UNIVERSIDAD DE CUNDINAMARCA

MANUAL DE ROLES Y RESPONSABILIDADES EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

FUSAGASUGÁ
2024

UNIVERSIDAD DE CUNDINAMARCA

MANUAL DE ROLES Y RESPONSABILIDADES EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

FUSAGASUGÁ
2024

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El presente manual pretende dar a conocer los distintos roles y responsabilidades en Seguridad y Privacidad de la Información, que son asignados a cada funcionario administrativo dentro de las distintas sedes, seccionales y extensiones, oficina de Bogotá, granjas agroambientales y el Centro Académico Deportivo – CAD, al momento de vincularse con la institución, sin importar su tipo de contratación; y que, por tanto, representan las directrices de necesario y obligatorio cumplimiento, al momento de recolectar, almacenar, circular, modificar o eliminar datos personales de Titulares e información reservada o confidencial de la Institución, a fin de reducir el riesgo de materialización de un incidente de seguridad y privacidad de la información.

Los lineamientos aquí descritos, se realizan en cumplimiento a la Guía N.4 Roles y Responsabilidades, proporcionada por el Ministerio de Tecnologías de la Información y las Comunicaciones Min TIC en el Modelo de Seguridad y Privacidad de la Información - MSPI, donde se indica cómo definir una estructura organizacional con funciones y responsabilidades para la ejecución de las actividades que esto conlleve, puesto que la designación del personal a estas tareas es necesario a tal punto que si no se entregan las responsabilidades para ciertos perfiles no se obtendrá la eficacia y efectividad que se requiere[1].

[1] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES –MinTIC. Guía N. 4 Roles y Responsabilidades. Seguridad y Privacidad de la Información. [Sitio web] Bogotá D.C: MINTIC. [Consultado: 11 julio 2021] Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

2. OBJETIVO GENERAL

Identificar y describir de forma detallada los distintos roles establecidos en la Estructura Organizacional de la Universidad, así como sus respectivas responsabilidades con el Programa Integral de Gestión de Datos Personales - PIGDP y del Sistema de Gestión de Seguridad de la Información - SGSI, a fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información, así como de dar cumplimiento a la Ley de Protección de Datos Personales y demás normatividad legal vigente a nivel Colombia.

2.1. OBJETIVOS ESPECÍFICOS

- Identificar y establecer el grupo de trabajo responsable de la Implementación del Modelo de Seguridad y Privacidad de la Información de la institución, así como los diferentes grupos de trabajo desde la Alta Dirección, definiendo el perfil y rol de conformidad con lo establecido según lineamiento de Seguridad de la Información – SGSI y lineamiento de Protección de Datos Personales de la Universidad de Cundinamarca.

- Determinar las diferentes responsabilidades con el Programa Integral de Gestión de Datos Personales – PIGDP y Sistema de Gestión de Seguridad de la Información - SGSI y dar a conocer los perfiles y responsabilidades de cada grupo de trabajo e identificar las personas idóneas para tomar cada rol. La socialización de estos grupos se debe comunicar a todos los miembros de la comunidad universitaria en general y a los funcionarios administrativos y docentes en particular.

3. ALCANCE

El alcance del presente manual y sus políticas está destinado a todos los funcionarios administrativos, docentes y estudiantes que se encuentren vinculados laboral o académicamente a la Universidad de Cundinamarca; y que en cumplimiento de sus responsabilidades contractuales o el desarrollo de actividades académicas se incluya el manejo de información reservada y confidencial y de datos personales (públicos, semi privados, privados y/o sensibles) de Titulares de la Universidad de Cundinamarca.

4. DEFINICIONES

ACTIVO DE INFORMACIÓN: Se refiere a cualquier información o elemento en físico y/o digital para el procesamiento, almacenamiento, comunicaciones, procesos, procedimientos y recursos humanos asociados con el manejo y uso de los datos para llevar a cabo las actividades estratégicas, misionales, de apoyo y seguimiento de la institución.[2]

ADMINISTRADOR DE SERVIDORES: Profesional o área encargada del monitoreo, configuración y manteniendo los recursos tecnológicos dedicados al almacenamiento de datos.

ADMINISTRADOR DE SISTEMAS DE INFORMACIÓN Y APLICATIVOS: "Profesional o área encargada de generar soluciones informáticas mediante la creación, adquisición y/o asesoramiento con la academia mediante la implementación de proyectos de grado y/o pasantías de sistema de información para los procesos de la Universidad de Cundinamarca".[3]

ADMINISTRADOR DE APLICATIVOS: "Profesional o área encargada de la parametrización, soporte y orientación a los usuarios en el buen uso de las aplicaciones establecidas en la Universidad de Cundinamarca y administrados por este proceso.".[4]

ADMINISTRADOR DE EQUIPOS DE CÓMPUTO Y HARDWARE: Profesional o área encargada de administrar y mantener en óptimas condiciones los recursos informáticos adquiridos y disponibles en la Universidad de Cundinamarca, garantizando la continuidad y disponibilidad de sus servicios tanto en Hardware como en Software.

