



UDEC
UNIVERSIDAD DE
CUNDINAMARCA

Sistema de Gestión de **SGSI**
Seguridad de la Información

Jornada de Sensibilización en Seguridad y Privacidad de la Información

Vigencia 2023

www.ucundinamarca.edu.co
Vigilada MinEducación

- 
- | | |
|-----------|---|
| 01 | Presentación del Equipo. |
| 02 | Resultados de las Jornadas de Sensibilización en Seguridad y Privacidad de la Información vigencia 2022 |
| 03 | ¿Por qué debemos participar en las Jornadas de Sensibilización del SGSI? |
| 04 | Roles y Responsabilidades del Sistema de Gestión de Seguridad de la Información en la Universidad de Cundinamarca |
| 05 | Etapas del Modelo de Gestión Integral de Seguridad de la Información |
| 06 | Temas a tratar según la encuesta sobre temas a incluir en las Jornadas de Sensibilización de Seguridad y Privacidad de la Información vigencia 2023 |
| | ¿En qué caso los titulares pueden solicitar la Supresión de Datos Personales? |
| | 6.1 |
| | 6.2 Teletrabajo y sus riesgos |
| 07 | Preguntas y Cierre |

Agenda



**Maria del Pilar
Delgado Rodriguez**

Coordinadora del SGSI



**Eimy Daniela
Melo Rodriguez**

Administradora de empresas



**Brenda Camila
Mesa Roza**

Profesional en Negocios
Internacionales



**Juan David
Lopez Zamora**

Ingeniero de Sistemas



**Gustavo Adolfo
Dominguez Sierra**

Ingeniero de Sistemas



**Lesly Daniela
Reyes Perez**

Ingeniera Electrónica



**Fabian Libardo
Parra Gutierrez**

Ingeniero de Sistemas



**Juan Diego
Burrell Tovar**

Ingeniero de Sistemas

01

Presentación del Equipo

Resolución

No. 140 del 30-11-2022

Por la cual se designa el coordinador del sistema de gestión de seguridad de la información – sgsi y la protección de datos personales de la universidad de cundinamarca.

RESUELVE:

ARTÍCULO PRIMERO –: Designar a la Ingeniera María del Pilar Delgado Rodríguez, identificada con la cédula de ciudadanía No. 51.937.413 de Bogotá y quien se desempeña como Profesional Universitario Código 3010, Grado 14 de la Planta de Personal de la Universidad de Cundinamarca, como Coordinadora del Sistema de Gestión de Seguridad de la Información y la Implementación de la Ley de Protección de los Datos de los Titulares de la Universidad de Cundinamarca, dependiendo de la Dirección de Planeación Institucional.

ARTICULO SEGUNDO. – Comuníquese la presente Resolución para su conocimiento a todas las áreas responsables de la institución.

Se subsana el hallazgo #1 “...por último, en los roles, responsabilidades y autoridad de seguridad de la información, el director de sistemas y tecnología es el mismo director del SGSI, creando conflicto en ejecución de actividades es decir que se presenta como juez y parte.” del plan de mejoramiento #763 asignado al Sistema de Gestión de Seguridad de la Información producto de la Auditoría Interna I del SGSI.

Estadísticas Generales de participación 2022

45%

INDICADOR DE EFICACIA - ASISTENCIA A JORNADAS DE
SENSIBILIZACIÓN

Con corte al día 01 de noviembre del 2022 se relaciona a continuación, el total de funcionarios administrativos y docentes (*excepto docentes hora catedra*) que asistieron a las jornadas de Sensibilización en Seguridad y Privacidad de la Información que se llevaron a cabo los días 06, 07, 09, 12, 19, 21, 26 y 28 de septiembre y los días 05, 10, 20 y 25 de octubre del 2022, para un total de 12 sesiones 8 de ellas de forma presencial y 4 en modalidad virtual dejando una participación de (646), frente al total de funcionarios administrativos y docentes activos en la Universidad de Cundinamarca (1.443), por lo cual el indicador de eficacia es del 45%.

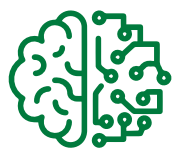
INDICADOR – PLAN DE SENSIBILIZACIÓN					
IDENTIFICADOR		SGIN04			
DEFINICIÓN					
El indicador permite medir la aplicación de los temas sensibilizados en seguridad de la información por parte de los usuarios finales. Estas mediciones se podrán realizar por medio de auditorías especializadas en el tema o de forma aislada por parte de los responsables de la capacitación y sensibilización.					
OBJETIVO					
El objetivo del indicador es establecer la efectividad de un plan de capacitación y sensibilización previamente definido como medio para el control de incidentes de seguridad.					
TIPO INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		FORMULA		FUENTE DE INFORMACIÓN	
VSI07: Número de fallas o no cumplimiento encontrados en las sensibilizaciones programadas o eventos realizados para evaluar el tema.		$(VSI07/VSI08)*100$		Oficial de Seguridad de la Información, auditorías internas, atención al usuario, listas de asistencia	
VSI08: Total de personal a capacitar.				Total de funcionarios de la entidad.	
METAS					
MÍNIMA	75-80%	SATISFACTORIA	80- 90%	SOBRESALIENTE	100%
OBSERVACIONES					
Para el levantamiento de la información que permita obtener datos para la medición el responsable debe idear planes, laboratorios o actividades periódicas que permitan medir lo capacitado o divulgado.					

02

Resultados de
las Jornadas de
Sensibilización
en Seguridad y
Privacidad de
la Información
vigencia 2022

¿Por qué debemos participar en las Jornadas de Sensibilización del SGSI?

Se debe participar porque según la Normatividad:



ISO 27001 numeral 7.3 – Toma de Conciencia



Guía 14 “Plan de Capacitación, sensibilización y comunicación de Seguridad de la Información” - MSPI



Tip 4: Todos los empleados deben conocer las Políticas de Tratamiento de Datos - SIC



ESG-SSI-PL01 Plan de Sensibilización y Entrenamiento en Seguridad y Privacidad de la Información.

03

¿Por qué debemos participaren las Jornadas de Sensibilización del SGSI?

Atendiendo el control A.7.2.3 Proceso Disciplinario de la Norma ISO 27001:2013, la Dirección de Control Disciplinario, envió oficio al Sistema de Gestión de Seguridad de la Información el día 29 de mayo de 2023.

Me dirijo a usted, con el fin de dar claridad sobre los pasos a seguir en cuanto a la recepción de quejas y el procedimiento a seguir establecido en el Acuerdo 003 de 2020 "POR EL CUAL SE ADOPTA EL ESTATUTO DISCIPLINARIO DEL PERSONAL ACADÉMICO Y ADMINISTRATIVO DE LA UNIVERSIDAD DE CUNDINAMARCA, así:

"ARTÍCULO 50. Oficiosidad: La acción disciplinaria se iniciará y adelantará de oficio, o por información proveniente de servidor público o por otro medio que amerite credibilidad, o por queja formulada por cualquier persona, y no procederá por anónimos, salvo en los eventos en que cumpla con los requisitos mínimos consagrados en el Código Único Disciplinario" (subrayado, negrilla y cursiva fuera de texto)

1. En primer lugar, una vez se tenga conocimiento, de alguna presunta conducta irregular por parte de algún funcionario o estudiante, es un deber, de informar a la Oficina de Control Disciplinario.
2. Una vez recibida la queja o informe, en esta Dirección, evaluará lo correspondiente, es decir si apertura indagación o investigación o decisión inhibitoria.

3. Si la decisión de la Dirección, adelanta la falta en que se describe en el numeral

"Custodiar y cuidar el material probado, empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos."

4. Dependiendo del material probado, formular pliego de estudiantes el

Es necesario indicar que cualquier información necesario acudir a cualquier otra dependencia para dar a conocer sobre hechos que atenten contra el buen nombre y buen funcionamiento de la Universidad.

3. Si la decisión es de aperturar indagación o investigación disciplinaria, esta Dirección, adelantará labores investigativas, tendientes a verificar la presunta falta en que se pudo incurrir, para el caso puntual, se tipificará la siguiente falta descrita en el numeral 4 de artículo 10 del citado acuerdo que indica:

"Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos."

Circular No.006 del 24 de Julio de 2023 de Secretaría General



ADOr003_V7

– FUSAGASUGÁ –

Página 1 de 1

12.

CIRCULAR No. 006

DE: ISABEL QUINTERO URIBE
CARGO: SECRETARIA GENERAL
PARA: DIRECTORES DE ÁREA, JEFES DE OFICINA, LIDERES DE PROCESOS, DECANOS Y COORDINADORES DE PROGRAMAS
CIUDAD Y FECHA: FUSAGASUGÁ, 2023-07- 24
ASUNTO: JORNADAS DE SENSIBILIZACIÓN EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Sistema de Gestión de Seguridad de la Información tiene como objetivo asegurar la confidencialidad, integridad y disponibilidad de la información, activo esencial de la institución; por ello, desde el **Plan Institucional de Sensibilización y Entrenamiento en Seguridad y Privacidad de la Información - ESG-SSI-PL01** se establecen los lineamientos y directrices necesarias para el cumplimiento de dicho objetivo. Así las cosas, la Comisión de Gestión en sesión ordinaria del 13 de junio de 2023, **aprobó las jornadas de sensibilización a nivel institucional** con el fin reforzar las buenas practicas e impactar en el comportamiento de los funcionarios administrativos y los docentes.

En ese sentido, **se requiere de la participación y cooperación** de los Directores de Área, Jefes de Oficina, Líderes de Proceso, Decanos y Coordinadores de Programa, junto con sus equipos de trabajo, **en la Jornada de Sensibilización en Seguridad y Privacidad de la Información**, en la cual se dará a conocer los avances de la implementación del Sistema de Gestión de Seguridad de la Información y la Ley de Protección de Datos Personales.

