los proveedores deberán reportar oportunamente los incidentes, vulnerabilidades, interrupciones o cambios que puedan afectar la información o los servicios de la Entidad. La atención deberá coordinarse con los procedimientos institucionales de incidentes y continuidad.

Los cambios relevantes en personal, infraestructura, ubicación de la información, subcontratistas, tecnologías o condiciones del servicio deberán ser informados y evaluados cuando puedan modificar el nivel de riesgo.

La Entidad podrá solicitar informes, certificaciones, registros, resultados de pruebas y demás evidencias necesarias para verificar el cumplimiento de las obligaciones contractuales.

Aspecto	Contraloría General de Boyacá	Proveedor o tercero
Requisitos	Define necesidades, riesgos y condiciones de seguridad	Acredita capacidad y acepta las obligaciones
Accesos	Autoriza, limita y supervisa	Usa únicamente los accesos asignados
Información	Define clasificación, uso y protección requerida	Protege la información y evita usos no autorizados
Incidentes	Coordina la respuesta y toma decisiones institucionales	Reporta, contiene y aporta información
Continuidad	Define prioridades y condiciones de recuperación	Aplica los mecanismos contractualmente acordados
Seguimiento	Supervisa y solicita evidencias	Suministra registros, informes y soportes
Terminación	Ordena la revocación y verifica el cierre	Devuelve o elimina información y accesos

Figura 16: Responsabilidades de seguridad en la relación con proveedores y terceros.
Fuente: elaboración propia

15.3. Terminación y cierre de la relación

Al finalizar el contrato, convenio o servicio deberán revocarse los accesos físicos y lógicos, devolverse los equipos, documentos, medios, credenciales y demás activos institucionales, y verificarse el cumplimiento de las obligaciones pendientes.

La información deberá ser entregada a la Contraloría en formatos accesibles y utilizables, junto con la documentación, configuraciones, códigos, respaldos o elementos requeridos para garantizar la continuidad del servicio cuando corresponda.

El proveedor deberá eliminar de manera segura las copias de información que no esté autorizado a conservar y certificar su eliminación cuando la clasificación, el riesgo o las condiciones contractuales así lo exijan.

Las obligaciones de confidencialidad, reserva, protección de datos personales y propiedad intelectual continuarán vigentes después de la terminación, conforme con la ley y con lo establecido contractualmente.

La finalización deberá quedar respaldada mediante actas, informes, certificados de eliminación, registros de revocación de accesos u otras evidencias aplicables.

16. GESTIÓN DE INCIDENTES DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

La Contraloría General de Boyacá deberá identificar, reportar, analizar y atender oportunamente los eventos e incidentes que puedan afectar la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad o privacidad de la información institucional.

La gestión de incidentes deberá orientarse a reducir su impacto, preservar la continuidad de los servicios, proteger las evidencias, coordinar la respuesta institucional y prevenir la repetición de situaciones similares.

Toda persona que tenga conocimiento de una pérdida, acceso no autorizado, suplantación, alteración, indisponibilidad, divulgación indebida, código malicioso, vulnerabilidad explotada o cualquier situación sospechosa deberá reportarla mediante los canales definidos por la Entidad.