[2] DEPARTAMENTO NACIONAL DE PLANEACIÓN, Consejo Nacional De Política Económica y Social República De Colombia, CONPES 3854 de 2016 [sitio web]. Bogotá D.C. [Consultado: 4 de agosto de 2022]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
[3] UNIVERSIDAD DE CUNDINAMARCA. Manual de Sistemas y Tecnología. [sitio web]. Fusagasugá. [Consultado: 19 de septiembre de 2022]. Disponible en: https://plataforma.ucundinamarca.edu.co/aplicaciones/calidad/apl_gen_ini.jsp?id=10
[4] Ídem

ADMINISTRADOR DEL PORTAL INSTITUCIONAL: Profesional o área encargada del publicar y gestionar los recursos digitales en el sitio web de las Universidad de Cundinamarca.

ADMINISTRADOR DE REDES SOCIALES DE LA UNIVERSIDAD: "Profesional o área encargada se encarga de gestionar, construir, informar y moderar comunidades que se construyen en torno a una marca, a través de redes sociales"[5]

ADMINISTRADORES DE LAS BASES DE DATOS: Profesional o área encargada de gestionar el sistema de base de datos (DBMS), es decir, administrar, supervisar y asegurar el buen uso de los datos institucionales, así como también garantizar el resguardo y la recuperación de los datos.

COMITÉ DEL SISTEMA DE ASEGURAMIENTO DE LA CALIDAD – SAC: "Es el conjunto de instituciones o instancias definidas por el marco normativo vigente que se articulas por medio de políticas y procesos diseñados con el propósito de asegurar la calidad de las instituciones y de sus programas."[6]

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Situación que indique una posible brecha en las Políticas o una falla en los controles y/o protecciones establecida. [7]

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 de la entidad[8].

RESPONSABLE DEL TRATAMIENTO: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos[9].

---

[5] UNIVERSIDAD DE CUNDINAMARCA. Manual de Sistemas y Tecnología. [sitio web]. Fusagasugá. [Consultado: 19 de septiembre de 2022]. Disponible en: https://plataforma.ucundinamarca.edu.co/aplicaciones/calidad/apl_gen_ini.jsp?id=10

[6] DECRETO 1330 de 2019. Artículo 2.5.2.1.2

[7] HOSPITAL GENERAL DE MEDELLÍN. Manual de Seguridad de la Información. Disponible en:https://www.hgm.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=203

[8] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN. Guía N. 21 para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Seguridad y Privacidad de la Información. [Sitio web] Bogotá D.C: MINTIC. [Consultado: 11 julio 2021] Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

[9] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN. Guía N. 4 de Roles y Responsabilidades. Seguridad y Privacidad de la Información. [Sitio web] Bogotá D.C: MINTIC. [Consultado: 11 julio 2021] Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.Pdf

SGSI: Sistema de Gestión de Seguridad de la Información. Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000)[10].

[10] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de Seguridad y Privacidad de la Información. Seguridad y Privacidad de la Información. [Sitio web] Bogotá D.C: MINTIC. [Consultado: 11 julio 2021] Disponible en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150517_Modelo_de_Seguridad_Privacidad.pdf

5. ROLES Y RESPONSABILIDADES

Las responsabilidades de Seguridad de la Información se asignarán según los roles estipulados en la Estructura Orgánica Funcional y Directivos (Figura 1), establecida mediante el Acuerdo 008 de 2012; donde además de las funciones contractuales adquiridas por cada funcionario, especificadas en la Resolución 064 de 2012, se asignarán a los coordinadores de las distintas áreas y/o dependencias, funciones y responsabilidades con la Seguridad de la Información de la Institución.

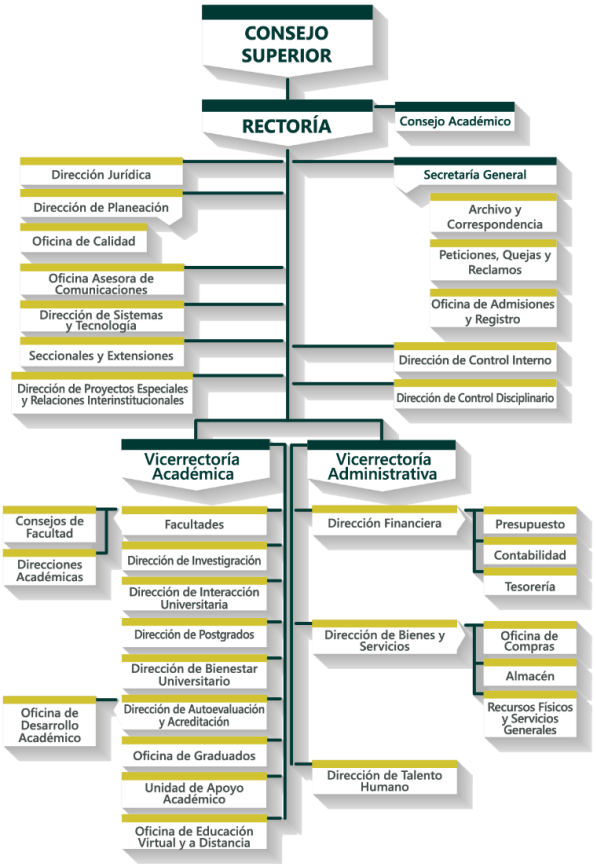

Figura 1. Estructura Orgánica Funcional y Directivos

5.1 RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

Según lo establecido por la Guía N° 4 del Modelo de Seguridad y Privacidad de la Información – MSPI las responsabilidades son las siguientes:

- Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias del proyecto, de manera que cumpla o exceda las necesidades y expectativas de los interesados en el mismo

- Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación de la entidad.
- Generar el cronograma de la implementación del Modelo de Seguridad y privacidad de la información.
- Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido.
- 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.
- Trabajar de manera integrada con el grupo o áreas asignadas.
- Asegurar la calidad de los entregables y del proyecto en su totalidad.
- Velar por el mantenimiento de la documentación del proyecto, su custodia y protección.
- Contribuir al enriquecimiento del esquema de gestión del conocimiento sobre el proyecto en cuanto a la documentación de las lecciones aprendidas.
- Liderar la programación de reuniones de seguimiento y velar por la actualización de los indicadores de gestión del proyecto.