Para el desarrollo de la jornada, previamente, a cada líder de área se le notificará por medio de correo electrónico la fecha y hora en que será agendado con su equipo. Cualquier inquietud deberá remitirla al Sistema de Gestión de Seguridad de la Información – SGSI, al siguiente correo electrónico: sgsi@ucundinamarca.edu.co

Cordialmente,


ISABEL QUINTERO URIBE
Secretaria General

Proyecto: Sistema de Gestión de Seguridad de la Información - 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

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

ESG-SSI-M004 Manual de Roles y Responsabilidades en Seguridad y Privacidad de la Información

Roles y Responsabilidades



04

Roles y Responsabilidades del Sistema de Gestión de Seguridad de la Información en la Universidad de Cundinamarca

5. ROLES Y RESPONSABILIDADES	10
5.1 RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN	10
5.2 COMITÉ DEL SISTEMA DE ASEGURAMIENTO DE LA CALIDAD – SAC y COMISIÓN DE GESTIÓN	11
5.3 OFICIAL DE TRATAMIENTO DE DATOS PERSONALES	11
5.4 OFICIAL DE SEGURIDAD DE LA INFORMACIÓN (CISO)	12
5.5 ALTA DIRECCIÓN, DIRECTORES Y JEFES DE ÁREA, DECANOS Y DIRECTORES DE PROGRAMA	13
5.6 DIRECCIÓN DE CONTROL INTERNO	14
5.7 EQUIPO TÁCTICO – OPERATIVO DEL SGSI	14
5.8 FUNCIONARIOS ADMINISTRATIVOS Y DOCENTES	15
5.9 FUNCIONARIOS DEL CENTRO ACADÉMICO DEPORTIVO – CAD	16
5.9.1 Responsabilidades con el SGSI del Director	16
5.9.2 Responsabilidades con el SGSI del Personal Administrativo	17
5.9.3 Responsabilidades con el SGSI de los Entrenadores Deportivos	17
5.9.4 Responsabilidades con el SGSI de Contratistas o Proveedores	18
6. RESPONSABILIDADES DE ACUERDO A LOS PERFILES	18
6.1 FUNCIONARIOS CON PERFIL DE USUARIO	18
6.2 FUNCIONARIOS CON ACCESO PRIVILEGIADO	19
6.2.1 Responsabilidades con el SGSI del Administrador de Sistemas de Información y Aplicativos	19
6.2.2 Responsabilidades con el SGSI del Administrador de Servidores	19
6.2.3 Responsabilidades con el SGSI del Administrador de Equipos de	19

Roles y Responsabilidades

Responsable de Seguridad de la Información

Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad.

Gestionar el equipo de proyecto de la entidad, definiendo roles, responsabilidades, entregables y tiempos.

Coordinar las actividades diarias del equipo y proporcionar apoyo administrativo.

Encarrilar el proyecto hacia el cumplimiento de la implementación del Modelo de Seguridad y privacidad de la Información para la entidad.

Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y escalar al Comité de seguridad en caso de ser necesario.

Monitorear el estado del proyecto en términos de calidad de los productos, tiempo y los costos.

Asegurar la calidad de los entregables y del proyecto en su totalidad.

Contribuir al enriquecimiento del esquema de gestión del conocimiento sobre el proyecto en cuanto a la documentación de las lecciones aprendidas.

Roles y Responsabilidades

Comité del Sistema de Aseguramiento de la Calidad – SAC y Comisión de Gestión
Promover que todos los funcionarios vinculados a la entidad conozcan, entiendan y ejerzan sus responsabilidades frente al cumplimiento del Programa Integral de Gestión de Datos Personales – PIGDP y el Sistema de Gestión de Seguridad de la Información - SGSI.
Apoyar el monitoreo y mejora continua del PIGDP y el SGSI.
Procurar la integración y articulación del SGSI con cada una de las directrices de la entidad.
Resolver de forma conjunta las situaciones puestas a consideración por el Oficial de Tratamiento de Datos Personales de la entidad.
Asegurar los mecanismos idóneos para reportar los incidentes de seguridad y privacidad que se presenten.

Roles y Responsabilidades

Alta Dirección, Directores y Jefes de Área, Decanos y Directores de Programa

Motivar a los funcionarios administrativos, docentes y estudiantes de la sede, seccionales, extensiones, oficina de Bogotá y Centro Académico Deportivo - CAD, a conocer las diferentes, políticas, procedimientos, manuales, guías e instructivos derivados del Sistema de Gestión de Seguridad de la Información-SGSI.

Incentivar el adecuado uso del Correo Electrónico Institucional para envío y recepción de información entre funcionarios administrativos y docentes, así como para el contacto con entidades externas a nombre de la Universidad, siguiendo lo establecido en ASIM005 Manual de Políticas de Uso Adecuado Del Correo Institucional.

Gestionar la adopción y cumplimiento del presente Manual de Roles y Responsabilidades entre los funcionarios administrativos de la Institución, en todas las modalidades de contratación

Gestionar los procesos necesarios para la aprobación, levantamiento, actualización y mantenimiento de los activos de información pertenecientes a la dirección y/o jefatura de la institución.

Apoyar la difusión y sensibilización de la seguridad de la información en la Universidad de Cundinamarca.

Roles y Responsabilidades

Funcionarios Administrativos y Docentes

Apoyar al jefe inmediato en la inscripción de bases datos que contengan datos personales (públicos, semi privados, privados y/o sensibles) según los lineamientos establecidos por el Sistema de Gestión de Seguridad de la Información – SGSI y la Superintendencia de Industria y Comercio - SIC.

Atender lo dispuesto en el documento ESG-SSI-F002 ACUERDO DE CONFIDENCIALIDAD PARA MIEMBROS DEL TALENTO HUMANO, PASANTES Y MONITORES y que es firmado por el funcionario al momento de su contratación.

Custodiar, usar y circular únicamente los Datos Personales de los titulares que hayan sido obtenidos mediante autorización y atendiendo las finalidades expuestas en la guía ESG-SSI-G007 GUIA FINALIDADES PARA EL TRATAMIENTO DE DATOS PERSONALES DE LOS TITULARES DE LA UNIVERSIDAD DE CUNDINAMARCA.

Roles y Responsabilidades

Funcionarios Administrativos y Docentes

Asistir y participar de las Jornadas de sensibilización y entrenamiento organizadas y/o convocadas por el Sistema de Gestión de Seguridad de la Información - SGSI atendiendo lo documentado en la Guía 14 del MinTIC y el Tip 4 de la Superintendencia de Industria y Comercio - SI

Cumplir con las políticas, lineamientos, directrices y normatividad como se define en el Manual ESG-SSI-M001 MANUAL DE POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN y cualquier documento que las desarrolle o complementa.

Reportar por los diferentes medios institucionales (sgsi@ucundinamarca.edu.co, pdpsgsi@ucundinamarca.edu.co, 8281483 Ext. 265) al Equipo Táctico Operativo del Sistema de Gestión de Seguridad de la Información - SGSI, ante cualquier irregularidad que se considere un evento y/o incidente de seguridad y privacidad de la información.

Marco Legal Externo para la Seguridad y Privacidad de la Información

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.” (Artículo 13, 14).

Decreto 1078 de 2015

“Por medio del cual se expide el Decreto único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones” (Título 9 “Políticas y lineamientos de tecnologías de la información”

Norma Técnica NTC – ISO/IEC 27001:2013

En transición a la NTC – ISO/IEC 27001:2022

Resolución 500 de 2021

“Por la cual se establecen los lineamientos y estándares para la estrategias de seguridad digital y se adopta el Modelo de Seguridad y Privacidad como habilitador de la Política de Gobierno Digital”

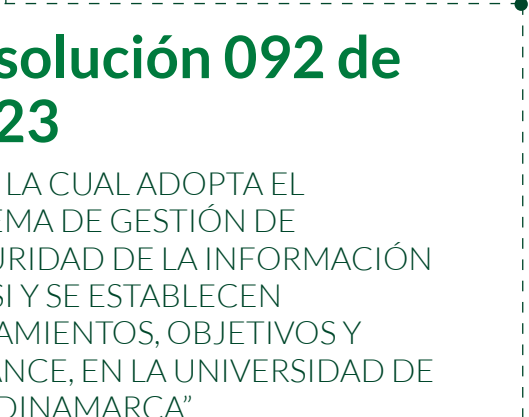
05

Etapas del Modelo de Gestión Integral de Seguridad de la Información



Resolución 091 de 2023

“POR LA CUAL SE ESTABLECEN LOS LINEAMIENTOS DE PROTECCIÓN DE DATOS PERSONALES DE LOS TITULARES DE LA UNIVERSIDAD DECUNDINAMARCA”



Resolución 092 de 2023

“POR LA CUAL ADOPTA EL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI Y SE ESTABLECEN LINEAMIENTOS, OBJETIVOS Y ALCANCE, EN LA UNIVERSIDAD DE CUNDINAMARCA”

Resolución 027 de 2020

“POR LA CUAL SE ESTABLECEN LOS ROLES Y RESPONSABILIDADES DE LOS SISTEMAS DE GESTIÓN DE LA UNIVERSIDAD DE CUNDINAMARCA”

Resolución 088 de 2023

“Por la cual se establece el Sistema de Aseguramiento de la Calidad de la Universidad de Cundinamarca”
Artículo cuadragésimo séptimo- La presente Resolución rige a partir de la fecha de su expedición y deroga en su totalidad la Resolución No. 026 del 10 de marzo de 2020, la Resolución 156 de 2017 y las disposiciones que le sean contrarias.



– (FUSAGASUGA) –

Página 1 de 29

10

RESOLUCIÓN No.088 DEL 2023-08-01

“POR LA CUAL SE ESTABLECE EL SISTEMA DE ASEGURAMIENTO DE LA CALIDAD DE LA UNIVERSIDAD DE CUNDINAMARCA”.

EL RECTOR DE LA UNIVERSIDAD DE CUNDINAMARCA, en uso de sus facultades legales, estatutarias y, en especial las conferidas por el literal (c) artículo 22 del Acuerdo 007 de 2015 del Consejo Superior **“POR EL CUAL SE EXPIDE EL ESTATUTO GENERAL DE LA UNIVERSIDAD”**

ARTÍCULO TRIGÉSIMO SEXTO. – COMISIÓN DE GESTIÓN Conformado por ocho (8) miembros con voz y voto:

1. El Vicerrector(a) Administrativo y Financiero, quien lo presidirá
2. Director de Planeación Institucional (En representación del Sistema de Gestión de la calidad, del Sistema de Gestión Ambiental y del Sistema de Gestión Antisoborno)
3. Director (a) financiero.
4. Directora de Talento Humano (En representación del Sistema de Gestión de Seguridad y Salud en el Trabajo)
5. Coordinador(a) del Sistema de Gestión de Seguridad de la Información.
6. Jefe de Recursos Físicos (En representación del Plan Estratégico de Seguridad Vial)
7. Dos (2) representantes de seccionales y extensiones, elegidos por esta comisión, a través del sistema de postulación ante la Secretaría General quien remitirá los candidatos.