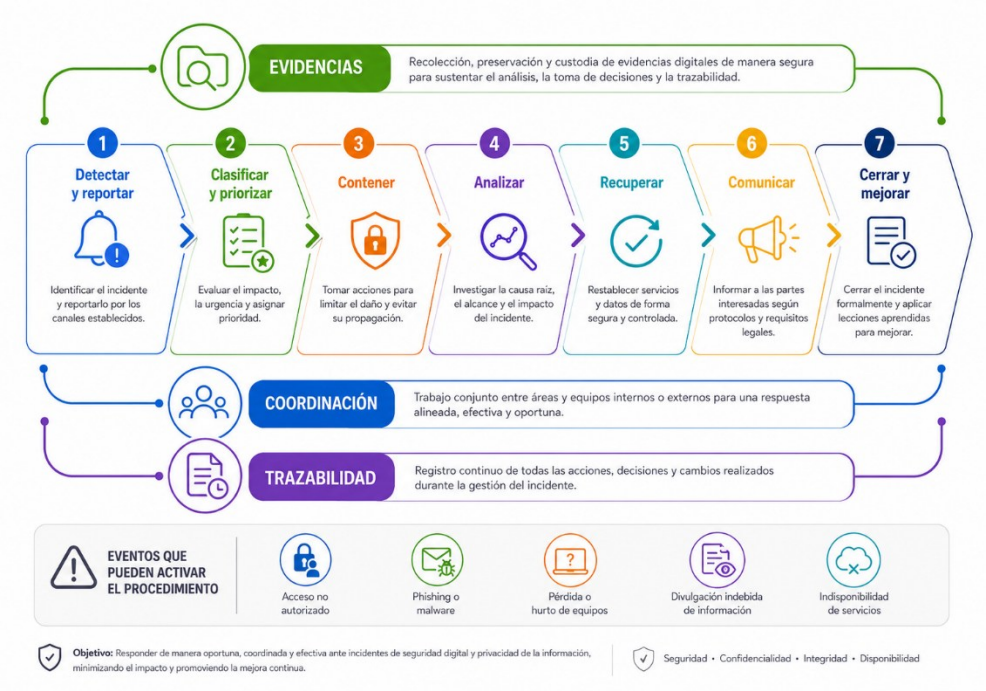

Figura 17: Flujo institucional de gestión de incidentes de seguridad digital.
Fuente: elaboración propia

16.1. Reporte, registro y clasificación

Los eventos de seguridad deberán reportarse de manera inmediata y con la información disponible, sin que sea necesario confirmar previamente que se trata de un incidente.

La Dirección Técnica de Sistemas o el equipo designado deberá registrar el evento, realizar una evaluación inicial y determinar su naturaleza, alcance, activos afectados, posibles consecuencias y nivel de severidad.

La clasificación deberá considerar, entre otros aspectos, la criticidad de la información y de los servicios afectados, la cantidad de usuarios involucrados, la duración de la interrupción, la posible exposición de datos personales y el impacto legal, operativo, financiero o reputacional.

Los eventos que no constituyan incidentes deberán conservarse como antecedentes cuando puedan aportar información para el monitoreo, la prevención o la mejora de los controles.

Figura 18: Niveles de severidad y escalamiento de incidentes.
Fuente: elaboración propia

16.2. Contención, análisis y recuperación

Una vez identificado el incidente, deberán adoptarse medidas proporcionales para limitar su propagación, proteger los activos afectados y reducir el impacto sobre los procesos y servicios institucionales.

Las acciones podrán incluir la restricción de accesos, aislamiento de equipos, bloqueo de cuentas, protección de registros, suspensión temporal de servicios o activación de mecanismos alternos de operación, según la naturaleza del evento.

El análisis deberá permitir determinar las causas, vulnerabilidades explotadas, información comprometida, alcance real y controles que fallaron o resultaron insuficientes.

La erradicación y recuperación deberán ejecutarse de manera controlada, verificando que la amenaza haya sido eliminada, que los sistemas se encuentren estables y que la información conserve condiciones adecuadas de integridad y disponibilidad.

Cuando el incidente genere una interrupción significativa, deberán activarse los mecanismos de continuidad y recuperación definidos por la Entidad.

16.3. Escalamiento, comunicaciones y coordinación

Los incidentes deberán escalarse de acuerdo con su severidad, impacto y obligaciones legales. La alta dirección, el Comité Institucional de Gestión y Desempeño, los responsables de proceso, Control Interno, Jurídica, Comunicaciones u otras dependencias deberán intervenir cuando la naturaleza del evento así lo requiera.

