RESOLUCIÓN 089 DE 2026
(04 DE JUNIO)

"Por la cual se actualiza el Programa Integral de Gestión de Datos Personales de la Universidad Surcolombiana adoptado mediante la Resolución número 086 de 2021"

EL RECTOR DE LA UNIVERSIDAD SURCOLOMBIANA

En uso de sus atribuciones legales y reglamentarias, en especial las conferida en el artículo 31 del Acuerdo 075 de 1994 -Estatuto General de la Universidad Surcolombiana- y

CONSIDERANDO

Que de conformidad con lo preceptuado en el numeral 2 y 18 del artículo 31 del Acuerdo Superior 075 de 1994 – Estatuto General de la Universidad Surcolombiana-, le corresponde al Rector: "*Cumplir y hacer cumplir las normas legales, estatutarias y reglamentarias vigentes*" igualmente, *"Adoptar procedimientos apropiados de planeación, programación, dirección, ejecución, evaluación y control de las actividades de la Universidad en concordancia con las políticas aprobadas por el Consejo Superior".*

Que de conformidad con lo consagrado en el artículo 15 de la Constitución Política de Colombia *"Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. (…)"*

Que el derecho consagrado en el artículo 15 de la Constitución Política de Colombia fue desarrollado por la Ley Estatutaria 1581 de 2012, 'Por la cual se dictan disposiciones generales para la protección de datos personales', la cual establece el régimen general de protección de datos personales, definiendo su ámbito de aplicación, los derechos de los titulares, los deberes de los responsables y encargados del tratamiento, así como las condiciones de legalidad para el tratamiento de la información personal."

Que la Ley Estatutaria 1581 de 2012, reglamentada parcialmente por los Decretos 1377 de 2013 y 886 de 2014, compilados en el Decreto Único Reglamentario 1074 de 2015, estableció las disposiciones generales para la protección de datos personales y reguló los derechos de los titulares, las obligaciones de los responsables y encargados del tratamiento, así como las condiciones para el tratamiento legítimo de la información personal.

Que mediante el Decreto 767 de 2022 se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Que de conformidad con el numeral 3.2 del artículo 2.2.9.1.2.1 del Decreto 767 de 2022, la Seguridad y Privacidad de la Información constituye uno de los habilitadores de la Política de Gobierno Digital, orientado a que los sujetos obligados desarrollen capacidades mediante la implementación de lineamientos de seguridad y privacidad de la información en sus procesos, trámites, servicios, sistemas de información, infraestructura y demás activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

Que mediante la Resolución No. 00500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones se establecieron los lineamientos y estándares para la estrategia de seguridad digital y se adoptó el Modelo de Seguridad y Privacidad de la Información como habilitador de la Política de Gobierno Digital.

Que mediante la Resolución No. 086 del 20 de abril de 2021 se aprobó el Programa Integral de Gestión de Datos Personales de la Universidad Surcolombiana, como instrumento orientado a garantizar el adecuado tratamiento de los datos personales y el cumplimiento de las disposiciones legales vigentes en la materia.

Que mediante la Resolución de Rectoría No. 120 de 2023 se creó el Grupo de Respuesta a Incidentes de Seguridad y Privacidad de la Información de la Universidad Surcolombiana, como instancia responsable de coordinar la atención y gestión de incidentes relacionados con la seguridad y privacidad de la información.

Que mediante la Resolución de Rectoría No. 209 de 2023 se creó el Comité de Seguridad y Privacidad de la Información de la Universidad Surcolombiana, como órgano encargado de promover, coordinar y asegurar la implementación de iniciativas, políticas, planes y estrategias relacionadas con la seguridad y privacidad de la información institucional.

Que mediante la Resolución de Rectoría No. 255 de 2023 se aprobó la actualización de la Política y los Objetivos del Sistema de Gestión de Seguridad y Privacidad de la Información de la Universidad Surcolombiana.

Que en sesión ordinaria del Comité de Seguridad y Privacidad de la Información de la Universidad Surcolombiana, realizada el veinte (20) de octubre de 2025, se aprobó la actualización del Programa Integral de Gestión de Datos Personales de la Universidad Surcolombiana, contenido en la Resolución No. 086 del 20 de abril de 2021

Que, en consecuencia, se hace necesario actualizar el Programa Integral de Gestión de Datos Personales de la Universidad Surcolombiana, con el fin de armonizarlo con la normatividad vigente en materia de protección de datos personales, seguridad y privacidad de la información, así como fortalecer los mecanismos institucionales para garantizar el adecuado tratamiento de los datos personales, la protección de los derechos de sus titulares y el cumplimiento de las disposiciones aplicables en la materia.

Que, en mérito de lo expuesto,

RESUELVE:

ARTÍCULO 1°. Aprobar la actualización del Programa Integral de Gestión de Datos Personales de la Universidad Surcolombiana, documento que hace parte integral de la presente Resolución.

ARTÍCULO 2°. El Programa Integral de Gestión de Datos Personales de la Universidad Surcolombiana se articula con el Sistema de Gestión de Seguridad y Privacidad de la Información y se implementa a través de las instancias creadas por las Resoluciones 209 y 120 de 2023.

RESOLUCIÓN 089 DE 2026
(04 DE JUNIO)

"Por la cual se actualiza el Programa Integral de Gestión de Datos Personales de la Universidad Surcolombiana adoptado mediante la Resolución número 086 de 2021"

ARTÍCULO 3°. La presente Resolución rige a partir de la fecha de su expedición y actualiza la Resolución 086 de 2021 y deja sin vigencia las demás disposiciones que sean contrarias a la presente Resolución.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

Dada en Neiva, a los cuatro (04) días del mes de junio del año dos mil veintiséis (2026).