5.2 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.

5.3 OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

- Definir los indicadores que permitan evaluar el nivel de gestión y el desarrollo del PIGDP.

- Asesorar y orientar a cada una de las áreas de la entidad, con la finalidad de desarrollar cada uno de los lineamientos que permitan la correcta adopción del PIGDP.
- Realizar capacitaciones periódicas a los funcionarios de la entidad, para sensibilizarlos sobre las responsabilidades asignadas y demás temas que se le relacionen.
- Definir los lineamientos en que los encargados del tratamiento de las bases de datos de la universidad realicen su tratamiento.
- Realizar seguimiento constante al PIGDP, implementando acciones de mejora continua y rindiendo los informes correspondientes a la Comisión de Gestión de ser el caso.
- Aconsejar a la Comisión de Gestión en las decisiones que deba tomar para lograr el cabal cumplimiento del PIGDP.
- Diligenciar los documentos implementados para el control y seguimiento de las actividades asociadas a la promoción y seguridad de los datos personales al interior de la universidad.
- Revisar de forma periódica y socializar internamente la Política de Protección de Datos Personales.
- Aprobar las modificaciones que se realicen a los procedimientos internos, relacionados con la protección de datos personales.
- Absolución de dudas frente al PIGDP.
- Articulación del inventario de los datos personales bajo los procesos que se desarrollan dentro de la Institución.
- Reportar las actualizaciones y novedades de reclamos e incidentes de Protección de Datos Personales sobre las bases de datos de la Universidad en la plataforma del Registro Nacional de Bases de Datos – RNBD.
- Informar periódicamente a la Comisión de Gestión los asuntos relacionados con la adopción del PIGDP y las posibles medidas de control.
- La función esencial de un OPD en la organización se encuentra la de supervisar el cumplimiento del Régimen General de Protección de Datos Personales. Precisamente, la importancia de que los responsables y encargados del Tratamiento cuenten con la colaboración de un OPD.
- A nivel institucional la Resolución 091 de 2023 “POR LA CUAL SE ESTABLECEN LOS LINEAMIENTOS DE PROTECCIÓN DE DATOS PERSONALES DE LOS TITULARES DE LA UNIVERSIDAD DECUNDINAMARCA”, en su ARTÍCULO DÉCIMO CUARTO. - establece OFICIAL DE PROTECCIÓN DE DATOS – “El Oficial de Protección de Datos Personales, será designado por la dirección de la Universidad de Cundinamarca, articulándose con la Coordinador(a) del Sistema de Gestión de Seguridad de la información y el equipo táctico - operativo del SGSI, quienes apoyarán la implementación de la Ley de Protección de Datos de los Titulares de la Universidad de Cundinamarca, para lo cual la dirección de la Universidad de Cundinamarca asegurará la capacitación continua de los funcionarios del área del SGSI”.

5.4 OFICIAL DE SEGURIDAD DE LA INFORMACIÓN (CISO)

- Generar e implantar políticas de seguridad de la información.
- Adoptar o adecuar el procedimiento formal para la gestión de riesgos, comunicando los resultados a la Comisión de Gestión.
- Validar el cumplimento de los lineamientos derivados del SGSI.
- Fomentar la capacitación idónea para todos los funcionarios de la Universidad de Cundinamarca en cuanto a seguridad de la información.
- Regular la gestión de activos de información, teniendo en cuenta su clasificación y las medidas de seguridad pertinentes.
- Supervisar la administración del control de acceso a la información.
- Apoyar los requerimientos necesarios que contribuyan a la seguridad de la información, en el desarrollo, implementación, mantenimiento o adquisición de los diversos sistemas de información.
- Comprobar los requisitos de seguridad de la información en las relaciones con proveedores, gestionando las acciones necesarias tanto interna como externamente.
- Velar por el cumplimiento normativo de la seguridad de la información.
- Estar al tanto de la gestión de incidentes de seguridad de la información.
- Liderar la implantación del SGSI.
- Asegurar la inclusión de la continuidad de seguridad de la información en el plan de continuidad del negocio.
- Validar la implantación de los requisitos de seguridad necesarios a nivel administrativo, tecnológico y operativo.
- Revisar periódicamente el estado del SGSI a partir de indicadores definidos.
- Presentar presupuesto anual para mantener y mejorar continuamente el SGSI.
- Implementar un programa de auditorías de seguridad, revisando y comunicando oportunamente los resultados a las partes interesadas.