ARTÍCULO CUADRAGÉSIMO. – COMISIÓN DE CONTROL INTERNO. Conformado por siete (7) miembros con voz y voto:

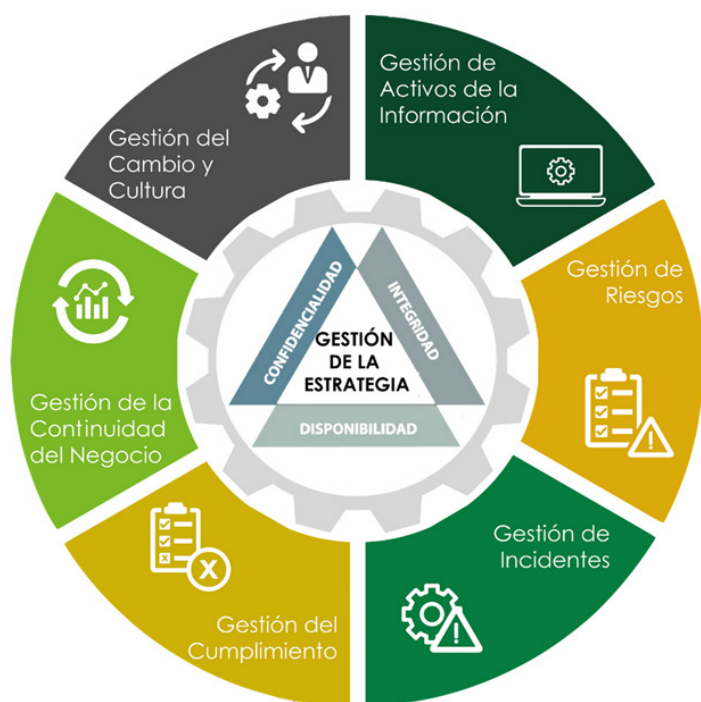
1. El Rector, quien lo presidirá y en su ausencia la Secretaría General
2. Secretaría General
3. Director(a) de Planeación Institucional.
4. Director(a) Jurídico
5. Representante de las Seccionales y Extensiones
6. Director de Control Disciplinario
7. Director Financiero.

El Director(a) de Control Interno, actuará como Secretario Técnico de la Comisión, con voz, pero sin voto.

El Coordinador(a) del Sistema de Gestión de Seguridad de la Información será invitado permanente con voz, pero sin voto.

Etapa 1: Gestión de Activos de la Información

La Universidad de Cundinamarca posee activos (Hardware, Software, Instalaciones, entre otros.) que almacenan, procesan y administran información de importancia para la institución, a los cuales se les denomina “Activos de la Información”.



ESG-SSI-P01 Gestión de Activos de la Información

¿Qué es un Activo de la Información??

Un activo de información en el contexto de un Sistema de Gestión de Seguridad de la Información y con base en la norma ISO/IEC 27001 se define como: “Cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, servicios, edificios, personas...) que tenga valor para la organización.”

Así pues, la Universidad de Cundinamarca continuando con la implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información, estableció el procedimiento ESG-SSI-P01 – Gestión de Activos de la información en el cual se establecen y socializan los lineamientos pertinentes para el cumplimiento de la normatividad legal vigente en el registro de activos de la información por parte de los responsables identificados por la institución, permitiendo la clasificación, valoración y etiquetado de estos activos.

**Inicio de las jornadas de
Entrenamiento para el Registro
de Activos de Información – 5 de
Septiembre de 2023**

Tipos de Activos de Información



IN-INFORMACIÓN

Datos procesados o almacenados física o electrónicamente tales como: Bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.



SE-SERVICIO

Sitio informático o página web para los servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos, Intranet, correo institucional, entre otros.



HW-HARDWARE

Dispositivos electrónicos, equipos de cómputo y de comunicaciones que por su criticidad pueden ser considerados activos de información. Tales como: Servidores, routers, discos duros, portátiles, entre otros.



SW-SOFTWARE

Programa informático para el despliegue de aplicaciones, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.



TH-TALENTO HUMANO

Personal académico y administrativo que realiza funciones en la Universidad de Cundinamarca, que de acuerdo a su conocimiento, experiencia y criticidad pueden ser considerados activos de información.

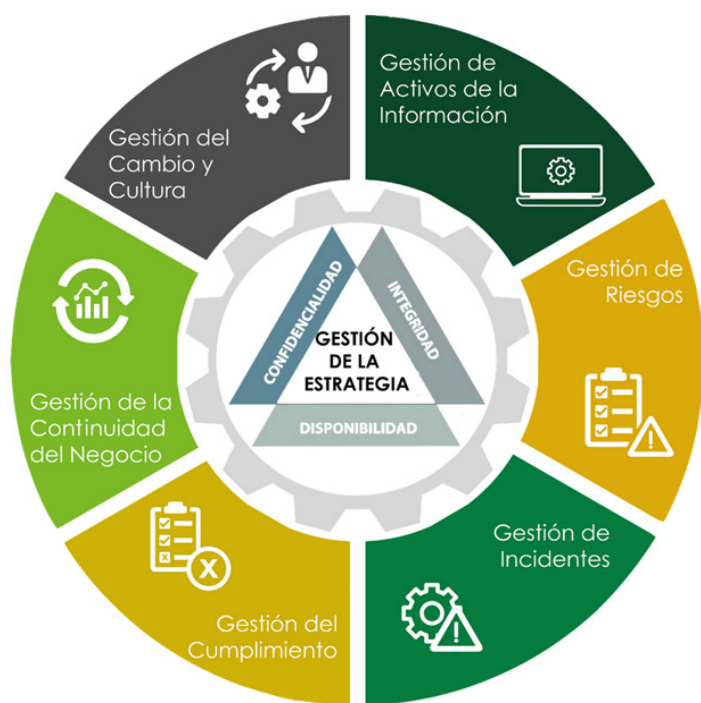


IL-INSTALACIONES

Recurso o espacio físico donde se dispone de información para su almacenamiento, procesamiento y comunicación, que debe contar con las condiciones óptimas de seguridad. (Oficinas, cuartos de suministro eléctrico, centro de datos, entre otros)

Etapa 2: Gestión de Riesgos

Mediante los Activos de la Información, se establecen los riesgos que puedan generar la posible pérdida de la Confidencialidad, la Integridad y/o Disponibilidad de la información de la institución.



Gestión de riesgos de seguridad y privacidad de la información

¿Qué es un riesgo en seguridad de la información?

Es la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias según la Norma ISO/IEC 27000.

Documentos de Referencia:

Guía No.7 MinTIC - Gestión de Riesgos y el Documento - Guía para la Administración del Riesgo y el diseño de controles en entidades públicas del DAFP

ESG-SSI-P12 - Gestión de riesgos de seguridad y privacidad de la información

El Sistema de Gestión de Seguridad de la Información - SGSI actualmente cuenta con el procedimiento ESG-SSI-P12 - GESTIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, en el que se determinan los lineamientos institucionales para la gestión de riesgos asociados que comprometen la confidencialidad, integridad y disponibilidad tanto de los activos de información como de los datos personales de Titulares de la Institución.

MANUAL DE ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - ESG-SSI-M009

Jornadas de Entrenamiento de las Matrices de Riesgos de Seguridad de la Información Vigencia 2023

Durante el primer periodo de la vigencia 2023, el Sistema de Gestión de Seguridad de la información – SGSI, construyó y socializó las matrices de riesgo a los procesos y/o áreas, a partir del reporte y consolidado del inventario de los activos de la información de la vigencia 2022.

Con este ejercicio se subsana el hallazgo Plan de Mejoramiento No. 763, hallazgo No.4:

LA GESTION DEL RIESGO PARA EL SGSI SE TIENE IDENTIFICADO LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION A NIVEL GENERAL, POR TIPO DE ACTIVO HARDWARE, SOFTWARE, INFORMACION, SERVICIOS Y TALENTO HUMANO, PERO NO SE TIENEN DEFINIDOS LOS CRITERIOS DE ACEPTACION, LOS PROPIETARIOS DE LOS RIESGOS Y EL TRATAMIENTO DEL RIESGO RESIDUAL. ASI MISMO AL VERIFICAR LA GESTION DEL RIESGO EN LOS DEMAS PROCESOS AUDITADOS NO SE EVIDENCIA LA IDENTIFICACION Y TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACION, LO CUAL NO PERMITE REALIZAR UN TRATAMIENTO ADECUADO, COMO TAMPOCO LA IDENTIFICACION DEL RIESGO RESIDUAL, POR ENDE, CADA PROCESO EN SU GESTION/ MATRIZ DE RIESGO DEBERA INCLUIR LOS RIESGOS DE SEGURIDAD Y PRIVACIDAD SEGUN CORRESPONDA, EN ARTICULACION CON EL SGSI.

Punto a tratar en la Comisión de Desempeño como un punto actividad pendiente de cumplir.

Jornadas de Socialización de las Matrices de Riesgos de Seguridad de la Información Vigencia 2023

El SGSI construyó 22 matrices de Riesgos las cuales se socializaron por procesos entre el 2 y el 27 de junio del 2023, como se evidencia a continuación:

CONSOLIDADO DE LAS JORNADAS DE SOCIALIZACION DE MATRICES DE RIESGOS ASOCIADOS A LOS ACTIVOS DE INFORMACION			
PROCESO	FECHA PROGRAMADA	OBSERVACIONES	MATRIZ DE RIESGOS FORMALIZADA
Dirección de Autoevaluación y Acreditación	Jueves 15 de junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Dirección de Proyectos Especiales y Relaciones Interinstitucionales	Miércoles 7 de junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Dirección de Planeación Institucional	Viernes 2 de junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Oficina Asesora de Comunicaciones	Jueves 22 de junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Sistema de Gestión - SST	Viernes 11 de agosto	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Sistema de Gestión - SGA	Jueves 22 de junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Sistema de Gestión - SSI	Lunes 5 de junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Sistemas Gestión - Calidad	Martes 6 de junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Oficina de Admisiones y Registro	Martes 6 de junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Dirección de Bienestar Universitario	Miércoles 7 junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Dirección de Investigación Universitaria	Miércoles 7 junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Oficina de Graduados	Martes 13 de junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Dirección de Interacción Universitaria	Miércoles 28 junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Unidad de Apoyo Académico	Jueves 8 junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI

Unidad de Apoyo Académico	Jueves 8 junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Dirección de Talento Humano	Viernes 9 junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Dirección de Bienes y Servicios	Martes 27 junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Dirección Financiera	Viernes 9 junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Dirección de Sistemas y Tecnología	Miércoles 14 de junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Oficina de Archivo y Correspondencia	Martes 13 de junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Dirección Jurídica	Miércoles 21 de junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Dirección de Control Interno	Viernes 16 de junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Dirección de Control Disciplinario	Lunes 5 de junio	Se realizo la socialización, se envio matriz con correcciones y/o comentarios mencionados. (Se encuentra a la espera de respuesta para formalizacion)	SI
Oficina de Peticiones, Quejas y Reclamos	Viernes 16 de junio	Se realizo la socialización y se formalizo la matriz de riesgos	SI

Jornadas de Socialización de las Matrices de Riesgos de Seguridad de la Información

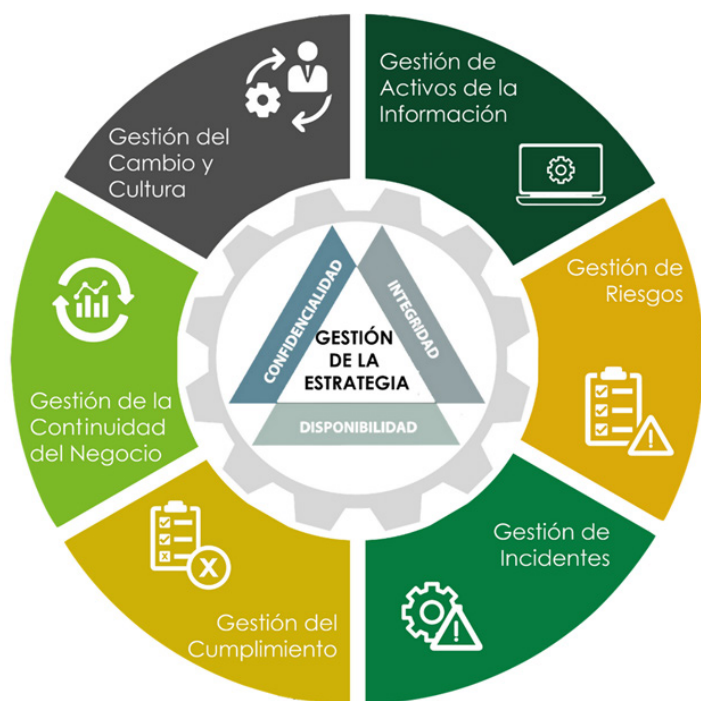
De igual forma, se realizó la socialización de las Matrices de Riesgo para el proceso de Formación y Aprendizaje por Facultades, entre los días 24 al 8 de agosto del presente año, como se evidencia en la siguiente tabla:

PROCESO FORMACION Y APRENDIZAJE	FECHA PROGRAMADA	OBSERVACIONES	MATRIZ DE RIESGOS FORMALIZADA
Faculta de Ingeniería	27 de Julio de 2023	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Faculta de Ciencias del Deporte y la Educación Física	04 de Agosto de 2023	Se remito correo electronico para concertar la fecha y hora para llevar a cabo la socializacion	Si
Faculta de Ciencias Administrativas, Económicas y Contables	25 de Julio de 2023	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Faculta de Educación	27 de Julio de 2023	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Faculta de Ciencias de la Salud	26 de Julio de 2023	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Facultad de Ciencias Sociales, Humanidades y Ciencias Políticas	26 de Julio de 2023	Se realizo la socialización y se formalizo la matriz de riesgos	SI
Facultad de Ciencias Agropecuaria	08 de Agosto de 2023	Se remito correo electronico para concertar la fecha y hora para llevar a cabo la socializacion	Si
Centro Académico Deportivo - CAD	27 de Julio de 2023	Se realizo la socialización y se formalizo la matriz de riesgos	SI

Con este ejercicio se subsana el hallazgo #4 del Plan del Mejoramiento #763 asignado al SGSI, producto de la Auditoría Interna I del SGSI y se entregará informe en la próxima Sesión Ordinaria de la Comisión de Desempeño.

Etapa 3: Gestión de Incidentes

El “Equipo de Respuesta Inmediata a Incidentes de Seguridad de la Información” son los encargados de realizar la gestión de incidentes institucional, cuyas etapas son: Detectar, Analizar, Contener, Erradicar y Recuperar, cualquier evento y/o incidente que atente o pretenda atentar contra la seguridad y privacidad de la información.



¿Qué es un Incidente de Seguridad de la Información?

Un incidente de seguridad de la información se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una política de seguridad de la información.

Guía No.21 para la Gestión y Clasificación de incidentes de Seguridad de la Información. MinTic

ESG-SSI-P09 Gestión de Incidentes de Seguridad de la Información

La Universidad de Cundinamarca mediante el documento ESG-SSI-P09 “Procedimiento de Gestión de Incidentes de Seguridad de la Información” adopta el modelo de gestión y tratamiento de incidentes de seguridad de la información emitido por el Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC) en su guía No.21 y gestiona los casos de reportes de eventos y/o incidentes de seguridad de la información mediante el ciclo de vida de gestión de incidentes expuesto a continuación:



Preparación



Detección de Análisis



Contención,
Erradicación y
Recuperación



Actividades Post-
Incidente

Etapas de la Gestión de Incidentes

Me dirijo a usted, con el fin de dar claridad sobre los pasos a seguir en cuanto a la recepción de quejas y el procedimiento a seguir establecido en el Acuerdo 003 de 2020 "POR EL CUAL SE ADOPTA EL ESTATUTO DISCIPLINARIO DEL PERSONAL ACADEMICO Y ADMINISTRATIVO DE LA UNIVERSIDAD DE CUNDINAMARCA, así:

"ARTÍCULO 50. Oficiosidad: La acción disciplinaria se iniciará y adelantará de oficio, o por información proveniente de servidor público o por otro medio que amerite credibilidad, o por queja formulada por cualquier persona, y no procederá por anónimos, salvo en los eventos en que cumpla con los requisitos mínimos consagrados en el Código Único Disciplinario" (subrayado, negrilla y cursiva fuera de texto)

1. En primer lugar, una vez se tenga conocimiento, de alguna presunta conducta irregular por parte de algún funcionario o estudiante, es un deber, de informar a la Oficina de Control Disciplinario.
2. Una vez recibida la queja o informe, en esta Dirección, evaluará lo correspondiente, es decir si apertura indagación o investigación o decisión inhibitoria¹.
3. Si la decisión es de aperturar indagación o investigación disciplinaria, esta Dirección, adelantará labores investigativas, tendientes a verificar la presunta falta en que se pudo incurrir, para el caso puntual, se tipificará la siguiente falta descrita en el numeral 4 de artículo 10 del citado acuerdo que indica:

"Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos."

4. Dependiendo del material probatorio recaudado, la Dirección evaluará dicho material probatorio y consecuentemente adoptará la decisión de archivo o de formular pliego de cargos², para el caso de funcionarios de la Udec, para los estudiantes elaborará informe de recomendación.

Es necesario indicar que esta Dirección siempre estará a disposición de recibir cualquier información sobre irregularidades al interior de la Institución, no es necesario acudir a cualquier otra dependencia para dar a conocer sobre hechos que atenten contra el buen nombre y buen funcionamiento de la Universidad.

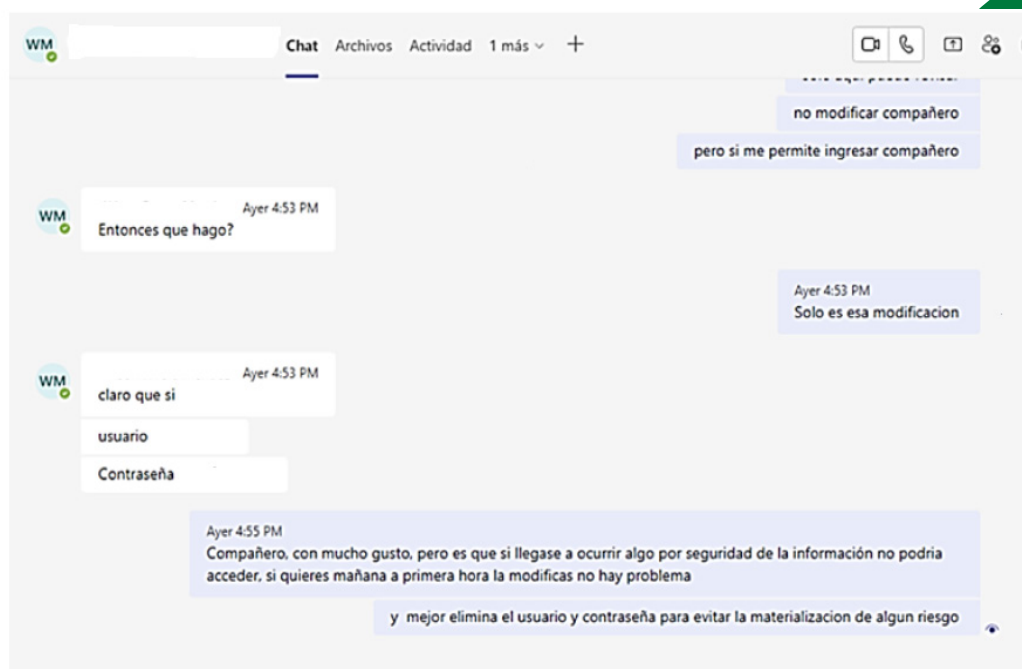
Incidentes Vigencia 2023

Durante la presente vigencia se han reportado en la sede, seccionales y extensiones que conforman la Universidad de Cundinamarca, 28 eventos y/o incidentes de seguridad de la información, que obedecen a distintos escenarios que pueden vulnerar la confidencialidad, integridad y/o disponibilidad de la información como se expone a continuación:

Tipo de evento y/o incidente	
Intentos de phishing o ingeniería social por medio de correos electrónicos identificados como sospechosos y cuyo contenido representa alto riesgo de vulneración de la seguridad y privacidad de la información.	19
Abuso y/o uso inadecuado de los servicios de información institucionales, por medio de la exposición de credenciales de acceso a plataformas virtuales u otros escenarios.	4
“Otros” tipos de incidente (generalmente casos muy específicos o de gravedad considerablemente alta para los titulares o la institución).	6
Comportamiento irregular identificado en el correo electrónico institucional de dos direcciones, donde se intentaron eliminar masivamente los correos electrónicos desde una IP perteneciente al segmento de red contratado por la universidad, descartando posibles accesos fraudulentos a la información.	2
TOTAL	31

Informe con corte a 15 de Agosto de 2023

Incidentes Llevados a la Dirección de Control Disciplinario



Viernes 21 de abril de 2023

Un funcionario reporta al Sistema de Gestión de Seguridad de la Información – SGSI un incidente de Seguridad de la Información, por compartir credenciales de acceso a la plataforma institucional.

