

	MACROPROCESO DE APOYO	CÓDIGO: ADOr006
	PROCESO GESTIÓN DOCUMENTAL	VERSIÓN: 10
	INFORME	VIGENCIA: 2024-09-02
		PAGINA: 1 de 10

13.1

Fusagasugá, 2025-11-27

Para: Doctora **ADRIANA ASENCIÓN TORRES ESPITIA**
Directora de Planeación Institucional
Universidad de Cundinamarca

Asunto: Respuesta “Solicitud de Informes Finales para la Quinta Sesión Ordinaria de la Comisión de Desempeño Institucional – Vigencia 2025”

El Sistema de Gestión de Seguridad de la Información - SGSI adelanta sus actividades de identificación, análisis, valoración y tratamiento de riesgos en cumplimiento de lo establecido en los numerales 6.1 “Acciones para abordar riesgos y oportunidades”, 8.2 “Evaluación de riesgos de la seguridad de la información” y 8.3 “Tratamiento de riesgos de la seguridad de la información” de la Norma ISO/IEC 27001:2022. Asimismo, se acoge a los lineamientos definidos en la “Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas” del Departamento Administrativo de la Función Pública - DAFP y en la Guía No. 7 “Gestión de Riesgos” del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC.

En concordancia con el marco normativo y metodológico, la gestión institucional del riesgo se desarrolla conforme a lo dispuesto en el procedimiento ESG-SSI-P12 “Gestión de Riesgos de Seguridad de la Información” y en el documento ESG-SSI-PL04 “Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información”, los cuales orientan la ejecución de las actividades del SGSI en la Universidad de Cundinamarca.

1. Logros alcanzados

Durante la vigencia 2025, el Sistema de Gestión de Seguridad de la Información - SGSI avanzó de manera significativa en la consolidación de la estrategia institucional de gestión de riesgos, dando cumplimiento a los lineamientos establecidos por la Norma ISO/IEC 27001:2022 y al Modelo de Seguridad y Privacidad de la Información - MSPI. A lo largo del año, se lograron los siguientes resultados:

Gestión y valoración de riesgos

- El SGSI realizó las jornadas de Socialización y construcción de 45 matrices de riesgos de 50 que habían proyectadas para los procesos y áreas que registraron activos de información con criticidad alta en la plataforma institucional.

Diagonal 18 No. 20-29 Fusagasugá – Cundinamarca
Teléfono: (601) 8281483 Línea Gratuita: 018000180414
www.ucundinamarca.edu.co E-mail: info@ucundinamarca.edu.co
NIT: 890.680.062-2

	MACROPROCESO DE APOYO	CÓDIGO: ADOr006
	PROCESO GESTIÓN DOCUMENTAL	VERSIÓN: 10
	INFORME	VIGENCIA: 2024-09-02
		PAGINA: 2 de 10

Las siguientes áreas no atendieron la convocatoria del SGSI a pesar de los reiterados correos en búsqueda de lograr una mesa de trabajo, por lo que no fue posible identificar, analizar, valorar ni tratar los riesgos asociados a sus activos de información críticos registrados en la plataforma institucional:

Tabla 1 Áreas que no tienen matriz de riesgos del SGSI

MACROPROCESO	PROCESO	AREA
Estratégico	Planeación Institucional	Seccional Girardot
		Extensión Soacha
Misional	Formación y Aprendizaje	Vicerrectoría Académica
		Facultad de Educación
		Facultad de Ciencias de la Salud

- Se elaboraron 42 planes de tratamiento de riesgos, que fueron aprobados mediante acta por los líderes responsables.
Adicionalmente, 3 áreas mantuvieron un riesgo residual en nivel aceptable, con compromiso de fortalecer los controles existentes.