Las comunicaciones internas y externas deberán ser coordinadas, oportunas y autorizadas. Ninguna persona deberá divulgar información sobre un incidente sin autorización cuando ello pueda afectar la investigación, la recuperación, la reputación institucional o los derechos de las personas.

Cuando el incidente involucre datos personales, infraestructura crítica, posibles conductas delictivas o servicios administrados por terceros, deberán evaluarse las obligaciones de notificación, denuncia, reporte o coordinación con las autoridades y organismos competentes.

Los proveedores deberán informar oportunamente los incidentes relacionados con los servicios prestados y suministrar los registros, análisis y evidencias requeridos para la respuesta institucional.

16.4. Evidencias, cierre y aprendizaje

Durante la atención del incidente deberán preservarse los registros, archivos, imágenes, comunicaciones, equipos y demás elementos que puedan servir como evidencia, aplicando controles de integridad, acceso y trazabilidad.

El cierre deberá documentar el incidente, las acciones realizadas, los activos afectados, las causas identificadas, el impacto, las decisiones adoptadas y las medidas correctivas o preventivas definidas.

Los incidentes relevantes deberán ser analizados para actualizar los riesgos, fortalecer los controles, ajustar procedimientos, mejorar la continuidad y orientar las actividades de formación y sensibilización.

La información de los incidentes deberá conservarse de acuerdo con su clasificación, las obligaciones legales y los criterios institucionales de gestión documental y seguridad.

17. PRIVACIDAD, CULTURA Y CUMPLIMIENTO

La Contraloría General de Boyacá deberá proteger los datos personales y demás información sujeta a condiciones especiales de confidencialidad, promoviendo al mismo tiempo una cultura institucional de uso seguro, responsable y consciente de la información y de los recursos tecnológicos.

La aplicación de esta política es obligatoria para los servidores públicos, contratistas, practicantes, proveedores y demás terceros que accedan o utilicen información institucional. Su cumplimiento deberá integrarse a las actuaciones administrativas, laborales, contractuales, académicas y tecnológicas de la Entidad.

17.1. Privacidad y protección de datos personales

El tratamiento de datos personales deberá realizarse de conformidad con la normativa vigente, la Política de Tratamiento y Protección de Datos Personales de la Contraloría General de Boyacá y las finalidades legítimas relacionadas con el cumplimiento de sus funciones.

La recolección, consulta, almacenamiento, uso, transmisión, transferencia, publicación, conservación y eliminación de datos deberá limitarse a la información necesaria y contar con medidas de seguridad proporcionales a su naturaleza y nivel de riesgo.

Los procesos, sistemas, formularios, contratos y servicios digitales que involucren datos personales deberán aplicar criterios de privacidad desde el diseño y por defecto. El acceso se limitará a las personas autorizadas y la información no podrá utilizarse o divulgarse para finalidades diferentes de las permitidas.

Antes de publicar o entregar documentos, bases de datos, imágenes o contenidos institucionales, deberá verificarse si contienen información que requiera anonimización, ocultamiento, restricción o protección especial.

Figura 19: Gestión institucional de la privacidad y protección de datos personales.
Fuente: elaboración propia

17.2. Cultura, sensibilización y formación

La Entidad promoverá una cultura de seguridad digital y privacidad basada en la responsabilidad individual, la prevención, la protección de la información y el reporte oportuno de situaciones sospechosas.

Las actividades de sensibilización y formación deberán responder a los riesgos institucionales y adaptarse a las funciones, obligaciones y niveles de acceso de los diferentes grupos de usuarios.

La Dirección Técnica de Sistemas coordinará las acciones generales de sensibilización, con el apoyo de Talento Humano, Comunicaciones y las demás dependencias competentes. Los servidores públicos, contratistas, practicantes y

terceros deberán participar en las actividades que les sean asignadas y aplicar los conocimientos adquiridos.