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-F002
	PROCESO GESTIÓN SISTEMAS INTEGRADOS	VERSIÓN: 3
	ACUERDO DE CONFIDENCIALIDAD PARA MIEMBROS DEL TALENTO HUMANO, PASANTES Y MONITORES	VIGENCIA: 2021-12-06
		PAGINA: 6 de 8

DECIMA QUINTA. CONFIDENCIALIDAD DE INFORMACIÓN DE AUTENTICACIÓN: La UNIVERSIDAD DE CUNDINAMARCA entregará la PARTE RECEPTORA, credenciales de acceso a servicios, sistemas de información y bases de datos para uso exclusivo de acuerdo con las funciones descritas en el contrato (laboral o de prestación de servicios según sea el caso). Por tanto, la PARTE RECEPTORA se obliga a conservar en total reserva y confidencialidad estas credenciales, así como toda la información que llegare a conocer a través de los accesos que le sean habilitados. Así mismo, se obliga a reportar al Oficial de Seguridad de la Información, cuando tenga conocimiento de la ocurrencia de cualquier incidente con sus credenciales de acceso, que puedan poner en riesgo la disponibilidad, integridad y/o confidencialidad de la información a la que accede.

Casos de phishing o ingeniería social presentados en la universidad de cundinamarca

De: FELIPE MIRANDA ABOGADO <facturacion@cpsabogados.com>
Enviado: martes, 7 de marzo de 2023 7:29 a. m.
Para: TESORERIA <tesoreria@ucundinamarca.edu.co>
Asunto: DERECHO DE PETICION

Bogotá D. C., 7 de Marzo de 2023

Asunto: Derecho de petición

Yo, **JESUS DAVID GUERRERO CÓRDOBA**, identificado con cedula de ciudadanía, **1.063.082.291**, de Bogotá - Cundinamarca, de conformidad con lo establecido en el artículo 23 de la Constitución Política, en concordancia con la Ley 1755 de 2015, comedidamente me permito presentar el siguiente Derecho de Petición el cual contiene toda la información pertinente.

IMPORTANTE.

Use como código de autenticidad **2073**, para descargar el Derecho de Petición sin problemas.

[Descargar - Derecho de Petición.](#)

Recuerde:

Cuando no se dé respuesta al/la peticionario/a dentro de dicho término, se entenderá para todos los efectos legales que la solicitud ha sido aceptada, y se entenderá, que la respectiva solicitud ha sido aceptada. Muchas gracias por la atención prestada.

7 marzo de 2023 Oficina Tesorería

De: Jimi Alexis Latorre Salcedo <alexisalcaldia2015@gmail.com>
Enviado: jueves, 18 de mayo de 2023 2:27 p. m.
Asunto: NOTIFICACION SENTENCIA AT 2021-00184-01 RAD INT 2021-00171-01 ACCIONANTE, EMSSANAR Y OTROS



Rama Judicial
Consejo Superior de la Judicatura
República de Colombia

CLAVE DE ACCESO: 5555

AVISO DE CONFIDENCIALIDAD: Este correo electrónico contiene información de la Rama Judicial de Colombia. Si no es el destinatario de este correo y lo recibió por error comuníquelo de inmediato, respondiendo al remitente y eliminando cualquier copia que pueda tener del mismo. Si no es el destinatario, no podrá usar su contenido, de hacerlo podría tener consecuencias legales como las contenidas en la Ley 1273 del 5 de enero de 2009 y todas las que le apliquen. Si es el destinatario, le corresponde mantener reserva en general sobre la información de este mensaje, sus documentos y/o archivos adjuntos, a no ser que exista una autorización explícita. Antes de imprimir este correo, considere si es realmente necesario hacerlo, recuerde que puede guardarlo como un archivo digital.

18 mayo de 2023 Oficina Tesorería

De: Conrado Giraldo <cgiraldo@contraloriadecundinamarca.gov.co>
Enviado: miércoles, 12 de abril de 2023 7:50 a. m.
Asunto: ESTADO DE CONSIGNACIÓN



CONSIGNACIÓN

Cordial Saludo

Transferencia realizada desde nuestra entidad bancaria para la aprobación de la transferencia revise su estado de cuenta para mayor seguridad dejamos

[VER AQUÍ ESTADO DE TRANSFERENCIA](#)
CÓDIGO DE INGRESO: 6565

12 de abril de 2023 Dirección de Control Interno

De: MINISTERIO DE TRANSPORTE <support@3c-contactcenter.com>
Enviado: martes, 18 de julio de 2023 1:21 a. m.
Para: CONTROL INTERNO UDEC <controlinterno@ucundinamarca.edu.co>
Asunto: MINTRANSPORTE FOTOMULTA N° 2022-SD74-1147



BOGOTÁ D.C 17 DE JULIO DEL 2023
NOTIFICACION: RADICACION DE COMPARENDO N.º 2022-SD74-1147

SEÑOR
INFRACADOR.

Respetuoso Saludo.

La SECRETARIA DISTRITAL DE MOVILIDAD por medio del presente comunicado le notifica que en la actualidad usted presenta en nuestra base de datos un COMPARENDO POR FOTO MULTA por un valor de **Novecientos ochenta y nueve mil quinientos veinte pesos 989,520 M/C**; según lo establecido en la ley 1843 de 2017.

Infracción:

Regulado por la **ley 2351 del 16 de abril del año 2005**.

- Invadir carril contrario y Transitar en contra vía por área no permitida.
- Por lo anterior en el siguiente enlace encontrará FOTOS/HORA y LUGAR donde se originó su comparendo: <https://www.runt.com.co/consultas-infracciones.transitoymultas.gov>
- Para visualizar el documento digitar la contraseña: **0020**

Cordialmente.

Berta Manjarrés Palomino
Secretaria Distrital De Movilidad

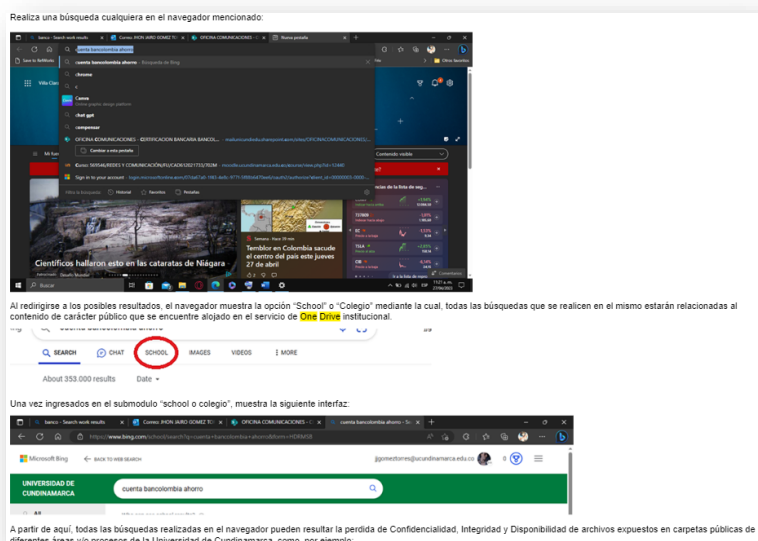
18 de julio de 2023 Dirección de Control Interno

Caso fortuito

	El lun, 31 jul 2023 a la(s) 11:37, Alfonso Aguirre Arias (alfonsoarias572@gmail.com) escribió: pero amor tu me prometiste que en cuanto llegaras a ese sitio me ibas hacer contrarar, si vez que tu solo prometes y prometes, cumples. por eso sigo enojado
	El lun, 31 jul 2023 a la(s) 11:40, Mauricio O'Byrne Ramirez (emedicaliderhus.org.co@gmail.com) escribió: mi amorcito lindo a este lugar estoy llegando apenas, debes darme mas tiempo estoy tratando de mover algunas fichas por aca con mi amiga Martha y Luz Dary ellas son las del poder en th de este hueco, me estan ayudando despues nos tocara darles una tajada de lo que hagamos. Les hablare de ti bebe en estos dias para poderle traer amor ami lado. pero ya sabes tu y yo aca no tenemos nada, por ahora estoy super estresado con estos putos comites con esas universidades si vieras es un chicharron peludo, estoy mamado de esas vainas
	El lun, 31 jul 2023 a la(s) 11:43, Alfonso Aguirre Arias (alfonsoarias572@gmail.com) escribió: vale, ¿ mi vida cuando nos vemos?
	El lun, 31 jul 2023 a la(s) 11:44, Mauricio O'Byrne Ramirez (emedicaliderhus.org.co@gmail.com) escribió: te dije que por ahora estoy muy ocupado en estos hp. comites con esas de universidades con todos esos y que doctores y viejas prepotentes que es como si le dieran ordenes a uno, si vieras que estres bebe
	El lun, 31 jul 2023 a la(s) 11:45, Alfonso Aguirre Arias (alfonsoarias572@gmail.com) escribió: quienes? cuales viejas?
	El lun, 31 jul 2023 a la(s) 11:47, Mauricio O'Byrne Ramirez (emedicaliderhus.org.co@gmail.com) escribió: Todas esas de las universidades, sabes que no soporto las viejas, me parecen un fastidio sabes amor? vivo con mucho estres como te decia necesito desestresarme, tu sabes lo que me gusta, ahi te envio esas cositas ricas que me encantan y bien grandes
	El lun, 31 jul 2023 a la(s) 11:48, Alfonso Aguirre Arias (alfonsoarias572@gmail.com) escribió: siiiiiiiii ya queria que llegaras ahi mmm me encantas seas caliente. recuerdas que te habia dicho del viaje a italia?
	

Chats divulgados en listas de distribución masivas

Otros tipos de Incidentes de Seguridad Reportados en la Institución



Viernes 27 de Abril de 2023

Un estudiante perteneciente al programa de Ingeniería de Sistemas y Computación de la Sede Fusagasugá reporta un incidente de seguridad y privacidad de la información, relacionado a la configuración de acceso público con el que cuentan algunas carpetas de archivos de diversos procesos y/o áreas de la Universidad de Cundinamarca alojadas en el servicio de almacenamiento en nube "One Drive" de Microsoft.