Tabla 2 Áreas que tienen matriz de riesgos, pero en estado aceptable

AREAS QUE TIENEN MATRIZ DE RIESGOS, PERO EN ESTADO ACEPTABLE
Oficina de Desarrollo Académico
Extensión Zipaquirá
Facultad de Ciencias Sociales, Humanidades y Ciencias Políticas

- Se realizó seguimiento a la ejecución de estos planes durante todo el año, incluyendo verificación de controles, revisión de acciones implementadas y articulación con los líderes de proceso.
- Durante el segundo semestre de la vigencia 2025 se realizó la actualización de las matrices de riesgos correspondientes a la Oficina de Tesorería, la Dirección de Sistemas y Tecnología y la Oficina de Educación Virtual y a Distancia, en atención a la materialización de incidentes de seguridad de la información en esas áreas. Estas actualizaciones permitieron recalcular el riesgo residual, ajustar los controles existentes y definir acciones adicionales para fortalecer la gestión y mitigación del riesgo, como se detalla a continuación:

Tipos de activos de la información

- TH: Talento Humano
- HW: Hardware
- IN: Información
- SE: Servicios
- IL: Instalaciones

Diagonal 18 No. 20-29 Fusagasugá – Cundinamarca
Teléfono: (601) 8281483 Línea Gratuita: 018000180414
www.ucundinamarca.edu.co E-mail: info@ucundinamarca.edu.co
NIT: 890.680.062-2

	MACROPROCESO DE APOYO	CÓDIGO: ADOr006
	PROCESO GESTIÓN DOCUMENTAL	VERSIÓN: 10
	INFORME	VIGENCIA: 2024-09-02
		PAGINA: 3 de 10

- SW: Software

Riesgos

- R1: Pérdida de confidencialidad
- R2: Pérdida de integridad
- R3: Pérdida de disponibilidad

Tabla 3 Consolidado de Riesgos de Seguridad v Privacidad de la Información materializados a nivel institucional

PROCESO	ÁREA	DESCRIPCIÓN DEL RIESGO	NIVEL DE RIESGO	IMPACTO
Financiera	Oficina de Tesorería	(IN - R3) Pérdida de disponibilidad del portal bancario.	Alto	Mayor
Sistemas y Tecnología	Dirección de Sistemas y Tecnología	(SE-R3) Riesgo por gestión de capacidad en el almacenamiento en el OneDrive.	Alto	Mayor
Formación y Aprendizaje	Oficina de Educación Virtual y a Distancia	(SE-R3) Pérdida de disponibilidad de la información debido a la ausencia de documentación.	Alto	Moderado

Informes institucionales remitidos a entes de control:

- El SGSI presentó dos informes a la Dirección de Control Interno relacionados con riesgos residuales altos y extremos:
-9 de abril de 2025
-16 de septiembre de 2025
- El 29 de octubre de 2025, se presentó el Informe de Entradas de Revisión por la dirección del SGSI, en el cual se socializaron los resultados de la evaluación de riesgos y estado del plan de tratamiento de riesgos, el estado de los planes de tratamiento y los incidentes materializados durante la vigencia.

Incidentes materializados durante la vigencia 2025

Como parte del proceso de seguimiento al riesgo residual institucional, durante el año se registraron tres incidentes materializados, los cuales fueron atendidos, analizados y documentados:

I. Incidente del portal bancario Davivienda – Oficina de Tesorería:

Diagonal 18 No. 20-29 Fusagasugá – Cundinamarca
Teléfono: (601) 8281483 Línea Gratuita: 018000180414
www.ucundinamarca.edu.co E-mail: info@ucundinamarca.edu.co
NIT: 890.680.062-2

	MACROPROCESO DE APOYO	CÓDIGO: ADOr006
	PROCESO GESTIÓN DOCUMENTAL	VERSIÓN: 10
	INFORME	VIGENCIA: 2024-09-02
		PAGINA: 4 de 10

Se presentaron bloqueos de portales bancarios debido a intentos de acceso desde equipos personales sin antivirus por parte de Gestores del Conocimiento.

El SGSI emitió recomendaciones, realizó visitas de verificación, coordinó sesiones técnicas con Davivienda y apoyó la investigación adelantada por el equipo de Ciberseguridad del Banco, dejando como respaldo el acta No. 211 del 15 de septiembre de 2025.

II. Incidente por cambio de políticas de almacenamiento – Dirección de Sistemas y Tecnología:

Microsoft 365 Education modificó sus políticas de almacenamiento, generando indisponibilidad y sobrecarga en OneDrive.