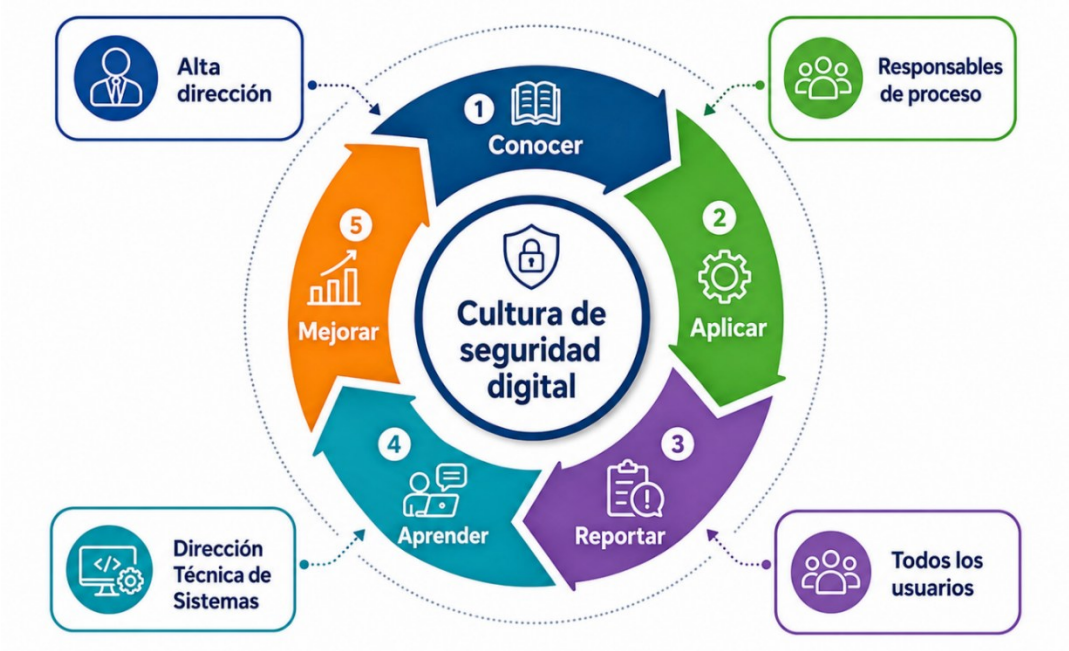

Figura 20: Ciclo institucional de cultura, sensibilización y formación en seguridad digital.
Fuente: elaboración propia

Los cronogramas, contenidos, públicos, canales y mecanismos de evaluación se definirán en los planes institucionales correspondientes. La Entidad conservará las evidencias necesarias para demostrar la ejecución de las actividades.

17.3. Cumplimiento y deber de reporte

Toda persona deberá conocer y cumplir los lineamientos de esta política, proteger la información a la que tenga acceso y comunicar las situaciones que puedan afectar su seguridad o privacidad.

Los responsables de proceso deberán promover su aplicación dentro de las dependencias y corregir oportunamente las situaciones que se encuentren bajo su competencia.

El desconocimiento de la política no exime de responsabilidad. Las dudas relacionadas con su aplicación deberán ser consultadas con la Dirección Técnica de Sistemas o con la dependencia competente, según la naturaleza del asunto.

El reporte de buena fe de eventos, vulnerabilidades o posibles incumplimientos deberá promoverse como una práctica preventiva. Ninguna persona deberá ocultar, alterar o eliminar información relacionada con un evento de seguridad.

17.4. Incumplimientos y medidas aplicables

El posible incumplimiento de esta política deberá ser evaluado de acuerdo con la naturaleza de la conducta, la información afectada, el nivel de riesgo, el daño causado y las obligaciones legales, funcionales o contractuales aplicables.

Cuando resulte necesario para proteger la información o contener un riesgo, la Entidad podrá adoptar medidas preventivas como la restricción temporal de accesos, el aislamiento de equipos, la conservación de registros o la suspensión de servicios específicos. Estas medidas no constituyen por sí mismas una sanción.