5.5 ALTA DIRECCIÓN, DIRECTORES Y JEFES DE ÁREA, DECANOS Y DIRECTORES Y/O COORDINADORES 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 y en el ESG-SSI-M003 Manual de Directrices para Contacto por Mensajería Instantánea

- 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
- Atender los requerimientos y solicitudes presentados por el Oficial de Seguridad de la Información.
- Apoyar la difusión y sensibilización de la seguridad de la información en la Universidad de Cundinamarca.
- 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.
- Articular las acciones pertinentes en la presentación de reportes a incidentes de seguridad de los funcionarios a cargo, siguiendo los lineamientos o guías expuestos por el SGSI.
- Coordinar con las áreas encargadas el control de acceso a las instalaciones o recintos de la institución priorizando los niveles de accesos permitidos.
- Promover el cuidado y buen uso de los activos fijos del institucional asignado a su cargo.
- Asegurar la gestión de las Autorizaciones para el Tratamiento de Datos personales, de los Titulares internos y externos de la Universidad de Cundinamarca, en cumplimiento de la Ley 1581 de 2012 y demás normatividad legal vigente.
- Recopilar, registrar y gestionar el registro de activos de la información del área, para su consolidación, publicación y posterior consulta en el portal de Datos abiertos de Colombia, en cumplimiento de la Ley 1712 de 2014
- Gestionar las actividades de los planes de Mejoramiento producto de Auditorías internas, Asesorías y verificaciones de Cumplimiento del Sistema de Gestión de Seguridad de la Información y la Ley de Protección de Datos Personales.

5.6 DIRECCIÓN DE CONTROL INTERNO

- Realizar seguimiento y reportar el cumplimiento a la normatividad legal vigente a nacional y de manera interna acerca de seguridad de la información.
- Reportar evolución del Sistema de Gestión de Seguridad de la Información a los órganos directivos pertinentes en la Universidad.

5.7 EQUIPO TÁCTICO – OPERATIVO DEL SGSI

Además de las anteriores responsabilidades que aplican para todos los usuarios, los funcionarios que forman parte del SGSI deben asumir las siguientes:

- Apoyar el Sistema de Gestión de Seguridad de la Información y al coordinador del SGSI con las actividades, planes y el seguimiento dentro de la Universidad.

- Proponer políticas, procedimientos, manuales, guías e instructivos que ayuden a dar cumplimiento a la normatividad legal vigente en materia de Seguridad de la Información y Protección de Datos Personales de los Titulares de la Universidad.
- Diseñar campañas y mecanismos para la apropiación de las diferentes, políticas, procedimientos, manuales, guías e instructivos derivados del Sistema de Gestión de Seguridad de la Información.
- Propender el cumplimiento de los lineamientos y directrices de Seguridad de la Información en el desarrollo de todos los Sistemas de Información y Aplicativos que utiliza la Universidad.
- Informar a la comunidad universitaria en general sobre las modificaciones, avances y reportes de la Institución en materia de Seguridad de la Información y Protección de Datos Personales.
- Asesorar a las respectivas área y oficinas en el desarrollo y **cumplimiento** de las actividades propuestas por el SGSI, propendiendo por la continuidad e idoneidad de los procesos y la adecuada prestación de servicios.
- Emplear la metodología indicada por el Oficial de Seguridad de la Información, en cuanto a la gestión de riesgos y la administración del registro periódico de activos de información, realizando las correcciones y/o ajustes a los que haya lugar.
- Gestionar adecuadamente los incidentes de seguridad de la información, a partir de los protocolos de respuesta previamente validados, según estándares de seguridad reconocidos.
- Capacitar periódicamente a todo el personal de la Universidad a nivel general y específico, en materia de seguridad de la información.
- Realizar auditorías internas de seguridad de la información en todas las áreas de la institución, según cronograma elaborado por el Oficial de Seguridad de la Información.

5.8 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 GUÍA FINALIDADES PARA EL TRATAMIENTO DE DATOS PERSONALES DE LOS TITULARES DE LA UNIVERSIDAD DE CUNDINAMARCA
- Asistir y participar de la 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 - SIC.

- Cumplir con las políticas, lineamientos, directrices y normatividad como se define en el Manual ESG-SSI-M001 MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN y cualquier documento que las desarrolle o complemente.
- 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.
- Participar de las visitas por parte de los Vigías de Seguridad de la Información cuando se requiera.
- Participar de las Auditorías internas y/o externas y Verificación de Cumplimiento de Protección de Datos que realice el Sistema de Gestión de Seguridad de la Información -SGSI.
- Tramitar cuando sea pertinente las consultas, solicitudes y reclamos de los titulares de la Universidad de Cundinamarca.

5.9 FUNCIONARIOS DEL CENTRO ACADÉMICO DEPORTIVO – CAD

5.9.1 Responsabilidades del Director con el SGSI

- Gestionar la adopción y cumplimiento del Manual de Roles y Responsabilidades entre los funcionarios administrativos del Centro Académico Deportivo - CAD, en todas las modalidades de contratación.
- Incentivar el adecuado uso del Correo Electrónico Institucional para envío y recepción de información entre funcionarios administrativos y entrenadores, 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 los procesos necesarios para la aprobación, levantamiento, actualización y mantenimiento de los activos de información pertenecientes al Centro Académico Deportivo – CAD.
- Coordinar con las áreas encargadas el control de acceso al Centro Académico Deportivo – CAD priorizando los niveles de accesos permitidos.
- Asegurar que se recolecte la autorización para el Tratamiento de Datos Personales de los deportistas del Club Cundinamarca y personal externo, y el adecuado uso, circulación y transferencia de los Datos Personales.
- Usar únicamente los Datos Personales que hayan sido obtenidos mediante autorización y atendiendo las finalidades expuestas en la guía ESG-SSI-G007 GUÍA FINALIDADES PARA EL TRATAMIENTO DE DATOS PERSONALES DE LOS TITULARES DE LA UNIVERSIDAD DE CUNDINAMARCA