La Dirección de Sistemas implementó medidas de contingencia que incluyeron depuración masiva de cuentas y grupos de Teams, eliminación de información obsoleta y acciones de optimización que permitieron liberar un estimado de 57,7 TB, mitigando el impacto sobre los usuarios institucionales.

III. Incidente de supresión de información en Moodle – Oficina de Educación Virtual y a Distancia:

Se presentó la eliminación de información en la plataforma Moodle debido a la ejecución de un script que suprimió cursos de forma no controlada, situación originada por la ausencia de lineamientos, manuales y procedimientos formales que regulen su administración. Si bien el incidente fue atendido y corregido de manera oportuna, se clasificó como un riesgo alto debido a la inexistencia de documentos normativos que orienten la gestión operacional de la plataforma.

IV. Acciones complementarias de gestión durante el año

- Se elaboró una matriz de riesgos específica para el proceso de migración del portal web institucional, liderado por la Oficina Asesora de Comunicaciones. El instrumento permitió identificar amenazas, analizar los impactos asociados y definir los controles necesarios para asegurar la continuidad operativa durante todas las etapas de la migración. Esta matriz constituye la base para el plan de mitigación que deberá implementarse antes y durante la puesta en producción del nuevo portal. El documento fue remitido a la Oficina Asesora de Comunicaciones el 22 de septiembre de 2025, con el propósito de que se adopten las acciones correspondientes para reducir el impacto de los riesgos inherentes al proceso de migración.
- Se solicitó la actualización del documento consolidado ESG-SSI-F041 – Matrices de Riesgos del SGSI, permitiendo su consulta en el Modelo de Operación Digital.

	MACROPROCESO DE APOYO	CÓDIGO: ADOr006
	PROCESO GESTIÓN DOCUMENTAL	VERSIÓN: 10
	INFORME	VIGENCIA: 2024-09-02
		PAGINA: 5 de 10

Con respecto a la matriz de riesgos para la Protección de Datos Personales correspondiente a las bases de datos institucionales de la Universidad de Cundinamarca se identificaron los factores de riesgo inherentes de cada base de datos, los controles existentes y el nivel de riesgo residual estimado.

Según el análisis se cubrió un total de 31 riesgos correspondientes a:

- **27 bases de datos específicas (PDP-R1 a PDP-R27)**
- **4 riesgos transversales institucionales (PDP-R28 a PDP-R31)** asignados al Oficial de Protección de Datos Personales (OPD) por su naturaleza general.

Cada una de las bases de datos fue evaluada en relación con:

- Factores de riesgo asociados.
- Consecuencias potenciales.
- Riesgo inherente.
- Controles existentes (procedimentales y tecnológicos).
- Riesgo residual estimado.

Las bases de datos analizadas fueron:

- PDP-R1 DESARROLLO DEL CICLO ACADEMICO DE LOS ESTUDIANTES
- PDP-R2 GESTIÓN DE LAS AUTORIZACIONES PARA EL TRATAMIENTO DE DATOS PERSONALES DE ESTUDIANTE
- PDP-R3 BASE DE DATOS DE QUEJOSOS
- PDP-R4 ESCUELAS DE FORMACION Y CLUBES DEPORTIVOS UCUNDINAMARCA
- PDP-R5 PARTICIPACIÓN ACTIVIDADES DE B.U.
- PDP-R6 Software Documental SAIA
- PDP-R7 BASE DE DATOS DE ASPIRANTES Y PROCESO DE ADMISION
- PDP-R8 Periodistas
- PDP-R9 FIRMAS DIGITALES
- PDP-R10 Formulario Acceso Personal Externo
- PDP-R11 Banco de Proveedores
- PDP-R12 USUARIOS Y PRIVILEGIOS DE PLATAFORMA INSTITUCIONAL
- PDP-R13 BASE DE DATOS CONTRATACION ORDENES DE PRESTACION DE SERVICIOS
- PDP-R14 PERSONAL VINCULADO A LA UNIVERSIDAD DE CUNDINAMARCA – FÍSICA
- PDP-R15 PERSONAL VINCULADO A LA UNIVERSIDAD DE CUNDINAMARCA
- PDP-R16 Preinscritos 2024-
- PDP-R17 INSCRITOS EN EDUCACION CONTINUADA PROGRAMA DE MUSICA
- PDP-R18 CASSA UDEC