RUBEN DARIO VALBUENA VILLARREAL
Rector

ALBERTO POLANÍA PUENTES
Secretario General

Proyectó:
MARTHA LILIANA HERMOSA TRUJILLO
Coordinadora Grupo Interno Seguridad de la Información y Protección de Datos Personales
Dirección de Centro de Información, Tecnologías y Control Documental-CITCD

Revisó: **GISELLA HERRERA RAMIREZ**
Asesora Jurídica Secretaria General

PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES

Tabla de contenido

1. Objetivo

La Universidad Surcolombiana, bajo el principio de unidad de propósito y dirección y en cumplimiento de la Ley 1581 de 2012 para la Protección de Datos Personales, la Ley 1266 de 2008 de Habeas Data, y el Decreto 767 de 2022 de Gobierno Digital, como aquellas que las reglamenten, adicionen, complementen o modifiquen; imparte los lineamientos para la implementación del Programa Integral de Gestión de Datos Personales, Habeas Data y Manejo de la Información Contenida en Bases de Datos, uso, administración, transmisión y demás actividades que involucren datos personales.

2. Alcance

Las directrices y políticas descritas en el presente documento se aplican para la Universidad Surcolombiana, desde el Consejo Superior Universitario, Rectoría, todas las dependencias académico-administrativas, procesos, facultades, programas académicos, contratistas, terceros, visitantes y demás funcionarios de acuerdo con las características de cada cargo, y demás aspectos relevantes para la implementación de este programa, con base en los principios de unidad de propósito y dirección y responsabilidad demostrada; lineamientos que debe implementar cada representante de la Estructura Orgánica de la Universidad, bajo la supervisión y monitoreo del Comité de Seguridad y Privacidad de la Información. Esta Política de Protección de Datos Personales se aplicará a todas las Bases de Datos y/o Archivos que contengan Datos Personales que sean objeto de Tratamiento por parte de la Universidad Surcolombiana, considerada como responsable y/o encargada del tratamiento de Datos Personales.

3. Normatividad

a) Ley 1266 de 2008, "Por la cual se dictan las disposiciones generales del Habeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".

b) Decreto 1727 de 2009, "Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información".

c) Decreto 2952 de 2010, "Por el cual se reglamenta los Artículos 12 y 13 de la Ley 1266 de 2008"

d) Ley 1581 de 2012 "Por el cual se dictan disposiciones generales para la protección de datos personales". Aplicable a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento.

e) Guía para la implementación del Principio de responsabilidad Demostrada (Accountability) de la Superintendencia de Industria y Comercio.

f) Decreto 1377 de 2013, "Por el cual se reglamenta parcialmente la ley 1581 de 2012.

g) Ley 1712 de 2014, "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones."

h) Decreto 886 de 2014, "Por el cual se reglamenta el Artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Base de Datos". Circular Externa 002 de 2015, Adicionar el Capítulo Segundo en el Título V de la Circular Única de la Superintendencia de Industria y Comercio.

i) Decreto Único 1074 de 2015, "Por el cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo", Capítulo 26, Registro Nacional de Base de Datos de la Superintendencia de Industria y Comercio.

j) Resolución 500 de 2021 del Ministerio de Tecnologías, "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital."

k) Decreto 767 de 2022, "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones."

l) Resolución 209 de 2023 de la Universidad Surcolombiana, "Por la cual se crea el Comité de Seguridad y Privacidad de la Información."

m) Resolución 120 de 2023 de la Universidad Surcolombiana, "Por la cual se crea el Grupo de Respuesta a Incidentes de Seguridad y Privacidad de la Información de la Universidad Surcolombiana."

n) Resolución 255 de 2023 de la Universidad Surcolombiana, "Por la cual se aprueba la actualización de la Política y Objetivos del Sistema de Gestión de Seguridad y Privacidad de la Información de la Universidad Surcolombiana."

o) Demás normas que modifiquen, complementen o deroguen las anteriores.

4. Definiciones

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

Aviso de privacidad: Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento.
Conducta Inequívoca: Corresponde al comportamiento claro del titular, o de una persona legitimada que no puede dar lugar a duda o equivocación en el consentimiento o autorización del tratamiento de sus datos personales.

Consentimiento: Es toda manifestación de voluntad, libre, específica, informada y explícita, mediante la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Dato Personal: Es cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables o que puedan asociarse con una persona natural o jurídica.

Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento.

Fuente de información: Es la persona, entidad u organización que recibe o conoce datos personales de los titulares de la información, en virtud de una relación comercial o de servicio o de cualquier otra índole y que, debido a autorización legal o del titular, suministra esos datos a un operador de información, el que a su vez los entregará al usuario final. Si la fuente entrega la información directamente a los usuarios y no, a través de un operador, aquella tendrá la doble condición de fuente y operador y asumirá los deberes y responsabilidades de ambos. La fuente de la información responde por la calidad de los datos suministrados al operador la cual, en cuanto tiene acceso y suministra información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstas para garantizar.

Incidente: Se refiere a cualquier evento en los sistemas de información o bases de datos manuales o sistematizadas, que atenta contra la seguridad de los datos personales en ellos almacenados. Estos incidentes deben ser reportados a la Superintendencia de Industria y Comercio.