Una vez se realizó la validación correspondiente al incidente y se determinó el nivel de gravedad e impacto de la información expuesta de manera pública en los servicios de almacenamiento en la nube, como medida de respuesta y contingencia se estableció lo siguiente:

- Se establecerá un plazo de 3 días hábiles para que los procesos y/o áreas que en cumplimiento y desarrollo de sus actividades requieran tener información almacenada en forma pública, comuniquen al Sistema de Gestión de Seguridad de la Información y/o al Área de Servicios Tecnológicos el motivo por el cual los archivos alojados en la nube deben permanecer públicos.
- Debido a que el incidente reportado vulnera la confidencialidad, integridad y disponibilidad de la información, se modificará masivamente la configuración de todos los equipos de cómputo que se encuentran en estado de acceso público y contienen carpetas de información que se encuentren almacenadas en el servicio de One Drive institucional, estableciendo para los equipos mencionados el estado de acceso privado.
- A partir del día 10 de mayo del año en curso, los procesos y/o áreas que no confirmen la necesidad de mantener sus equipos y archivos en estado de acceso público, pasarán de forma automática a estado de acceso privado.

Funciones de los vigías de seguridad de la información



El o los Vigías de Seguridad de la Información – SGSI, es un rol que tienen los funcionarios del Sistema de Gestión de Seguridad de la Información – SGSI.



La participación activa de los vigías del SGSI es vital para dinamizar y mantener una cultura de apropiación de los conceptos y directrices del SGSI a nivel institucional.



El o los vigías del SGSI, realizan visitas a las diferentes áreas a nivel institucional, donde de manera aleatoria verificaran el cumplimiento de las políticas y directrices documentadas y que deben ser comunicadas a la comunidad universitaria a través de los diferentes mecanismos de socialización



El o los Vigías de Seguridad de la Información – SGSI, reportan los incidentes de seguridad de la información, que evidencien al interior de la institución, al equipo de respuesta inmediata a incidentes de seguridad de la información en las herramientas que se dispongan para tal fin.

Resultados Visitas de Vigía de Seguridad de la Información Vigencia 2023

Proceso	Área / oficina	Fecha de verificación	Fortalezas	Debilidades
Dirección de Investigación Universitaria	Dirección de Investigación	2023-05-25	64,3%	35,7%
Dirección Financiera	Oficina de Apoyo Financiero	2023-05-26	42,8%	57,2%
Dirección de Control Interno	Dirección de Control Interno	2023-05-30	85,7%	14,3%
Unidad de Apoyo Académico	Salas de cómputo Bloque A	2023-06-06	71,4%	28,6%
Dirección de Planeación institucional	Dirección de Planeación Institucional	2023-06-05	89,2%	10,8%
Gestión Sistemas Integrados	Seguridad y Salud en el Trabajo	2023-06-08	85,7 %	14,3%
Dirección de Bienes y Servicios	Recursos Físicos y Servicios Generales	2023-08-14	84,6%	15,4%

Lineamientos Verificados

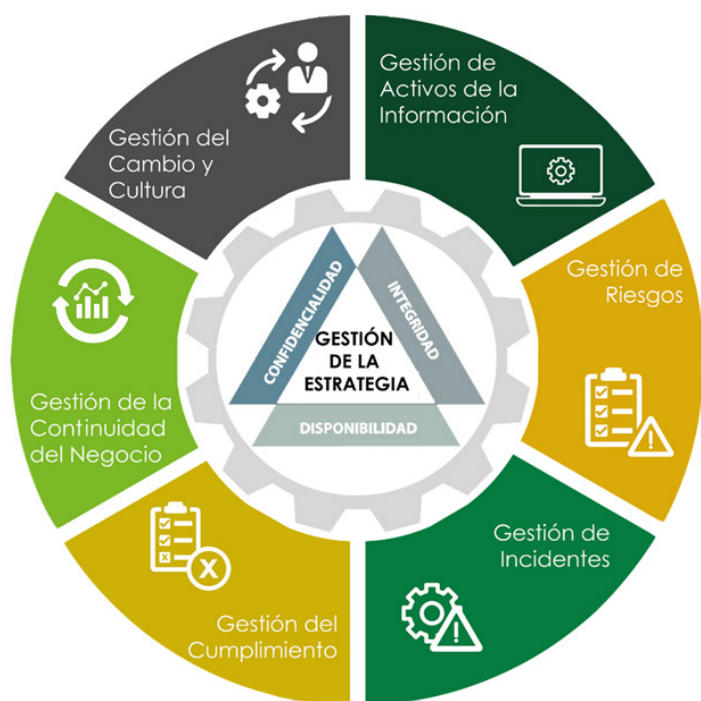
ESG-SSI-F035 Reporte de verificación

- Tratamiento de datos personales
- Tratamiento de datos sensibles
- Uso adecuado de correo institucional
- Manual de roles y responsabilidades
- Manual escritorio limpio y pantallas limpia
- Control de acceso físico a áreas seguras

Visitas del Rol de Vigías de Seguridad de la Información			
Programadas	6	Atendidas	6
Solicitadas	1	Atendidas	1
Total	7	Total	7

Etapa 4: Gestión del Cumplimiento

La Universidad de Cundinamarca como institución pública del estado, debe asegurar el cumplimiento de la normatividad legal vigente, establecida para el tratamiento y protección de datos personales como se indica en la ley 1581 del 2012 y demás decretos reglamentarios.



Marco Legal para la Protección de Datos Personales

Constitución Política

Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.

Artículo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación

Ley 1266 de 2008

“Por la cual se dictan las disposiciones generales del hábeas 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.”

Ley 1581 de 2012

Artículo 9º. Autorización del Titular.
Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.

Decreto Único 1074 de 2015

Capítulo 25 – REGLAMENTA
PARCIALMENTE LA LEY 1581 DE
2012

SECCIÓN 2 AUTORIZACIÓN

Artículo 2.2.2.25.2.1. Recolección de
los datos personales

Artículo 2.2.2.25.2.2. Autorización

Ley 1918 de 2018

“Por medio de la cual se establece el régimen de inhabilidades a quienes hayan sido condenados por delitos sexuales cometidos contra menores, se crea el registro de inhabilidades y se dictan otras disposiciones”

Datos Personales

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.



Fecha nacimiento



Placa de Vehículo



Fotos y Videos



Nombres y Apellidos



De Salud



Email



Móvil



Móvil



Huella Dactilar

Tipos de datos personales



Datos Públicos

Es el dato que la Ley o la Constitución Política determina como tal, así como todos aquellos que no sean semiprivados o privados.



Datos Semiprivados

Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas



Datos Privados

Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.



Datos Sensibles

Es el dato que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación y los datos de menores de edad (-18)

Ley Estatutaria 1581 de 2012

Artículo 3º. Definiciones. Para los efectos de la presente ley, se entiende por:

- Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales;
- Titular: Persona natural cuyos datos personales sean objeto de Tratamiento;
- Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Artículo 10. Casos en que no es necesaria la autorización. La Autorización del Titular no será necesaria cuando se trate de:

Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;

- Datos de naturaleza pública;
- Casos de urgencia médica o sanitaria;
- Tratamiento de información autorizada por la ley para fines históricos, estadísticos o científicos;
- Datos relacionados con el Registro Civil de las Personas

Quien acceda a los datos personales sin que se medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente Ley.

Artículo 23º. Sanciones. La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:

- Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;
- Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;
- Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;
- Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;

Parágrafo. Las sanciones indicadas en el presente artículo sólo aplican para las personas de naturaleza privada. En el evento en el cual la Superintendencia de Industria y Comercio advierta un presunto incumplimiento de una autoridad pública a las disposiciones de la presente ley, remitirá la actuación a la Procuraduría General de la Nación para que adelante la investigación respectiva.

Gestión de Autorizaciones



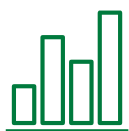
Se hizo el envío de correo electrónico a los estudiantes que no habían gestionado la autorización.



Se estableció la autorización como requisito en la revisión de carpeta de estudiantes próximos a graduarse.



Se contactó a cada uno de los estudiantes en estado “RECHAZADO” vía Teams invitándolos a gestionar la autorización.



Se llevó a cabo junto con la Oficina de Admisiones y Registro, la campaña denominada “**ACTUALIZACIÓN DE DOCUMENTOS DE ESTUDIANTES NUEVOS Y ANTIGUOS**” en Sede, Seccionales y Extensiones de la Universidad de Cundinamarca.

Sanciones a Universidades

UNIVERSIDAD CATÓLICA DE COLOMBIA	28/06/2022	La investigada realizó el envío de un correo electrónico de carácter publicitario a la dirección electrónica institucional del denunciante, el cual es un dato semiprivado, sin contar con su autorización previa, expresa e informada para el tratamiento de sus datos personales; así como tampoco le informó sobre la finalidad de la recolección de sus datos y los derechos que le asisten. Por otra parte, la sociedad, pese a tener implementadas algunas medidas tendientes a proteger el derecho de habeas, estas no fueron suficientes, y las funcionarias que enviaron el correo publicitario al titular no fueron debidamente capacitadas sobre el Régimen de protección de datos personales.	RESOLUCIÓN 40839 de 2022	EN FIRME
----------------------------------	------------	---	--	----------

\$53.205.600

UNIVERSIDAD MANUELA BELTRÁN	20/02/2018	DEBER DE TRAMITAR LAS PETICIONES Y RECLAMOS PRESENTADAS POR LOS TITULARES: SE VIOLA CUANDO NO SE ATIENDE EN DEBIDA FORMA LA SOLICITUD DE ACCESO DE INFORMACIÓN QUE PRESENTA EL TITULAR	RESOLUCIÓN 11396 REPOSICIÓN 30877 de 2018	EN FIRME
-----------------------------	------------	--	--	----------

\$7.812.420

Finalidades para el Tratamiento de Datos

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-G007
	PROCESO GESTIÓN SISTEMAS INTEGRADOS	VERSIÓN: 2
	GUÍA FINALIDADES PARA EL TRATAMIENTO DE DATOS PERSONALES DE LOS TITULARES DE LA UNIVERSIDAD DE CUNDINAMARCA	VIGENCIA: 2023-07-28
		PAGINA: 1 de 9

OBJETIVO:	Definir las finalidades por macroproceso y proceso, por las cuales se recolectan datos de titulares en la Universidad de Cundinamarca, de acuerdo a las actividades académico administrativas que se desarrollan, tanto internas como externas.
ALCANCE:	El presente documento va dirigido a todas las áreas académico administrativas de la Universidad de Cundinamarca