- Inscribir las bases de datos a su cargo, que contengan datos personales (públicos, semi privados, privados y/o sensibles) según los lineamientos establecidos por el SGSI.
- No compartir información confidencial con terceros no autorizados, tal como se documenta en el ESG-SSI-F002 ACUERDO DE CONFIDENCIALIDAD PARA MIEMBROS DEL TALENTO HUMANO, PASANTES Y MONITORES.
- Asistir y participar de la 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 - SIC.
- 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 presentada en el CAD, que se considere un evento y/o incidente de seguridad y privacidad de la información.
- Participar de las visitas por parte de los Vigías de la Información cuando se requiera.
- Participar de las Auditorías internas y/o externas y Verificación de Cumplimiento de Protección de Datos que realice el Sistema de Gestión de Seguridad de la Información -SGSI.
- Respetar y cumplir las Políticas, Lineamientos, Directrices, y Procedimientos, en materia de Seguridad y Privacidad de la Información.
- Verificar el retiro de roles en la plataforma institucional y/o cualquier otro sistema de información al cual tuviese acceso y que albergue información sensible del Centro Académico Deportivo – CAD de los funcionarios cuando se presente algún retiro o licencia.
- Salvaguardar y dar uso adecuado a los activos de la información registrados en el Centro Académico Deportivo – CAD.

5.9.2 Responsabilidades del Personal Administrativo del CAD con el SGSI

- Recolectar la autorización para el Tratamiento de Datos Personales de los deportistas del Club Cundinamarca y personal externo, y el adecuado uso, circulación y transferencia de los Datos Personales.
- Usar únicamente los Datos Personales que hayan sido obtenidos mediante autorización y atendiendo las finalidades expuestas en la guía ESG-SSI-G007 GUÍA FINALIDADES PARA EL TRATAMIENTO DE DATOS PERSONALES DE LOS TITULARES DE LA UNIVERSIDAD DE CUNDINAMARCA
- Asistir y participar de la 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 - SIC.
- 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 presentada en el CAD, que se considere un evento y/o incidente de seguridad y privacidad de la información.
- Participar de las visitas por parte de los Vigías de la Información cuando se requiera.
- Participar de las Auditorías internas y/o externas y Verificación de Cumplimiento de Protección de Datos que realice el Sistema de Gestión de Seguridad de la Información -SGSI.
- Dar un uso adecuado a la información, así como de los activos de la información asignados en su espacio de trabajo.
- Respetar y cumplir las Políticas, Lineamientos, Directrices, y Procedimientos, en materia de Seguridad y Privacidad de la Información.

5.9.3 Responsabilidades de los Entrenadores Deportivos con el SGSI

- Usar únicamente los Datos Personales que hayan sido obtenidos mediante autorización y atendiendo las finalidades expuestas en la guía ESG-SSI-G007 GUÍA FINALIDADES PARA EL TRATAMIENTO DE DATOS PERSONALES DE LOS TITULARES DE LA UNIVERSIDAD DE CUNDINAMARCA.
- Comunicarse únicamente por las líneas Institucionales de WhatsApp con el padre del deportista (si es menor de edad).
- Asistir y participar de la 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 - SIC.
- 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 presentada en el CAD, que se considere un evento y/o incidente de seguridad y privacidad de la información.
- Participar de las visitas por parte de los Vigías de la Información cuando se requiera.
- Participar de las Auditorías internas y/o externas y Verificación de Cumplimiento de Protección de Datos que realice el Sistema de Gestión de Seguridad de la Información -SGSI.
- Respetar y cumplir las Políticas, Lineamientos, Directrices, y Procedimientos, en materia de Seguridad y Privacidad de la Información.

5.9.4 Responsabilidades de Contratistas o Proveedores con el SGSI

- Respetar y cumplir las Políticas, Lineamientos, Directrices, y Procedimientos, en materia de Seguridad y Privacidad de la Información, que se encuentran disponibles para consulta en el Modelo de Operación Digital, macroproceso Estratégico, procesos Sistemas Integrados – Sistema de Gestión de Seguridad de la Información - SGSI.

6. RESPONSABILIDADES DE ACUERDO CON LOS PERFILES

6.1 FUNCIONARIOS CON PERFIL DE USUARIO

Los funcionarios que cuentan con un perfil de usuario son todos aquellos que utilizan los sistemas de información y aplicativos de la Institución para realizar sus respectivas labores, pero no tienen privilegios para adminístralos, ni gestionarlos. En este grupo se encuentran todos los funcionarios operativos que dependen de una oficina o una dirección dentro de la institución, además cuentan con este mismo perfil los Docente y Estudiantes que utilizan la Plataforma, Aula Virtual y Portal Institucional; y que por tanto deben cumplir con las siguientes responsabilidades:

- Respetar y cumplir los procedimientos, directrices y lineamientos definidos en la Política de Seguridad de la Información, establecida en la 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".
- Propender por la continua confidencialidad, integridad y disponibilidad de la información.
- Dar un uso adecuado a la información, así como de los activos de la información asignados en su espacio de trabajo.
- Acatar la normativa legal vigente a nivel nacional sobre Seguridad y Privacidad de la Información.
- Reportar y/o notificar al Sistema de Gestión de Seguridad de la Información, al Área de Servicios Tecnológicos, al Oficial de Seguridad de la Información o al Oficial de Tratamiento de Datos Personales, cualquier irregularidad que se considere un evento que atente contra la confidencialidad, integridad y disponibilidad de la información, así como situaciones sospechosas que evidencien un riesgo al incumplimiento de la normatividad.