Operador de información: Es la persona, entidad u organización que recibe de la fuente datos personales sobre varios titulares de la información, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la ley. Por tanto, el operador, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. Salvo que el operador sea la misma fuente de la información, este no tiene relación comercial o de servicio con el titular y por ende no es responsable por la calidad de los datos que le sean suministrados por la fuente.

RNBD: El Registro Nacional de Bases de Datos es el directorio público de las bases de datos sujetas a Tratamiento que operan en el país y es administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos.

Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

Responsabilidad Demostrada: Probar a los entes de control y vigilancia como a los titulares de la información el cumplimiento de la entidad ante el diseño, implementación y ejecución del Programa Integral de Gestión de Datos Personales.

SISI: Sistema Integral de Supervisión Inteligente, basado en riesgos; de la Superintendencia de Industria y Comercio para su control y vigilancia.

Titular: Persona natural cuyos datos personales sean objeto de Tratamiento.
Titular de la información: Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías de la normatividad aplicable.

Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o Encargado del Tratamiento de datos personales, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del responsable.
Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Usuario: El usuario es la persona natural o jurídica que, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información.

El usuario, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. En el caso en que el usuario a su vez entregue la información directamente a un operador, aquella tendrá la doble condición de usuario y fuente, y asumirá los deberes y responsabilidades de ambos.

5. Principios Rectores

a) Principio de acceso y circulación restringida: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la normatividad aplicable y la Constitución.
En este sentido, el tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la normatividad. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la normatividad.

b) Principio de confidencialidad: Todas las personas que intervengan en el tratamiento o administración de datos personales que no tengan la naturaleza de públicos, están obligadas, en todo tiempo, a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento y la administración de datos, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la Ley 1581 de 2012 y en los términos de la misma.

c) Principio de finalidad: El tratamiento de la información contenida en las Bases de Datos de la universidad obedece a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al titular previo o al momento del otorgamiento de la autorización.

d) Principio de legalidad en materia de tratamiento de datos: El tratamiento de la información contenida en las Bases de Datos, le será aplicable en lo pertinente, lo establecido en la ley 1581 de 2012 y en las demás disposiciones que la desarrollen, modifiquen y/o complementen.

e) Principio de libertad: El tratamiento de la información contenida en las Bases de Datos de la Universidad sólo puede ejercerse con el consentimiento previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

f) Principio de seguridad: La información sujeta a tratamiento a que se refiere la ley 1581 de 2012, la ley 1266 de 2008 de habeas data, así como la resultante de las consultas que de ella hagan

sus usuarios, se manejará con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

g) Principio de transparencia: En el tratamiento de la información contenida en las Bases de Datos, la Universidad garantizará el derecho del titular a obtener en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan de conformidad a las disposiciones de la ley.

h) Principio de veracidad o calidad: La información sujeta a tratamiento, será veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

6. Gobierno del Programa

6.1. Comité de Seguridad y Privacidad de la Información

Para el adecuado y oportuno funcionamiento del Programa de Protección de Datos Personales, se requiere el compromiso del Comité de Seguridad y Privacidad de la Información, creado mediante Resolución 209 de 2023, brindando el apoyo para consolidar la cultura organizacional respecto a la protección y tratamiento de datos. El Comité Seguridad y Privacidad de la Información estará integrado por:

1. Rector
2. Vicerrector Administrativo
3. Vicerrector Académico
4. Vicerrector de Investigaciones y Proyección Social
5. Secretario General
6. Jefe de Oficina Asesora de Planeación
7. Director Centro de Información, Tecnologías y Control Documental
8. Jefe de Oficina Asesora Jurídica
9. Profesional Área de Gestión Documental
10. Jefe de Oficina de Aseguramiento de la calidad
11. Profesional de planta responsable de la Seguridad de la Información y Oficial de Protección de Datos Personales
12. Coordinador del Sistema de Comunicación de la Universidad Surcolombiana

Invitado: Jefe de la Oficina de Control Interno

En cuanto a las principales responsabilidades del comité en materia de protección de datos personales, estas son:

a) Promover los derechos de los titulares de los datos personales conforme a la sección 2.2. de la Resolución 209 de 2023.

b) Disponer de modelos de autorización de tratamiento de datos personales.

c) Designar al Oficial de Protección de Datos Personales.

d) Aprobar y monitorear el Programa Integral de Gestión de Datos Personales de la Universidad Surcolombiana.

e) Realizar el acompañamiento para el diseño e implementación del programa.

f) Presentar ante el Consejo Superior Universitario y mantener informado los avances y resultados de la implementación del Programa Integral de Protección de Datos Personales.

g) Aprobar las responsabilidades de las áreas responsables respecto a la recolección, almacenamiento, uso, circulación y eliminación o disposición final de los datos personales que se tratan.

h) Mantener un inventario de las bases de datos personales en poder de la organización y clasificarlas según su tipo.

i) Registrar las bases de datos de la organización en el registro Nacional de Bases de Datos y actualizar el reporte entendiendo a las instrucciones que sobre el particular emita la SIC, en los tiempos establecidos por ley.

j) Brindar apoyo oportuno y promover acciones para la coordinación del Profesional de Planta con funciones de responsable de Seguridad de la Información y Oficial de Protección de Bases de Datos para la implementación y ejecución del Programa.

6.2. Oficial de Protección de Datos Personales

La función principal del Oficial de Protección de datos personales es velar por la implementación efectiva de las políticas y procedimientos adoptados por la Universidad.