Diagonal 18 No. 20-29 Fusagasugá – Cundinamarca
Teléfono: (601) 8281483 Línea Gratuita: 018000180414
www.ucundinamarca.edu.co E-mail: info@ucundinamarca.edu.co
NIT: 890.680.062-2

	MACROPROCESO DE APOYO	CÓDIGO: ADOr006
	PROCESO GESTIÓN DOCUMENTAL	VERSIÓN: 10
	INFORME	VIGENCIA: 2024-09-02
		PAGINA: 6 de 10

- PDP-R19 CUERPOS COLEGIADOS DE LA UNIVERSIDAD DE CUNDINAMARCA
- PDP-R20 Base de datos convenio C-20230512-027
- PDP-R21 UNIDAD AMIGA DE LOS ADOLESCENTES Y JOVENES
- PDP-R22 CONVENIOS INTERNACIONALES
- PDP-R23 AUTOEVALUACION DE SINTOMAS COVID – 19
- PDP-R24 GRADUADOS
- PDP-R25 Codeudores de Fr, Acp, Dn (Física)
- PDP-R26 Codeudores, Fr, Acp, Dn
- PDP-R27 BD Estudiantes Instituto de Posgrados

En todas ellas se identificaron los siguientes factores de riesgo recurrentes:

- Acceso no autorizado o fraudulento
- Uso no autorizado por parte del responsable
- Adulteración no autorizada
- Eliminación no autorizada

Y se documentaron sus posibles consecuencias, siempre estando presentes:

- Sanciones legales
- Daño reputacional
- Afectación misional
- Violación de principios de protección de datos personales

El riesgo inherente de cada base de datos se asignó considerando:

- Naturaleza y sensibilidad de los datos
- Volumen
- Exposición tecnológica o física
- Procesos que lo administran
- Rol del responsable

Para cada base de datos se identificaron los controles actualmente implementados en la Universidad, entre ellos:

Controles tecnológicos

- Autenticación y gestión de privilegios
- Accesos restringidos
- Seguridad perimetral
- Bitácoras y registros de acceso
- Configuraciones de seguridad en sistemas

Controles procedimentales

- Uso de autorizaciones de tratamiento
- Custodia documental
- Procedimientos institucionales

Diagonal 18 No. 20-29 Fusagasugá – Cundinamarca
Teléfono: (601) 8281483 Línea Gratuita: 018000180414
www.ucundinamarca.edu.co E-mail: info@ucundinamarca.edu.co
NIT: 890.680.062-2

	MACROPROCESO DE APOYO	CÓDIGO: ADOr006
	PROCESO GESTIÓN DOCUMENTAL	VERSIÓN: 10
	INFORME	VIGENCIA: 2024-09-02
		PAGINA: 7 de 10

- Roles y responsabilidades definidas
- Protocolos de recepción, administración y actualización de la información

A cada control se le asignó:

- Custodio
- Naturaleza (tecnológico / procedimental)
- Tipo (preventivo, detectivo, correctivo)
- Frecuencia del control
- Frecuencia adecuada esperada
- Mecanismo de monitoreo
- Frecuencia de monitoreo
- Categoría del control

El riesgo residual se estimó teniendo en cuenta la eficacia de los controles identificados. Esta calificación muestra qué tan mitigado queda el riesgo luego de aplicar las medidas existentes

La matriz se encuentra en versión borrador técnico, pues:

- Las calificaciones de riesgos y controles fueron asignadas con base en los insumos actuales.
- Cada proceso debe validar los riesgos que le pertenecen.
- Cada responsable debe confirmar si los controles identificados son correctos o si existen adicionales.

En conjunto, estos resultados evidencian una gestión integral del riesgo durante la vigencia 2025, consolidando avances en la identificación, tratamiento y seguimiento de riesgos institucionales, fortaleciendo además la capacidad de respuesta ante incidentes y asegurando mejoras continuas en los niveles de protección de la información.