DEFINICIONES

AUTORIZACIÓN: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de Datos Personales.¹

DATO PERSONAL: Cualquier información vinculada o que pueda asociarse a varias personas naturales determinadas o determinables.²

TRATAMIENTO: Cualquier operación o conjunto de operaciones sobre Datos Personales, tales como la recolección, almacenamiento, uso, conservación, uso interno, uso externo, supresión.³

PRINCIPIO FINALIDAD: El Tratamiento debe obedecer a una finalidad específica, de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

DESCRIPCIÓN DE ACTIVIDADES Y/O RECOMENDACIONES

A continuación, se relacionan las finalidades agrupadas por macroproceso y proceso:

PROCESO	FINALIDAD
Comunicaciones	1. Notificación vía mensaje de texto de las campañas publicitarias e información relacionada con la actividad académica de los estudiantes tales como generación del recibo de pago, plazos de matrícula, eventos y actividades institucionales, entre otros.
	2. Diseñar, planear e implementar diferentes estrategias de mercadeo y promoción eficaz y eficiente para la oferta educativa de la Universidad de Cundinamarca en sus diferentes modalidades.
Planeación Institucional	3. Almacenar y administrar la información recopilada de los administrativos, docentes y comunidad en general, con el fin de llevar a cabo los diferentes eventos estratégicos coordinados por la Dirección de Planeación Institucional.
Sistemas Integrados	4. Registrar información para la medición de clima y cultura organizacional con el fin de definir, ejecutar y evaluar estrategias para su intervención.
	5. Recolectar y consolidar la información asociada a los datos personales de los titulares de la Universidad De Cundinamarca, con el fin de definir, ejecutar y evaluar las actividades pertinentes del Sistema de Gestión de Seguridad y Salud en el trabajo, dando cumplimiento a las normas aplicables legales vigentes y el Decreto 1072 de 2015, el cual tiene como objetivo ARTÍCULO 2.2.4.6.1. Objeto y campo de aplicación. El presente capítulo tiene por objeto definir las directrices de obligatorio cumplimiento para implementar el Sistema de Gestión de la Seguridad y Salud en el Trabajo (SG-SST), que deben ser aplicadas por todos los empleadores públicos y privados, los contratantes de personal

ESG-SSI-G007 Guía Finalidades para el Tratamiento de Datos Personales de los Titulares de la Universidad de Cundinamarca

Transversales	6. Establecer comunicación y contacto por los medios autorizados previamente con el fin de enviar información a los diferentes titulares interesados en algún programa académico o servicios de pregrado, posgrado y educación continuada.
	7. Tomar registro fotográfico y de video de los diferentes eventos en los cuales participen diferentes titulares de la institución, con el fin de realizar publicidad de los eventos organizados.

B. MACROPROCESO MISIONAL

PROCESO	FINALIDAD
Admisiones y Registro	8. Almacenar y administrar la información de los estudiantes con el fin de llevar a cabo la prestación del servicio académico ofertado por la institución en las diferentes modalidades de pregrado, posgrado y educación continuada.
	9. Generar facturación relacionada con el proceso de admisiones de la universidad.
	10. Llevar el registro, control y conservación conforme a los parámetros legales de las actas y títulos de

Documental	26. Recolectar y almacenar en el software documental SAIA las firmas de los directivos, jefes, decanos y coordinadores, funcionarios competentes y autorizados según el Manual de Gestión Documental, con el fin de gestionar las comunicaciones oficiales, la cual será administrada por la oficina de Archivo y Correspondencia y almacenada por el proveedor contratado para tal fin. Una vez se desvincule, retire o finalice el contrato del funcionario y/o contratista de la institución, será suprimida la firma de la base de datos y del software, lo cual será documentado mediante acta.
Financiera	27. Gestionar de manera adecuada las solicitudes para realizar el pago de cada uno de los componentes que integran las prestaciones sociales de los funcionarios administrativos y docentes en cualquier modalidad de contratación de la institución.
Sistemas y Tecnología	28. Crear bases de datos de acuerdo a las características y perfiles de los titulares de los Datos Personales, todo de acuerdo con lo dispuesto en la ley.
	29. Gestionar los servicios de verificación y autenticidad de la firma digital para los directivos, jefes y decanos de la Universidad de Cundinamarca, mediante las herramientas tecnológicas establecidas para su trámite.
Talento Humano	30. Mantener el registro de cada uno de los funcionarios administrativos y docentes en

ESG-SSI-F002 Acuerdo de Confidencialidad para Miembros del Talento Humano, Pasantes y Monitores

DECIMA QUINTA. CONFIDENCIALIDAD DE INFORMACIÓN DE AUTENTICACIÓN: La UNIVERSIDAD DE CUNDINAMARCA entregará la PARTE RECEPTORA, credenciales de acceso a servicios, sistemas de información y bases de datos para uso exclusivo de acuerdo con las funciones descritas en el contrato (laboral o de prestación de servicios según sea el caso). Por tanto, la PARTE RECEPTORA se obliga a conservar en total reserva y confidencialidad estas credenciales, así como toda la información que llegare a conocer a través de los accesos que le sean habilitados. Así mismo, se obliga a reportar al Oficial de Seguridad de la Información, cuando tenga conocimiento de la ocurrencia de cualquier incidente con sus credenciales de acceso, que puedan poner en riesgo la disponibilidad, integridad y/o confidencialidad de la información a la que accede.

Señores

PROTECCIÓN DE DATOS SGI
Universidad de Cundinamarca.

Cordial saludo,

De manera atenta y en atención al correo que antecede, solicito de su amable colaboración respecto a la siguiente inquietud:

La persona que está realizando la solicitud es un estudiante que pertenece al semillero de investigación, cuya información contiene números de identificación de las personas inscritas en esa época, la consulta es, esa información la puede solicitar el estudiante o es necesario que la haga el docente líder del semillero con su respectiva justificación.

Gracias, quedamos atentos a comentarios.

Buenas tardes un cordial saludo, realizo una solicitud de las siguientes actas de dirección de investigación:

Acta N° [redacted]; radicado n° [redacted] del semillero de investigación [redacted] Solicitud de [redacted] de ese entonces.

y del acta N° [redacted] radicado n° [redacted] sección A del semillero [redacted] Solicitud de [redacted] de ese entonces.

Muchas gracias y espero pronta su respuesta.

Asunto: Respuesta "Solicitud de actas de [redacted]"

Respetada funcionaria [redacted]

En atención al correo que antecede, me permito informar que atendiendo la normatividad de la Ley de Protección de Datos Personales, que se viene implementando en la Universidad de Cundinamarca y como reposa en la Resolución No. 000050 de 2018 "POR LA CUAL SE ESTABLECE LA POLÍTICA DE TRATAMIENTO DE DATOS DE LOS TITULARES DE LA UNIVERSIDAD DE CUNDINAMARCA", ARTÍCULO 10° - DEBERES DE LA UNIVERSIDAD DE CUNDINAMARCA COMO RESPONSABLE Y ENCARGADA DEL TRATAMIENTO DE LOS DATOS PERSONALES, numeral 4. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

De igual manera, solo podemos asegurar la confidencialidad, integridad y disponibilidad de la Información de la Institución, cuando está a cargo de funcionarios administrativos y docentes, teniendo en cuenta que al momento de su vinculación firman el documento ESG-SSI-F002 - Acuerdo de Confidencialidad para miembros del Talento Humano, Pasantes Y MONITORES, donde en su cláusula DECIMA QUINTA. Reposa lo siguiente:

***CONFIDENCIALIDAD DE INFORMACIÓN DE AUTENTICACIÓN:** La UNIVERSIDAD DE CUNDINAMARCA entregará la PARTE RECEPTORA, credenciales de acceso a servicios, sistemas de información y bases de datos para uso exclusivo de acuerdo con las funciones descritas en el contrato (laboral o de prestación de servicios según sea el caso). Por tanto, la PARTE RECEPTORA se obliga a conservar en total reserva y confidencialidad estas credenciales, así como toda la información que llegare a conocer a través de los accesos que le sean habilitados. Así mismo, se obliga a reportar al Oficial de Seguridad de la Información, cuando tenga conocimiento de la ocurrencia de cualquier incidente con sus credenciales de acceso, que puedan poner en riesgo la disponibilidad, integridad y/o confidencialidad de la información a la que accede.

Por lo expuesto anteriormente, no se puede suministrar información de titulares a ninguna persona, que no haya firmado el documento ESG-SSI-F002, en este contexto los estudiantes no firman este documento, excepto los que están en modalidad de pasantía o monitoría.

Por último, es importante recomendar que se acerca la época electoral y la universidad en pasadas elecciones, se ha visto afectada porque utilizan las bases de datos para hacer propaganda electoral.

Pendiente de sus comentarios/o sugerencias

Registro Nacional de Bases de Datos - RNBD

Se cumplió al 100% con el cronograma para el Registro Nacional de Bases de Datos – RNBD vigencia 2023, el cual constaba de 16 actividades. Teniendo como resultado lo siguiente:

Base de Datos: Conjunto organizado de datos personales que sea objeto de tratamiento

NO.	NOMBRE DE LA BASE DE DATOS	No. Radicados
1	AFILIACIONES ARL ESTUDIANTES (PRACTICANTES)	21-133124--000002-000
2	INFORMACION PARA EL DESARROLLO DE LAS INVESTIGACIONES ACADEMICAS, LA INNOVACION Y LA TECNOLOGIA	21-133250--000001-000
3	REGISTRO DE PARTICIPACION EN EVENTOS DE CAMPOS CULTURALES	21-133264--000001-000
4	WORKSHOP LATINOAMERICANO "Dialogando en el mundo del software" Ucundinamarca 2021	22-119368--000001-000
5	REGISTRO DE INGRESO A LAS INSTALACIONES DE LA UNIVERSIDAD	21-133263--000001-000

Bases de datos eliminadas

NO.	NOMBRE DE LA BAS DE DATOS	No. Radicados
1	BASE DE DATOS CONTRATACION ORDENES DE PRESTACION DE SERVICIOS	23-128378--000000-000
2	PERSONAL VINCULADO A LA UNIVERSIDAD DE CUNDINAMARCA FÍSICA	23-128431--000000-000