Así, dentro de sus funciones se encuentra:

1) Estructurar, diseñar y administrar el programa que permita a la organización cumplir con las normas sobre protección de datos personales, así como establecer controles, su evaluación y revisión permanente.

2) Promover la elaboración e implementación de un sistema que permita administrar los riesgos de tratamiento de datos personales.

3) Coordinar la definición e implementación de los controles del programa integral de Gestión de Datos personales.

4) Servir de enlace y coordinador con las demás dependencias de la Universidad para asegurar una implementación transversal del programa integral de gestión de datos personales.

5) Impulsar una cultura de protección de datos dentro de la Universidad.

6) Mantener un inventario de las bases de datos personales en poder de la Universidad y clasificarlas según su tipo.

7) Registrar las bases de datos de la Universidad en el registro Nacional de Bases de Datos y actualizar el reporte entendiendo a las instrucciones que sobre el particular emita la SIC, en los tiempos establecidos por ley.

8) Obtener las declaraciones de conformidad de la SIC cuando sea requerido.

9) Revisar y actualizar los contenidos de los contratos de transmisiones internacionales de datos que se suscriban con encargados no residentes en Colombia.

10) Analizar las responsabilidades de cada dependencia de la Universidad, para diseñar un programa de entrenamiento en protección de datos personales específico para cada uno de ellos.

11) Realizar un entrenamiento general en protección de datos personales para todo el personal de la Universidad.

12) Realizar el entrenamiento necesario a los nuevos empleados, que tengan acceso por las condiciones de su empleo, a datos personales gestionados por la organización.

13) Integrar las políticas de protección de datos dentro de las actividades de las dependencias de la Universidad.

14) Medir la participación, y calificar el desempeño, en los entrenamientos de protección de datos.

15) Requerir que, dentro de los análisis de desempeño de los empleados, se encuentre haber contemplado satisfactoriamente el entrenamiento sobre protección de datos personales.

16) Velar por la implementación de planes de auditoría interna para verificar el cumplimiento de sus políticas de tratamiento de la información personal.

17) Acompañar y asistir a la Universidad en la atención a las visitas y los requerimientos que realice la SIC.

18) Realizar seguimiento al programa integral de gestión de datos personales.

19) Dará trámite a las solicitudes de los titulares para el ejercicio de sus derechos.

20) Controlar y actualizar el inventario de información personal continuamente para identificar y evaluar nuevas recolecciones, usos y divulgaciones.

21) Revisar las políticas siguiendo los resultados de las evaluaciones o auditorías.

22) Mantener como documentos históricos las evaluaciones de impacto y las de amenazas a la seguridad y riesgos.

23) Revisar y actualizar, en forma periódica, la formación y la educación impartida a todos los empleados de la Universidad, como el resultado de evaluaciones continuas y comunicar los cambios realizados a los controles del programa.

24) Revisar y adaptar los protocolos de respuesta en el manejo de violaciones e incidentes de seguridad para implementar las mejores prácticas o recomendaciones y lecciones aprendidas de revisiones posteriores a esos incidentes.

25) Revisar y, en su caso, modificar los requisitos establecidos en los contratos suscritos con los encargados del tratamiento.

26) Actualizar y aclarar las comunicaciones externas para explicar las políticas de tratamiento de datos.

27) Reportar semestralmente la evolución del riesgo, los controles implementados, el monitoreo y, en general, los avances y resultados del programa.

6.3. Auditoría Interna

La Oficina de Control Interno, debe incluir dentro de sus planes los programas para verificar el cumplimiento del Programa de Protección de Datos Personales y señalar el procedimiento a seguir en caso de que se presenten violaciones a los códigos de seguridad o se detecten riesgos en la administración de la información.

7. Sistema de control

Siendo un programa basado en controles, que responde al tamaño y estructura de la organización, destinado al cumplimiento, implementación y consolidación del régimen de protección de datos. Entendiéndose por "controles" una etapa dentro del sistema de gestión en el que se verifica si los resultados de la implementación se ajustan a las obligaciones del régimen de protección de datos personales y políticas para el tratamiento de la información personal.

En tanto la Universidad cumpla con cada uno de los pasos a identificar, se acercará a cumplir con el principio de responsabilidad demostrada. De lo contrario, tendrá que tomar las medidas necesarias que la conduzcan a satisfacer este principio.

En línea con lo expuesto, a continuación, se describe la forma general los controles que deberá verificar el Oficial de Protección de Datos Personales para asegurar que las políticas adoptadas por la organización se implementen al interior de la Universidad:

7.1. Elementos generales de la responsabilidad demostrada

a) Establecer procedimientos efectivos para la administración de los datos personales, con el fin de garantizar los derechos y responsabilidades de acuerdo con la normatividad y la implementación de la misma, bajo el principio de responsabilidad demostrada.

b) Documentar las consultas y reclamos, y mantener el inventario de las bases de datos con información personal.

c) Conocer qué datos personales se almacenan, cómo se utilizan y si realmente se necesitan, teniendo en cuenta la finalidad para la cual se recolectan; mantener documentos y registros que garanticen la integridad, oportunidad, confiabilidad y disponibilidad de la información.

d) Manejar adecuadamente los riesgos inherentes al tratamiento de la información personal: Desarrollar las etapas del programa para la prevención y control del riesgo, definidas en la Identificación, medición y control del riesgo.

e) Adecuar la infraestructura tecnológica para que soporte el programa: Contar con la tecnología y los sistemas necesarios de acuerdo con el tamaño y naturaleza de la entidad, para garantizar la adecuada administración del programa de protección de datos personales y la exposición al riesgo.

f) Divulgación de la información interna y externa: Diseño de un sistema efectivo, eficiente y oportuno de atención de consultas y reclamos por parte de los titulares de la información, como reportes y requerimientos a los entes de control y supervisión.

g) Capacitación: Diseño de programas anuales de capacitación dirigidos a todos los empleados nuevos y antiguos de la entidad, como el diseño de programas de capacitación específicas para aquellos empleados que dentro de sus funciones administren o realicen el tratamiento de la información.