Los hechos podrán ser comunicados a las instancias administrativas, disciplinarias, contractuales, fiscales, penales o de control competentes, respetando el debido proceso y las competencias institucionales.

En el caso de contratistas, proveedores y terceros, el incumplimiento podrá dar lugar a las medidas previstas en el contrato, convenio, acuerdo de confidencialidad o instrumento jurídico correspondiente.

Los eventos identificados deberán utilizarse como insumo para fortalecer controles, actualizar riesgos, ajustar procedimientos y orientar nuevas actividades de sensibilización.

18. SEGUIMIENTO, EVALUACIÓN, ACTUALIZACIÓN Y VIGENCIA

La Contraloría General de Boyacá realizará el seguimiento a la implementación y efectividad de esta política, con el propósito de verificar su cumplimiento, identificar oportunidades de mejora y mantenerla actualizada frente a los riesgos, cambios tecnológicos, necesidades institucionales y disposiciones aplicables.

La evaluación deberá considerar no solo la ejecución de actividades, sino también la capacidad de los controles para proteger la información, reducir los riesgos y apoyar la continuidad de los procesos y servicios institucionales.

La Dirección Técnica de Sistemas coordinará el seguimiento técnico de la política y de los instrumentos asociados, con la participación de los responsables de proceso, la dependencia encargada de planeación, el Comité Institucional de Gestión y Desempeño y las demás áreas competentes.

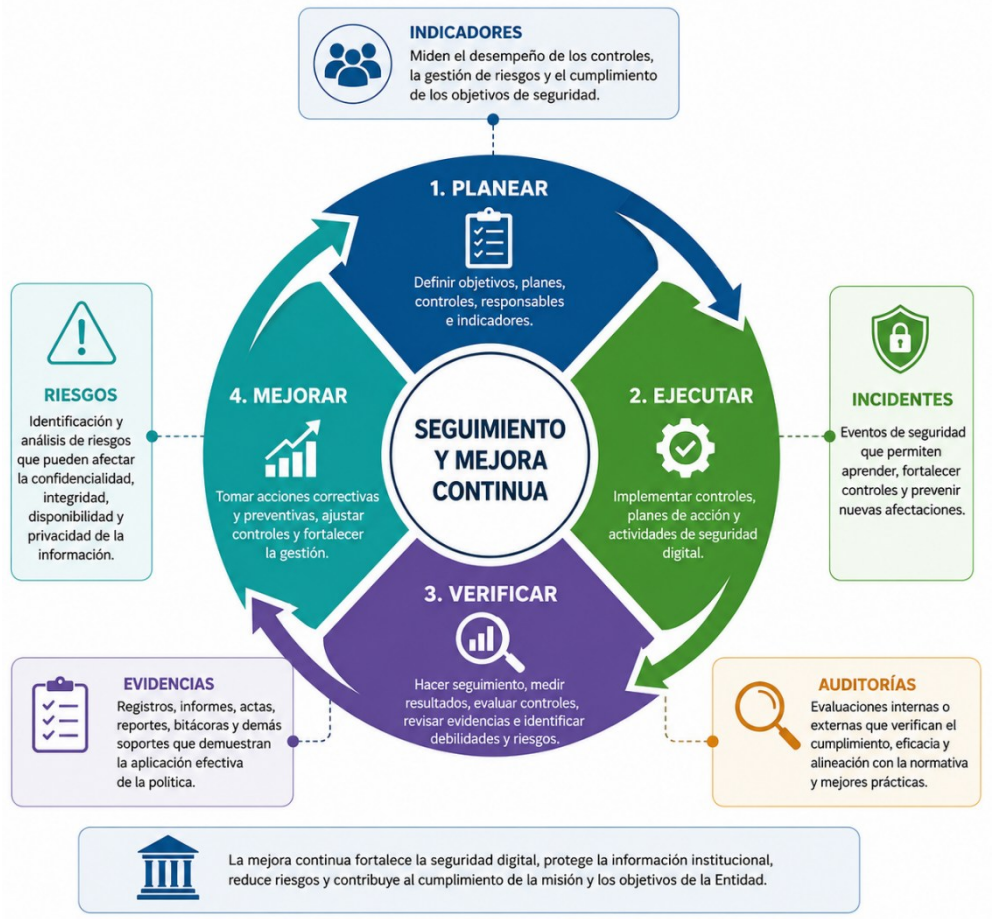

Figura 21: Ciclo institucional de seguimiento, evaluación y mejora continua.
Fuente: elaboración propia