Bases de datos eliminadas

Registro Nacional de Bases de Datos - RNBD

NO.	NOMBRE DE LA BASE DE DATOS	No. Radicados
1	BANCO DE PROVEEDORES	19-10799--000004-000
2	ESCUELAS DE FORMACION Y CLUBES DEPORTIVOS UCUNDINAMARCA	21-133199--000001-000
3	USUARIOS Y PRIVILEGIOS DE PLATAFORMA INSTITUCIONAL	22-119406--000001-000
4	BASE DE DATOS DE GRADUADOS	19-10866--000003-000
5	CUERPOS COLEGIADOS DE LA UNIVERSIDAD DE CUNDINAMARCA	21-133246--000002-000
6	CASSA UDEC	22-119423--000001-000
7	UNIDAD AMIGA DE LOS ADOLESCENTES Y JOVENES	21-133265--000002-000
8	BASE DE DATOS DE QUEJOSOS	21-133190--000002-000
9	BASE DE INTERACCIÓN SOCIAL UNIVERSITARIA	21-133256--000002-000
10	BASE DE DATOS DE ASPIRANTES Y PROCESO DE ADMISION	21-133172--000002-000
11	DESARROLLO DEL CICLO ACADEMICO DE LOS ESTUDIANTES	19-25704--000004-000
12	Caracterización Morfológica y funcional en escolares del occidente de Bogotá.	22-119193--000001-000
13	Estilos de vida en estudiantes ciencias del deporte UdeC.	22-119318--000001-000
14	PERSONAL VINCULADO A LA UNIVERSIDAD DE CUNDINAMARCA	19-10791--000004-000
15	REPORTE CONDICIONES DE SALUD COVID 19	22-188755--000001-000
16	GESTIÓN DE LAS AUTORIZACIONES PARA EL TRATAMIENTO DE DATOS PERSONALES DE ESTUDIANTES	21-133153--000002-000
17	GRADUADOS	19-10866--000003-000

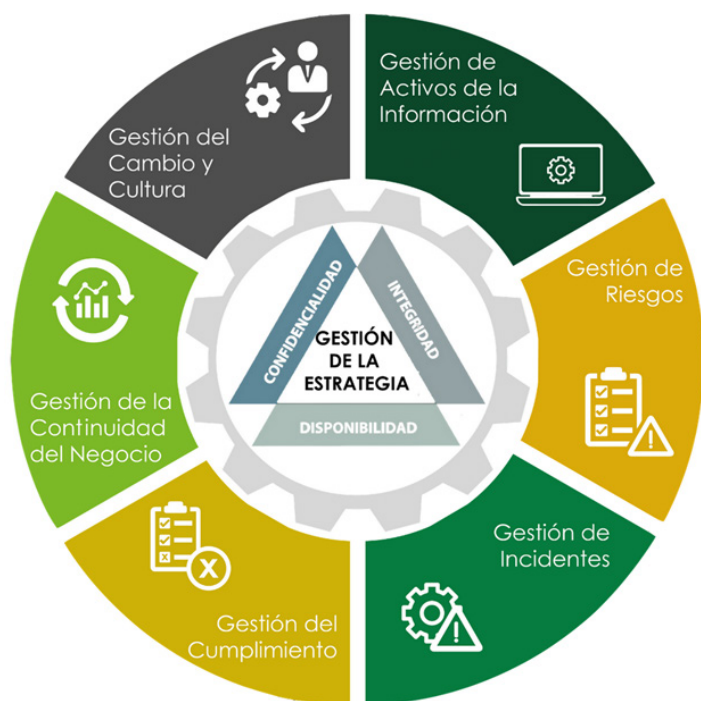
Etapa 5: Gestión de la Continuidad del Negocio

El Sistema de Gestión de Seguridad de la Información, establece los lineamientos de “Backup” o respaldo de información, de todos y cada uno de los procesos gestionados por el SGSI, con el fin resguardar la confidencialidad, integridad y disponibilidad de la información de la institución.



Etapa 6: Gestión del Cambio y Cultura

Se establecen los lineamientos fundamentales para difundir la estrategia de seguridad de la información a los diferentes niveles de la organización, para generar un cambio positivo.



Encuesta sobre temas a incluir en las Jornadas de Sensibilización de Seguridad y Privacidad de la Información vigencia 2023

Asunto: Encuesta sobre temas a incluir en las Jornadas de Sensibilización de Seguridad y Privacidad de la Información vigencia 2023

Respetados Directivos:

Comedidamente, me permito solicitar de su valiosa colaboración con el diligenciamiento de la encuesta que se relaciona en el enlace y que tiene como propósito identificar las necesidades en cuanto a temas que pueden ser abordados en las próximas Jornadas de Sensibilización de Seguridad y Privacidad de la Información, acorde al Plan Institucional de Sensibilización y Entrenamiento en Seguridad y Privacidad de la Información – ESG-SSI-PL01, donde se enmarca la importancia de tener impacto en el conocimiento de los funcionarios de la Universidad de Cundinamarca o reforzar buenas prácticas, facilitando que los funcionarios reconozcan los temas de interés y como afectan estos su cotidianidad.

<https://forms.office.com/r/d4n58VKydB>

Agradezco diligenciar la encuesta antes del día 12 de julio de 2023.

Pendiente de sus comentarios y/o sugerencias.

Cordialmente,



UCUNDINAMARCA
GENERACIÓN SIGLO 21

María del Pilar Delgado Rodríguez
Coordinadora del Sistema de Gestión de Seguridad de la Información - SGSI
sgsi@ucundinamarca.edu.co
Teléfono +57 (1) 828 14 83 Ext. 265
Diagonal 18 No. 20-29

Activar Windows

Ve a Configuración para activar Windows.

07 de julio de 2023

Resultados Forms enviado

6. Sobre Privacidad de la Información ¿Cuál de los siguientes temas le gustaría que formara parte de las Jornadas de Sensibilización en Seguridad y Privacidad de la Información?

[Más detalles](#)

Uso Correcto de contraseñas	7
En que caso los titulares pueden...	22
Transferencia internacional de D...	4
Otras	3



7. Sobre Seguridad de la Información ¿Cuál de los siguientes temas le gustaría que formara parte de las Jornadas de Sensibilización en Seguridad y Privacidad de la Información?

[Más detalles](#)

Teletrabajo y sus riesgos	18
Cifrado de información	13
Resultados de Auditoría	3
Otras	2



06

Temas a tratar según la encuesta sobre temas a incluir en las Jornadas de Sensibilización de Seguridad y Privacidad de la Información vigencia 2023



Por voluntad del Titular, siempre y cuando no vaya en contra de la ley.



Cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.



Cuando se haya superado el periodo razonable para el cumplimiento de los fines para los que fueron recolectados.



Hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recabados.

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-P06
	PROCESO GESTIÓN SISTEMAS INTEGRADOS	VERSIÓN: 2
	SUPRESIÓN DE DATOS PERSONALES	VIGENCIA: 2022-02-16
		PAGINA: 1 de 7

OBJETIVO:	Dar cumplimiento a los lineamientos estipulados en la normatividad legal vigente en cuanto a protección de datos, así como a los derechos que tienen los titulares de la Universidad de Cundinamarca.
ALCANCE:	El presente procedimiento va dirigido a todos los titulares de datos personales que pertenezcan a algún grupo de interés con el que la Universidad de Cundinamarca tenga vinculación contractual, académica, etc.
LÍDER DE PROCEDIMIENTO:	Oficial de Tratamiento de Datos Personales

DEFINICIONES	
CAUSAHABIENTE:	Persona que ha sucedido o se ha subrogado por cualquier título en el derecho de otra u otras. ¹
DATO PERSONAL:	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. ²
PETICIONARIO:	Que pide o solicita oficialmente algo. ³
SUPRESIÓN:	implica la eliminación o borrado seguro, total o parcial, de la información personal de acuerdo con lo solicitado por el titular en los registros, archivos, bases de datos o tratamientos realizados por la entidad. ⁴
TITULAR:	Persona natural cuyos datos personales sean objeto de Tratamiento. ⁵

6.1

**¿En qué casos
el Titular puede
solicitar la
Supresión de
Datos Personales?**



Uno de los principales riesgos del teletrabajo en relación a la Seguridad de la Información, es el acceso a los materiales, equipos o recursos de la empresa desde espacios ajenos a la organización



Se deben aplicar los mecanismos necesarios para detectar cualquier patrón anormal en el tráfico de la red



El uso indebido de contraseñas puede exponer a la compañía a los ciberdelincuentes.



7. RESULTADO EJERCICIO DE TELETRABAJO, TRABAJO REMOTO Y/O TRABAJO EN CASA

TELETRABAJO	TRABAJO EN CASA
DECRETO 1072 DE 2015	LEY 2088 DE 2021
Artículo 2.2.1.5.2. Teletrabajo y teletrabajador. Para efectos del presente capítulo el teletrabajo es una forma de organización laboral, que se efectúa en el marco de un contrato de trabajo o de una relación laboral dependiente, que consiste en el desempeño de actividades remuneradas utilizando como soporte las tecnologías de la información y la comunicación –TIC– para el contacto entre el trabajador y empleador sin requerirse la presencia física del trabajador en un sitio específico de trabajo. El teletrabajo solo aplica para los funcionarios de planta, provisionales de planta y libre nombramiento, libre remoción. Se debe reglamentar en la Universidad de Cundinamarca de acuerdo a la normatividad existente.	Artículo 2. Definición de Trabajo en Casa. Se entiende como trabajo en casa la habilitación al servidor público o trabajador del sector privado para desempeñar transitoriamente sus funciones o actividades laborales por fuera del sitio donde habitualmente las realiza, sin modificar la naturaleza del contrato o relación laboral, o legal y reglamentaria respectiva, ni tampoco desmejorar las condiciones del contrato laboral, cuando se presenten circunstancias ocasionales, excepcionales o especiales que impidan que el trabajador pueda realizar sus funciones en su lugar de trabajo, privilegiando el uso de las tecnologías de la información y las comunicaciones. Decretado por el gobierno, como fue el caso específico del COVID-19.



6.2

Teletrabajo y sus Riesgos



Asesoría Teletrabajo MinTIC

Seguimiento ▾

Este evento ocurrió el (Jue 13/07/2023, 'de' 11:00 AM a 12:00 PM)

Microsoft Teams Meeting:
Reunión de Teams

Mensajes Detalles de la reunión

Asesoría **TELETRABAJO** Min TIC Reunión de Microsoft Teams

Únete a través de tu computadora, aplicación celular o dispositivo de sala

[Haz clic aquí para unirse a la reunión](#)

ID de reunión: 2023 07 13 11 00 00

Código de acceso: 111 111 111

[Descargar Teams](#) | [Unirse en la web](#)



Ministerio de Tecnologías de la Información y las Comunicaciones **MinTIC**