6.2 FUNCIONARIOS CON ACCESO PRIVILEGIADO

Los funcionarios con acceso privilegiado son los ingenieros que pertenecen a la Dirección de Sistemas y Tecnología, con privilegios para administrar, gestionar, crear y realizar modificaciones en los Sistemas de Información y aplicativos que son utilizados por Administrativos, Docentes y Estudiantes de la Institución, así como acceso a equipos de usuario, red cableada, centros de datos y acceso físico a las áreas restringidas que están relacionadas con los sistemas de información institucionales. De igual forma, reúne a los funcionarios que administran el Portal Institucional y las Redes Sociales de la Universidad.

Teniendo en cuenta lo anterior se asignan las Responsabilidades con el Sistema de Gestión de Seguridad de la Información, según el acceso que tengan a la información, así:

6.2.1 Responsabilidades con el SGSI del Administrador de Sistemas de Información y Aplicativos.

- Implementar procedimientos formales para impedir el acceso no autorizado a los Sistemas de Información.
- Dar reporte de eficiencia de los procedimientos.
- Documentar, comunicar y controlar la asignación de derechos de acceso a los Sistemas de Información, bases de datos y servicios de información.

6.2.2 Responsabilidades con el SGSI del Administrador de Servidores

- Restringir el acceso físico al personal no autorizado a la sala donde se encuentren servidores.
- Registrar todos los cambios que se realicen a las salas de servidores o al cableado, especificando el nombre y documento de identificación del funcionario que accedió, motivo, procesos, actividades o cambios realizados, etc.

6.2.3 Responsabilidades con el SGSI del Administrador de Equipos de cómputo y hardware.

- Documentar y controlar la apropiada asignación de contraseñas a los equipos de cómputo.
- Realizar el respaldo o Back Up necesario y en los tiempos estipulados, según el Manual de Políticas de Back Up de la Institución.
- Documentar los cambios o mantenimientos que se realicen a los equipos de cómputo.

6.2.4 Responsabilidades con el SGSI del Administrador del Portal Institucional y Redes Sociales de la Universidad.

Controlar el tipo de datos e información publicados en el portal institucional y en las redes sociales, velando porque no se incumpla ninguna política derivada del SGSI y adoptada por la Universidad.

Informar a estudiantes, administrativos, docentes y comunidad en general, sobre las políticas, procedimientos, manuales, guías e instructivos derivados del SGSI y adoptados por la Universidad.

6.2.5 Responsabilidad con el PIGDP de los funcionarios administradores de las bases de datos

- Informar al Oficial de Tratamiento de Datos Personales sobre los riesgos identificados en las bases de datos de la Institución.

- Dar cumplimiento a las responsabilidades asignadas por el Oficial de Tratamiento de Datos Personales.
- Evaluar de forma periódica los niveles de acceso a las bases de datos de los funcionarios de cada área.
- Informar cualquier cambio en las bases de datos de su custodia para realizar las actualizaciones que por Ley deben realizarse, en especial frente a cambios sustanciales.

6.3 FUNCIONARIOS ÁREA DE SERVICIOS TECNOLÓGICOS

Los funcionarios del área de servicios tecnológicos deben aceptar las siguientes responsabilidades, adicionales a las ya especificadas a nivel de usuario:

- Ejecutar las instrucciones impartidas por el SGSI o el Oficial de Seguridad de la Información, acordes a las políticas de seguridad de la información establecidas en la Universidad de Cundinamarca y en el desarrollo de su competencia.
- Garantizar las medidas técnicas y operativas necesarias para implementar controles de seguridad de la información en toda la infraestructura de T.I.
- Implementar las medidas necesarias para asegurar la confidencialidad, integridad y disponibilidad de los servicios suministrados, incluyendo todo el equipo informático administrado.
- Utilizar privilegios de administración únicamente para el desarrollo de sus funciones laborales y acordes al fortalecimiento de la seguridad de la información. Está prohibido emplearlos para beneficios personales o de terceros sin autorización.
- Establecer medidas de seguridad de la información en conjunto con el SGSI en Data Center, acordes a las políticas de seguridad establecidas por la empresa propietaria del mismo.

6.4. FUNCIONARIOS ÁREA DE SISTEMAS DE INFORMACIÓN

Los funcionarios que pertenecen al área de sistemas de información, además de cumplir con las responsabilidades a nivel de usuario, deben:

- Ejecutar las instrucciones impartidas por el SGSI o el Oficial de Seguridad de la Información, acordes a las políticas de seguridad y privacidad de la información establecidas en la Universidad de Cundinamarca y en el desarrollo de su competencia.
- Recibir y aplicar la capacitación brindada por la institución en materia de seguridad y privacidad de la información, al desarrollar, probar, desplegar, implementar y mantener los diferentes sistemas de información
- Promover la incorporación de mecanismos de identificación, autenticación, autorización y auditoría que contribuyan a la confidencialidad, integridad y

disponibilidad de la información, accesible desde los distintos sistemas empleados.