7.2. Procedimientos operacionales

Consisten en la elaboración de procedimientos que hagan alusión a la recolección y utilización de los datos personales. Por tanto, es necesario que los funcionarios a cargo:

a) Conozcan dónde se almacenan los datos: Discos locales, sistemas de respaldo basados en disco, en cintas fuera de las instalaciones, en la nube, en hojas electrónicas, documentos impresos, entre otros. Cada tecnología y formato requiere su propio tipo de protección.

b) Conozcan de la información según su necesidad: Crear políticas que limiten la creación y el acceso a las bases de datos personales. Se deberá asignar el acceso basado en descripciones herméticas de puestos, de acuerdo con las funciones y perfiles. Automatizar las entradas de acceso al registro para que nadie que ha tenido acceso a las bases de datos genere un riesgo en la operación.

c) Seguridad de la red: Mecanismos de protección de las bases de datos como son herramientas actualizadas de firewall y software antivirus. Debe extender la protección sobre los teléfonos inteligentes y las tabletas que los empleados utilizan para fines de la Universidad.

d) Monitorear el ciclo de vida de los datos: Plan de gestión del ciclo de vida de los datos para garantizar la destrucción segura de los datos antiguos y obsoletos de la Universidad para su supresión.

7.2.1. Recolección o recopilación de datos personales:

La recolección de los datos deberá limitarse a aquellos datos personales que tienen como finalidad el conocimiento de las personas con las cuales la institución para el cumplimiento de sus objetivos o focos estratégicos y cumplimiento de las demás disposiciones legales y

comerciales impartidas por entes de control y supervisión; para ello dispondrá de los medios, canales, uso de redes, entre otros para la recolección de la información.
No se podrán recolectar datos personales sin autorización del titular.

7.2.2. Almacenamiento de los datos personales:

El almacenamiento implica la implementación de los mecanismos, políticas y procedimientos para salvaguardar los datos, respetando la privacidad, creando confianza, y disponer de los canales o medios al titular para acceder a ella bajo los criterios de seguridad y calidad de la información.

Como parte de este proceso, la Universidad debe:
a) Identificar los datos que debe proteger, y por cuánto tiempo;
b) Construir una estrategia de respaldo múltiple que incluya respaldos, dentro y fuera de las instalaciones;
c) Predecir las consecuencias de un ataque exitoso, luego resguardar las vulnerabilidades reveladas en este ejercicio;
d) Tomar los archivos de papel en cuenta, ya que también pueden ser robados;
e) Inventariar todo el hardware que podría albergar datos antiguos y disponer de forma segura las herramientas obsoletas.
f) Educar a los empleados para el manejo de bases de datos: Capacitar a los empleados acerca de las vulnerabilidades, construir una cultura de seguridad en la cual todo el mundo entienda el valor crítico de sus datos.

7.2.3. Tratamiento de la Información:

La Universidad, actuando en calidad de Responsable del Tratamiento de Datos Personales, para el adecuado desarrollo de sus actividades, así como para el fortalecimiento de sus relaciones con terceros, realiza procesos de recolección, almacenamiento, uso, circulación o supresión correspondientes a personas naturales con quienes tiene o ha tenido relación, sin que la enumeración signifique limitación, funcionarios, trabajadores oficiales y familiares de éstos, clientes, distribuidores, contratistas, proveedores, acreedores y deudores.
Los datos personales contenidos en bases de datos podrán ser tratados de manera automatizada o manual.

- Son bases de datos manuales, los archivos cuya información se encuentra organizada y almacenada de manera física.
- Son bases de datos automatizadas, aquellas que se almacenan y administran con la ayuda de herramientas informáticas.

Se prohíbe el tratamiento de datos sensibles, excepto cuando:

a) El titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.

b) El tratamiento sea necesario para salvaguardar el interés vital del titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.

c) El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

d) El tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares.

7.2.4. Derechos de los niños, niñas y adolescentes:

Según lo dispuesto por el Artículo 7º de la Ley 1581 de 2012 y el Artículo 12 del Decreto 1377 de 2013, La Universidad sólo realizará el Tratamiento, esto es, la recolección, almacenamiento, uso, circulación y/o supresión de Datos Personales, salvo aquellos datos que sean de naturaleza pública; para lo cual dicho tratamiento debe cumplir con los siguientes parámetros y requisitos:

a) Que responda y respete el interés superior de los niños, niñas y adolescentes.
b) Que se asegure el respeto de sus derechos fundamentales.
Cumplidos los anteriores requisitos, La Universidad deberá obtener la autorización del representante legal del niño, niña o adolescente, previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

7.2.5. Uso, suministro y circulación de la información

La información personal recolectada tendrá un tratamiento conforme a la finalidad de los datos y para el suministro de la información al titular previa autorización; de la misma manera se podrá suministrar a los operadores autorizados para su administración, de manera verbal o escrita, o puesta a disposición de las siguientes personas y en los siguientes términos:

a) A los titulares, a los terceros debidamente autorizadas por estos o por la ley y a sus causahabientes o sus representantes legales.