2. Contratiempos presentados – Vigencia 2025

Durante la vigencia 2025 se presentaron diversas situaciones que afectaron el desarrollo normal de algunas actividades programadas dentro del Sistema de Gestión de Seguridad de la Información - SGSI. Entre los principales contratiempos se destacan:

- Rotación de personal en el SGSI, derivada de la salida de varios ingenieros encargados de tareas técnicas y de apoyo operativo.
Esta situación generó retrasos en la ejecución de actividades planificadas, así como en la continuidad de procesos relacionados con la gestión del riesgo y el acompañamiento a las áreas institucionales.
- Limitaciones para realizar jornadas de sensibilización y entrenamiento en Seguridad y Privacidad de la Información.

Diagonal 18 No. 20-29 Fusagasugá – Cundinamarca
Teléfono: (601) 8281483 Línea Gratuita: 018000180414
www.ucundinamarca.edu.co E-mail: info@ucundinamarca.edu.co
NIT: 890.680.062-2

	MACROPROCESO DE APOYO	CÓDIGO: ADOr006
	PROCESO GESTIÓN DOCUMENTAL	VERSIÓN: 10
	INFORME	VIGENCIA: 2024-09-02
		PAGINA: 8 de 10

Debido al proceso institucional de acreditación de alta calidad, múltiples áreas estuvieron en reuniones permanentes, lo que impidió la programación y ejecución de las jornadas de sensibilización y entrenamiento previstas en el cronograma del SGSI.

- Debido al incidente relacionado con el servicio de almacenamiento en OneDrive, se generó una indisponibilidad temporal y obligó a replantear la operación programada. Debido a un cambio inesperado en las políticas de Microsoft 365 Education, no fue posible aplicar el control de bloqueo de puertos USB, ya que fue necesario permitir de forma temporal el uso de dispositivos externos para que las áreas pudieran continuar gestionando y resguardando su información crítica.
- Se presentaron dificultades de articulación con algunas áreas institucionales (Seccional Girardot, Extensión Soacha, Vicerrectoría Académica, Facultad de Educación y Facultad de Ciencias de la Salud), lo que generó retrasos en la consolidación oportuna del seguimiento anual de los riesgos.

Estos contratiempos representaron desafíos significativos en la vigencia 2025, afectando tanto la ejecución del cronograma del SGSI como la implementación de controles clave para la mitigación de riesgos institucionales.

3. Recomendaciones

Con el fin de fortalecer la gestión institucional del riesgo de seguridad de la información y mejorar la eficacia del SGSI en la vigencia 2026, se formulan las siguientes recomendaciones:

- Planificar y definir la estrategia institucional para el tratamiento de riesgos 2026, estableciendo cronogramas, responsables y recursos requeridos, con el fin de asegurar un proceso ordenado y sistemático desde el inicio del año.
- Avanzar en la implementación del Frente de Continuidad del Negocio, correspondiente a la Etapa 5 del Sistema de Gestión de Seguridad de la Información, incluyendo:
 - Análisis de impacto al negocio (BIA).
 - Estrategias de continuidad.
 - Procedimientos operativos.

Esto permitirá fortalecer la capacidad de resiliencia institucional ante incidentes o interrupciones imprevistas.

- Fortalecer y documentar la gestión del cambio para los procesos, plataformas, infraestructuras y servicios relacionados con el SGSI,

Diagonal 18 No. 20-29 Fusagasugá – Cundinamarca
 Teléfono: (601) 8281483 Línea Gratuita: 018000180414
www.ucundinamarca.edu.co E-mail: info@ucundinamarca.edu.co
 NIT: 890.680.062-2

	MACROPROCESO DE APOYO	CÓDIGO: ADOr006
	PROCESO GESTIÓN DOCUMENTAL	VERSIÓN: 10
	INFORME	VIGENCIA: 2024-09-02
		PAGINA: 9 de 10

garantizando trazabilidad, comunicación adecuada y control sobre los cambios que impactan la información institucional.