- Utilizar privilegios de administración únicamente para el desarrollo de sus funciones laborales y acordes al fortalecimiento de la seguridad de la información. Está prohibido emplearlos para beneficios personales o de terceros sin autorización.
- Establecer medidas de seguridad de la información en conjunto con el SGSI, al adquirir sistemas de información por parte de terceros.
- Establecer, documentar, implementar y realizar seguimiento a los controles del Anexo A de la norma ISO/IEC 27001:2013, de acuerdo con la competencia del área

6.5. FUNCIONARIOS - VIGÍAS DE SEGURIDAD DE LA INFORMACIÓN

Los vigías de seguridad de la información son funcionarios del Sistema de Gestión de Seguridad de la Información – SGSI, que actuarán como veedores de seguridad y privacidad de la información, con un alto grado de responsabilidad y una conciencia clara frente a los principios del SGSI, serán dinamizadores de los lineamientos (políticas) global de seguridad de la información y de protección de datos personales de los titulares dela Universidad de Cundinamarca, de acuerdo con la normatividad legal vigente interna y/o externa.

Funciones de los vigías de seguridad de la Información – SGSI

- El o los Vigías de Seguridad de la Información – SGSI, es un rol que asumirán los funcionarios del Sistema de Gestión de Seguridad de la Información – SGSI, para lo cual deben estar certificados en la Norma ISO/IEC 27001 y conocer la normatividad a nivel nacional en Seguridad y privacidad de la Información – MSPI expedida por el Mintic y la Superintendencia de Industria y Comercio, de igual forma la normatividad interna.
- La participación 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, deberán realizar visitas a las diferentes áreas a nivel institucional, donde de manera aleatoria verificaran el cumplimiento de los lineamientos y directrices documentadas y que deben ser comunicadas a la comunidad universitaria a través de los diferentes mecanismos de socialización, como son las jornadas de sensibilización y entrenamiento, el aula virtual del SGSI, la campaña de protección de datos, los correos del sgsi@ucundinamarca.edu.co y alertas@ucundinamarca.edu.co
- El o los Vigías de Seguridad de la Información – SGSI, deben asegurar que se visitaran todas las áreas de sedes, seccionales, extensiones, oficina de Bogotá, Centro Académico deportivo y granjas agroambientales, por lo menos una vez en cada vigencia (siempre y cuando se cuente con el personal suficiente en el SGSI), con el fin de asegurar las buenas prácticas en cada sitio, para este punto se contara con el compromiso, apoyo y participación de

los directores de área, jefes de oficina, directores administrativos de seccionales y extensiones y los ingenieros de apoyo.

- Documentar las debilidades encontradas y que son malas prácticas por parte de los funcionarios y que son eventos que se pueden convertir en posibles riesgos. Comunicar a la Comisión de Gestión, en sesión ordinaria e informar las acciones adelantadas para minimizar los eventos detectados.
- Documentar las fortalezas encontradas y las buenas prácticas por parte de los funcionarios. Comunicar a la Comisión de Gestión, en sesión ordinaria e informar el mecanismo para su institucionalidad.
- Revisión al cumplimiento de los procedimientos, manuales, guías e instructivos de la Dirección de Sistemas y Tecnología donde se propenda alguno de los principios de la seguridad de la información (Confidencialidad, integridad y disponibilidad).
- Él o los Vigías de Seguridad de la Información – SGSI, deberán reportar 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.

6.6 FUNCIONARIOS – EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El equipo encargado de dar respuesta a los incidentes de Seguridad y Privacidad de la información, estará liderado por los coordinadores del Área de Servicios Tecnológicos y del Sistema de Gestión de Seguridad de la Información-SGSI, quienes actuarán como responsables del tratamiento de eventos e incidentes que se presenten en la institución y que no cumplan con las políticas, lineamientos, directrices y normas tanto internas como externas, así mismo, se designarán gestores de cada una de las áreas mencionadas anteriormente para apoyar la gestión y las actividades táctico y operativas que se desarrollan en el procedimiento ESG-SSI-P09 – Gestión de Incidentes de Seguridad de la Información. Adicionando a las anteriores responsabilidades mencionadas a nivel de funcionarios.

Funciones del equipo de respuesta inmediata a incidentes de Seguridad de la Información:

- El equipo de respuesta a incidentes de Seguridad y Privacidad de la información es una responsabilidad que asumirán los funcionarios del Sistema de Gestión de Seguridad de la Información – SGSI y el Área de Servicios Tecnológicos en compañía del Oficial de Seguridad de la Información (CISO) o el Oficial de Protección de Datos Personales.
- Articular de forma adecuada los procedimientos relacionados a la gestión de incidentes de seguridad de la información, con las áreas involucradas, de acuerdo con los controles establecidos en el anexo A de la norma ISO/IEC 27001.

- Detectar, analizar, evaluar y tratar los casos de eventos o incidentes que atenten contra los principios de Seguridad y Privacidad de la Información, dentro de la Universidad.
- Recolectar y analizar la evidencia física y/o digital, con el fin de darle el tratamiento que está requiera, en caso de una acción legal y/o disciplinaria ya sea interna o externa.
- Clasificación, valorización y priorización de los incidentes de Seguridad y Privacidad de la Información y en caso de requerirse, deberán generar plan de contención para estos, articulados con entes de control.
- Seguimiento a los eventos y/o incidentes de seguridad y privacidad de la información, para cierre o socialización para la toma de decisión en el Comité SAC, Comisión de Gestión, Comisión de Control Interno y demás instancias de la Alta Dirección, cuando se materialice un riesgo por perdida de Confidencialidad, Integridad y/o Disponibilidad de la Información, y según el caso se dará tramite a la Dirección de control Disciplinario para los fines pertinentes
- Escalar a las instancias pertinentes, los incidentes de Seguridad de la información donde se involucre la realización de una investigación forense en la Universidad.
- Escalar a las instancias externas pertinentes, los incidentes donde se afecte o ponga en riegos la seguridad de la información de la Universidad.
- Comunicar el desarrollo y el manejo de los incidentes a las partes interesadas, asegurar la resolución de estos, como también el cierre formal de este, además deberán documentar lecciones aprendidas del incidente, desde la recopilación y la organización de las evidencias resultantes, como producto de investigación, adicional a esto, dependiendo de la situación se informará a las entidades competentes y/o partes interesadas.