b) A los usuarios de la información, dentro de los parámetros de la ley 1266 de 2008 Habeas Data.

c) A cualquier autoridad judicial, previa orden judicial.

d) A las entidades públicas o administrativas en el ejercicio de sus funciones legales o de orden judicial.

e) A los órganos de control y demás dependencias de investigación disciplinaria, fiscal, o administrativa, cuando la información sea necesaria para el desarrollo de una investigación en curso.

f) A otros operadores de datos, cuando se cuente con autorización del titular, o cuando sin ser necesaria la autorización del titular el banco u operador de datos de destino tenga la misma finalidad o una finalidad que comprenda la que tiene el operador que entrega los datos. Si el receptor de la información fuere un banco de datos extranjero, la entrega sin autorización del titular sólo podrá realizarse dejando constancia escrita de la entrega de la información y previa verificación por parte del operador de que las leyes del país

respectivo o el receptor otorgan garantías suficientes para la protección de los derechos del titular.

7.2.6. Conservación de la información:

Las bases de datos deberán ser conservadas por el tiempo del cumplimiento de una obligación legal o contractual; sin embargo de acuerdo a las disposiciones de Debida Diligencia frente a los posibles riesgos en términos del Lavado de Activos y de la Financiación al Terrorismo, luego de terminada la relación, todos los registros, tanto locales como internacionales podrán estar por un periodo de al menos cinco (5) años, para que estas puedan cumplir con las peticiones de información emanadas de las autoridades competentes. No obstante, el titular de los datos personales podrá solicitar en cualquier momento la eliminación de sus datos.

Estos registros deben ser suficientes para permitir la reconstrucción de identificación individual de manera tal que se ofrezca evidencia, de ser necesario, para procesamiento de una actividad criminal; una vez cumplida la o las finalidades, deberán proceder a la supresión de los datos personales en su posesión.

Se debe conservar la información en las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. Se debe mantener copia de la autorización otorgada por el Titular.

7.2.7. Eliminación, supresión de Datos Personales:

Esta información recolectada tendrá como disposición final la eliminación de la Base de Datos original, dejando el registro en una Base de Datos destinada al reconocimiento de eliminación de esta información, la cual no estará sujeta a ningún tipo de tratamiento.
La información relacionada a la seguridad nacional, así como para la prevención, detección, monitoreo y control del lavado de activos y el financiamiento al terrorismo, como la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países, no es sujeta a eliminación o supresión.

7.3. Protocolos

En materia de seguridad y privacidad de la información, se estipula la elaboración de unos protocolos de respuesta que se anticipen a riesgos y/o acciones que conlleven una vulnerabilidad de seguridad. Previéndose junto con lo anterior, mecanismos para rendir informes internos y reportar incidentes de seguridad y privacidad a titulares de la información, la Superintendencia de Industria y Comercio y Alta Dirección.

Teniendo en cuenta lo anterior, la Universidad Surcolombiana establecerá los protocolos ante las violaciones a los códigos de seguridad que ponen en riesgo la información de los titulares y son causantes de impactos muy significativos a la reputación.

Se debe tener en cuenta los riesgos internos y externos, que permitan identificar sus vulnerabilidades a tiempo y enfocar los recursos para la adopción de medidas de mitigación de riesgos que minimicen dicho impacto tanto para la organización como para los titulares de la información. Para implementar estos protocolos, la Universidad Surcolombiana como mínimos de contar con:

- Una persona responsable para manejar los incidentes o vulneraciones a los sistemas de información donde se gestionan datos personales y a los archivos físicas.

- Establecer los canales para rendir informes internos y reportar los incidentes a los titulares, al Oficial de Protección de Datos y a la Superintendencia de Industria y Comercio.

- Definir canales de comunicación de manera eficiente con los titulares para informarles:

i. Los incidentes de seguridad relacionado con el uso de datos personales y las posibles consecuencias.
ii. Proporcionar herramientas a dichos titulares afectados para minimizar el daño potencial o causado.

8. Registro Nacional en la Base de Datos (RNBD)

Serán objeto de inscripción en el Registro Nacional de Bases de Datos, las bases de datos que contengan datos personales cuyo tratamiento automatizado o manual se realice por personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano o fuera de él, en este último caso, siempre que la Universidad le es aplicable la legislación colombiana en virtud de normas y tratados internacionales.

Se deberán inscribir en el RNBD de manera independiente, cada una de las bases de datos que contengan datos personales sujetos a tratamiento. La Información mínima que debe contener el Registro Nacional de Bases de Datos es la siguiente:

a) Datos de identificación, ubicación y contacto

b) Datos de identificación, ubicación y contacto del o de los Encargados del Tratamiento de la base de datos (si los hay).

c) Canales para que los titulares ejerzan sus derechos.

d) Nombre y finalidad de la base de datos.

e) Forma de tratamiento de la base de datos (manual y/o automatizada), y

f) Política de tratamiento de la información.