- Emitir un pronunciamiento institucional dirigido a las áreas con planes de mejoramiento derivados de auditorías del SGSI, con el objetivo de reforzar el compromiso de los líderes de proceso y asegurar el cumplimiento oportuno de las acciones establecidas.
- Formalizar lineamientos, procedimientos y manuales técnicos relacionados con plataformas críticas como Moodle, Microsoft 365, portales bancarios, servicios en nube y sistemas transversales. Esto permitirá reducir la probabilidad de incidentes derivados de fallas operativas, desconocimiento o ausencia de directrices formales.

Estas recomendaciones permiten orientar la mejora continua del SGSI y servirán como base para optimizar la gestión del riesgo, fortalecer la capacidad institucional y asegurar el cumplimiento de los requisitos establecidos por la Norma ISO/IEC 27001:2022.

4. Metas proyectadas

- Implementar una estrategia de seguimiento trimestral a los riesgos críticos, que permita evaluar de manera continua la eficacia de los planes de tratamiento, mantener actualizado el registro institucional de riesgos y considerar nuevos escenarios derivados de auditorías e incidentes, asegurando una gestión preventiva y alineada con los estándares internacionales.
- Fortalecer los procesos de sensibilización y entrenamiento institucional en seguridad y privacidad de la información, incorporando alternativas como el curso auto gestionable del SGSI, con el propósito de consolidar una cultura organizacional orientada a la protección de la confidencialidad, integridad y disponibilidad de la información.
- Revisar y ajustar la “Matriz de Flujos de Comunicación” del Sistema de Gestión de Seguridad de la Información- SGSI, Ciberseguridad y el Programa Integral de Gestión de Datos Personales - PIGDP, en articulación con el Oficial de Protección de Datos Personales.
- Avanzar en la implementación del Frente de Continuidad del Negocio, incorporando análisis de impacto al negocio (BIA), estrategias de continuidad, procedimientos operativos y pruebas de validación, para asegurar la resiliencia institucional ante interrupciones y sostener la operación de los procesos misionales.
- Emitir pronunciamientos institucionales que refuercen el compromiso con los planes de mejoramiento, promoviendo la responsabilidad de los líderes de proceso y asegurando el cumplimiento oportuno de las

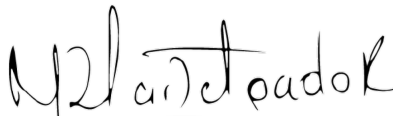
Diagonal 18 No. 20-29 Fusagasugá – Cundinamarca
Teléfono: (601) 8281483 Línea Gratuita: 018000180414
www.ucundinamarca.edu.co E-mail: info@ucundinamarca.edu.co
NIT: 890.680.062-2

*Documento controlado por el Sistema de Gestión de la Calidad
Asegúrese que corresponde a la última versión consultando el Portal Institucional*

	MACROPROCESO DE APOYO	CÓDIGO: ADOr006
	PROCESO GESTIÓN DOCUMENTAL	VERSIÓN: 10
	INFORME	VIGENCIA: 2024-09-02
		PAGINA: 10 de 10

- acciones derivadas de auditorías internas y externas, como parte del fortalecimiento del Sistema de Gestión de Seguridad de la Información.
- VI. Fortalecer la gestión del cambio en procesos, plataformas e infraestructuras, asegurando trazabilidad y control sobre los ajustes que impactan la información institucional, con el objetivo de reducir riesgos asociados a modificaciones no controladas y mantener la estabilidad operativa.
 - VII. Incrementar la resiliencia institucional frente a incidentes, mediante la atención, análisis y cierre oportuno de eventos de seguridad y privacidad, aplicando el ciclo de vida de gestión de incidentes para minimizar impactos operativos, reputacionales y legales.
 - VIII. Optimizar la gestión de activos de información, estableciendo cronogramas y estrategias para su administración y socialización ante la Comisión de Gestión, asegurando que los activos críticos estén identificados y protegidos conforme a su nivel de riesgo.

Cordialmente,



MARÍA DEL PILAR DELGADO RODRÍGUEZ
Coordinadora del Sistema de Gestión de Seguridad de la Información – SGSI

Transcriptor: (Carolina Berrio Osorio, Duvan Felipe Castillo Avila, Danilo Esteban Silva Rey)

Sistema de Gestión de Seguridad de la Información – SGSI

13.1-30.