18.1. Seguimiento e indicadores

El seguimiento deberá permitir verificar el avance de los planes, la aplicación de los controles, el tratamiento de los riesgos, la atención de incidentes, la ejecución de actividades de sensibilización y el cumplimiento de las responsabilidades establecidas.

Los indicadores deberán ser proporcionales a las capacidades de la Entidad y orientarse a medir aspectos relevantes de cumplimiento, cobertura, eficacia y mejora. Su definición, fórmula, periodicidad, fuente y responsable se establecerán en los instrumentos institucionales correspondientes.

Los responsables de proceso deberán suministrar la información y evidencias requeridas para evaluar las acciones bajo su competencia. La Dirección Técnica de

Sistemas consolidará los resultados relacionados con la implementación del MSPI y la seguridad digital.

Los resultados relevantes deberán presentarse a las instancias institucionales competentes para facilitar la toma de decisiones y la priorización de acciones.

18.2. Evaluación y mejora continua

La evaluación de la política podrá apoyarse en autoevaluaciones, auditorías, revisiones de riesgos, análisis de incidentes, pruebas de controles, resultados de continuidad, informes de proveedores y demás mecanismos institucionales.

Las debilidades, desviaciones y oportunidades identificadas deberán dar lugar a acciones de mejora acordes con su nivel de riesgo, impacto y prioridad.

Las acciones deberán contar con responsables y mecanismos de seguimiento, y podrán incorporarse al Plan de Seguridad y Privacidad de la Información, al Plan de Tratamiento de Riesgos, a planes de mejoramiento u otros instrumentos aplicables.

La Oficina de Control Interno realizará evaluaciones independientes dentro del alcance de sus funciones, sin asumir la ejecución de los controles ni de las acciones correctivas.

18.3. Revisión y actualización

La política deberá revisarse cuando se presenten cambios normativos, institucionales, tecnológicos, contractuales o de riesgo que puedan afectar su contenido o aplicación.

También podrá actualizarse como resultado de incidentes relevantes, auditorías, cambios en el MSPI, incorporación de nuevas tecnologías, modificación de procesos o identificación de controles insuficientes.

La revisión no implica necesariamente modificar el documento. Cuando se determine que continúa siendo adecuado, deberá conservarse evidencia de la evaluación realizada.

Las modificaciones sustanciales deberán surtir el proceso institucional de revisión, aprobación y control documental correspondiente.

18.4. Aprobación, divulgación y vigencia

La presente política será aprobada por la instancia competente de la Contraloría General de Boyacá y entrará en vigencia a partir de su aprobación o de la fecha definida en el acto o registro correspondiente.

La Dirección Técnica de Sistemas coordinará su divulgación y publicación a través de los canales institucionales, con el apoyo de las dependencias competentes.

Los servidores públicos, contratistas, practicantes, proveedores y demás terceros sujetos a esta política deberán conocer y aplicar sus lineamientos de acuerdo con las funciones, obligaciones y accesos asignados.

La presente versión sustituye las disposiciones internas anteriores que le sean contrarias o que regulen de manera general la misma materia, sin afectar la vigencia de procedimientos, planes e instructivos compatibles con sus lineamientos.

La política deberá permanecer disponible para consulta y ser comunicada en los procesos de inducción, reinducción, contratación, supervisión y demás escenarios institucionales que resulten aplicables.