Por último, se debe inscribir, de acuerdo con la Circular Externa 002 de la SIC:

a) Información almacenada en la base de datos: Es la clasificación de los datos personales almacenados en cada base de datos, agrupados por categorías y subcategorías, de acuerdo con la naturaleza de los mismos.

b) Medidas de Seguridad de la Información: Corresponde a los controles implementados por el responsable del tratamiento para garantizar la seguridad de las bases de datos que está registrando, teniendo en cuenta las preguntas dispuestas para el efecto en el RNBD.

c) Procedencia de los datos personales: La procedencia de los datos se refiere a si estos son recolectados del titular de la información o suministrados por terceros y si se cuenta con la autorización para el tratamiento o existe una causal de exoneración, de acuerdo con lo establecido en el art. 10 de la ley 1581 de 2012.

d) Transferencia internacional de datos personales: La información relacionada con la transferencia internacional de datos personales comprende la identificación del destinatario como responsable del tratamiento, el país en el que este se encuentra ubicado y si la operación está cobijada por una declaración de conformidad emitida por la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio.

e) Transmisión internacional de datos personales: La información relacionada con la transmisión internacional de datos comprende la identificación del destinatario como encargado del tratamiento, el país en el que este se encuentra ubicado, si se tiene un contrato de transmisión de datos en los términos señalados en el Artículo 2.2.2.25.5.2 de la sección 5 del capítulo 25 del Decreto Único 1074 de 2015 o si la operación está cobijada por una declaración de conformidad emitida por la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio.

f) Cesión o transferencia nacional de la base de datos: La información relacionada con la cesión o transferencia nacional de datos incluye la identificación del cesionario, quien se considerará responsable del tratamiento de las bases de datos cedida a partir del momento en que se perfeccione la cesión. No es obligatorio para el cedente registrar la cesión de la base de datos. Sin embargo, el cesionario, como responsable del tratamiento, debe cumplir con el registro de la base de datos que ha sido cedida.

g) Responsable de novedades: Una vez finalizada la inscripción de la Base de Datos en el RNBD, se reportan como novedades los reclamos presentados por los titulares y los incidentes de seguridad que afecten la base de datos, de acuerdo con las siguientes reglas:

h) Reclamos presentados por los titulares: Corresponde a la información de los reclamos presentados por los titulares ante el responsable y/o el encargado del tratamiento, según sea el caso, dentro de un semestre calendario (enero – junio y julio – diciembre). Esta información se debe registrar teniendo en cuenta lo manifestado por los titulares y los tipos de reclamos prestablecidos en el registro. El reporte deberá ser resultado de consolidar los reclamos presentados por los Titulares ante el responsable y el (los) encargado (s) del tratamiento.

i) Incidentes de Seguridad: Se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el responsable del tratamiento o por su encargado, que deberán reportarse al RNBD dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.

j) La información relacionada con las medidas de seguridad, los reclamos presentados por los titulares y los incidentes de seguridad no estará disponible para consulta pública.

k) Las bases de datos que se creen con posterioridad deberán inscribirse dentro de los dos (2) meses siguientes, contados a partir de su creación.

l) Actualización de la Información contenida en el Registro Nacional en la Base de Datos.

m) Deberán actualizar en el Registro Nacional de Bases de Datos la información inscrita cuando haya cambios sustanciales. La información contenida en el RNBD deberá actualizarse: (i) Dentro de los primeros diez (10) días hábiles de cada mes, a partir de la inscripción de la base de datos, cuando se realicen cambios sustanciales en la información registrada; y (ii) Anualmente, entre el 2 de enero y el 31 de marzo, a partir de la inscripción de la base de datos, independientemente de que, durante dicho año, se hayan realizado actualizaciones de acuerdo con lo dispuesto en ítem (i) de este artículo.

n) Cambios sustanciales: Son aquellos cambios que se relacionen con la finalidad de la base de datos, el Encargado del tratamiento, los canales de atención del titular, la clasificación o tipo de

datos personales almacenados en cada base de datos, las medidas de seguridad de la información implementadas, la política de tratamiento de la información y la transferencia y transmisión internacional de datos personales.

Adicionalmente, dentro de los quince (15) primeros días hábiles de los meses de febrero y agosto de cada año, a partir de su inscripción, los responsables del Tratamiento deben actualizar la información de los reclamos presentados por los titulares, referida en el número (i) del literal g) del numeral del punto 17.2.3. anterior. El primer reporte de reclamos presentados por los titulares se deberá realizar en el primer semestre de 2021 con la información que corresponda al segundo semestre del 2020.

9. Gestión de Incidentes de Seguridad y Privacidad de la Información

La Universidad se apoya en el Grupo de Respuesta a Incidentes de Seguridad y Privacidad de la Información creado mediante Resolución 120 de 2023 para la gestión adecuada de incidentes que afecten la confidencialidad, integridad o disponibilidad de los datos personales.

Las responsabilidades y procedimientos para el manejo de incidentes están definidos en la mencionada resolución, y todos los incidentes deberán ser reportados de acuerdo con las siguientes normas:

a) Los incidentes de seguridad relacionados con datos personales deben ser reportados a la Superintendencia de Industria y Comercio dentro de los quince (15) días hábiles siguientes al momento en que se detecten.

b) El reporte debe incluir:

- Detalles del incidente
- Tipo de datos afectados
- Cantidad de titulares afectados
- Medidas técnicas y administrativas correctivas implementadas

c) Se debe informar a los titulares afectados cuando el incidente pueda poner en riesgo sus derechos.

d) Todos los incidentes de seguridad deben ser documentados como parte del análisis posterior al incidente para implementar mejoras.

10. Derechos de los Titulares y Procedimientos

10.1 Derechos de los titulares

La Universidad Surcolombiana reconoce y garantiza los siguientes derechos a los titulares de datos personales conforme a la Resolución No. 209 de 2023:

a) Conocer, actualizar y rectificar sus datos personales frente a los responsables del tratamiento o encargados del tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.

b) Solicitar prueba de la autorización otorgada al responsable del tratamiento salvo cuando expresamente se exceptúe como requisito para el tratamiento, de conformidad con lo previsto en el Artículo 10 de la Ley 1581 de 2012.

c) Ser informado por el responsable del tratamiento o el encargado del tratamiento, previa solicitud, respecto del uso que se ha dado a sus datos personales.

d) Revocar la autorización y/o solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. Para ello el Comité pondrá a disposición un formato que permita ejercer el derecho de autodeterminación informativa.

e) Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento, dentro de los límites de las funciones propias de la Universidad.

10.2 Procedimiento para ejercer derechos

La Universidad establece el siguiente procedimiento para atender las solicitudes de los titulares:

a) Canales de atención: Los titulares pueden ejercer sus derechos a través de:
- Correo electrónico: habeasdata@usco.edu.co
- Oficina física: Sede Central, Av. Pastrana Borrero - Cra. 1

b) Requisitos de la solicitud: La solicitud debe contener:
- Identificación del titular
- Descripción de los hechos que dan lugar a la solicitud
- Dirección física o electrónica para recibir respuesta
- Documentos que sustenten la solicitud (cuando aplique)

c) Plazos de respuesta:
- Consultas: Diez (10) días hábiles, prorrogables por cinco (5) días hábiles más.
- Reclamos: Quince (15) días hábiles, prorrogables por ocho (8) días hábiles más

Procedimiento específico:

1. Recepción de la solicitud
2. Verificación de la identidad del titular
3. Análisis y trámite de la solicitud
4. Respuesta al titular
5. Implementación de las acciones requeridas

El Oficial de Protección de Datos Personales es el encargado de gestionar las solicitudes y coordinar con las dependencias correspondientes para dar respuesta al titular.

11. Capacitación y Sensibilización

En consideración a que el régimen de protección de datos personales es un asunto que exige el conocimiento de todos los niveles de la Universidad, deberán diseñarse programas de capacitación que tengan por objeto, dar a conocer las obligaciones propias del régimen de protección de datos personales, así como las medidas implementadas por la Universidad en el marco del cumplimiento a la Ley 1581 de 2012 y decretos reglamentarios. Junto con la capacitación de carácter general, deberá diseñarse capacitaciones complementarias que se

encuentren adaptadas a las funciones de cada dependencia o funcionario que realiza el tratamiento de información personal.

Teniendo en cuenta lo anterior, se desarrollarán programas de formación y educación de todos los empleados de la Universidad que en el día a día trata datos personales como parte de sus funciones. Estos programas incluirán una formación de carácter general sobre la materia, y para la persona que maneje todos los datos personales directamente, deberá existir una capacitación complementaria adaptada específicamente a sus funciones. Se realizará un entrenamiento general en protección de datos personales para todos los funcionarios de la Universidad, teniendo en cuenta:

a) El programa de entrenamiento debe ser dirigido de igual manera a los nuevos empleados y/o contratistas, que tengan acceso por las condiciones de su empleo, a datos personales gestionados por la Universidad.

b) Los contenidos de estos programas deberán ser actualizados por lo menos una vez al año o cuando se presenten cambios a la finalidad del tratamiento de la información, de las políticas, procesos y procedimientos.

c) Las políticas de protección de datos se deben integrar dentro de las actividades de las dependencias de la Universidad, medir la participación, y calificar el desempeño, en los entrenamientos de protección de datos personales, el cual debe haber contemplado satisfactoriamente el entrenamiento.

12. Evaluación y Mejora Continua

El Programa Integral de Gestión de Datos Personales exige una evaluación y revisión continua de los controles que lo integran, con el fin de determinar la pertinencia y eficacia del plan de gestión. En consecuencia, el Oficial de Protección de Datos Personales será la persona encargada al interior de la organización de desarrollar un plan de supervisión y revisión anual que tome en cuenta las siguientes etapas:

1. Fase de diagnóstico: En ella deberá evaluarse en qué estado de cumplimiento se encuentra la organización, acudiéndose, entre otras, a:
   Elaboración de auditorías internas
   Debilidades identificadas en la atención de consultas y reclamos
   Revisión de las tendencias y obligaciones legales que surjan con ocasión a la protección de datos personales
2. Fase de adecuación: Consiste en determinar las acciones a implementar por la Universidad, en aras de hacer más efectivo el Plan Integral de Gestión de Datos Personales.
3. Fase de implementación: Previa aprobación del Comité de Seguridad y Privacidad de la Información de la Universidad, efectuar los cambios que resulten pertinentes en los componentes del Programa Integral de Gestión de Datos Personales. Con acciones de capacitación al personal.
4. Fase de revisión: La guía para la implementación del principio de responsabilidad demostrada, exige que la revisión del Programa Integral de Gestión de Datos Personales sea anual, sin embargo, nada impide que, en razón a la debida diligencia, la Universidad efectúe revisiones periódicas de las acciones implementadas.

Control de Cambios

VERSIÓN	FECHA	DESCRIPCIÓN
1.0	20-04-2021	Versión inicial
2.0	20-10-2025	Actualización conforme a Resoluciones de Rectoría Nro. 120, 209 y 255 de 2023. Se incluye en la presente versión los apartados de: 9. Gestión de Incidentes de Seguridad y Privacidad de la Información, 10. Derechos de los titulares y procedimientos, 11. Capacitación y sensibilización; 12. Evaluación y mejora.