7. SEGURIDAD DEL PERSONAL

7.1 VINCULACIÓN DE LOS FUNCIONARIOS

La Universidad de Cundinamarca reconoce la importancia del Talento Humano para la realización y cumplimiento de sus funciones misionales de la institución, así como el riesgo que conlleva la recolección, almacenamiento, uso, circulación y/o supresión de la información por parte del mismo; por tal motivo, y con la intención de contar con funcionarios idóneos, donde se garantice que el proceso de vinculación se realizará acordé con la legislación vigente y dando cumplimiento a los roles y responsabilidades con el SGSI, se dan las siguientes normas de vinculación de funcionarios administrativos y docentes en sede, seccionales, extensiones, oficina de Bogotá y Centro Académico Deportivo – CAD.

7.1.1 Normas dirigidas a la Alta Dirección

- La Alta Dirección debe demostrar su compromiso con la gestión de seguridad y privacidad de la información, por medio de la aprobación de políticas, normas y demás lineamientos del SGSI.
- La Alta Dirección debe promover la importancia de la Seguridad y Privacidad de la Información entre todos los funcionarios administrativos y docentes, motivando el entendimiento, la toma de conciencia y el estricto cumplimiento, de las políticas, normas, procedimientos, manuales, directrices y lineamientos para la Seguridad y Privacidad de la Información.
- La Alta Dirección debe definir, establecer y aprobar el proceso disciplinario, así como el tratamiento de las faltas a las políticas de Seguridad y Privacidad de la Información o los incidentes que puedan presentarse.

7.1.2 Normas dirigidas a la Dirección de Talento Humano

- La Dirección de Talento Humano durante el proceso de vinculación de funcionarios administrativos y docentes debe realizar, antes de su vinculación definitiva, las verificaciones necesarias para confirmar la autenticidad de la información suministrada por el personal candidato a ocupar cualquier cargo en la Institución.
- La Dirección de Talento Humano debe certificar que los funcionarios administrativos y docentes de la Universidad de Cundinamarca firmen el formato ESG-SSI-F001 - Autorización para el Tratamiento de Datos Personales de titulares de la Universidad y ESG-SSI-F002- Acuerdo de confidencialidad para miembros del talento humano, pasantes y monitores, anexando estos documentos como requisito indispensable durante el proceso de contratación.
- La Dirección de Talento Humano debe convocar a los funcionarios administrativos y docentes vinculados a la institución, a las charlas, conversatorios y demás eventos programados que promuevan la concienciación en Seguridad y Privacidad de la Información, así como proveer los recursos para la respectiva ejecución del evento y su control de asistencia, aplicando las sanciones pertinentes por falta de asistencia no justificada.

7.1.3 Normas dirigidas a Supervisores de contrato, Directores de área, Jefes de Oficina, Decanos y Directores de programa.

- Cada Supervisor de contrato, Director de área, Jefe de oficina, Decano o Director de programa debe verificar la existencia de la Autorización de Tratamiento de Datos Personales de titulares de la Universidad y Acuerdo de confidencialidad para miembros del talento humano, pasantes y monitores previamente firmados, de todos los funcionarios antes de entregar acceso a la información y permisos a los Sistemas de Información de la Universidad.
- Cada Supervisor de contrato, Director de área, Jefe de oficina, Decano o Director de programa debe hacer entrega al funcionario de los activos de la información que estarán a su cargo durante el desarrollo del contrato y que

deben ser devueltos al finalizar el mismo, utilizando el formato ESG-SSI-F010 – Checklist para entrega y devolución de activos de la información.

7.1.4 Normas dirigidas al Oficial de Tratamiento de Datos Personales

- El Oficial de Tratamiento de Datos Personales debe velar que durante el desarrollo de vinculación y reinducción de funcionarios administrativos y docentes se informe a los mismos las políticas, normas, cláusulas, sanciones, procedimientos, manuales, directrices y lineamientos con los que cuenta la Universidad de Cundinamarca en cuanto a Seguridad y Privacidad de la Información.
- El Oficial de Tratamiento de Datos Personales debe verificar que todos los funcionarios administrativos y docentes vinculados, hayan diligenciado y firmado los formatos ESG-SSI-F001 - Autorización para el Tratamiento de Datos Personales de titulares de la Universidad y ESG-SSI-F002- Acuerdo de confidencialidad para miembros del talento humano, pasantes y monitores.

7.1.5 Normas dirigidas a funcionarios administrativos y docentes que se vinculan a la Institución

- Los funcionarios administrativos y docentes por vincularse en la institución deben firmar los formatos ESG-SSI-F001 - Autorización para el Tratamiento de Datos Personales de titulares de la Universidad y ESG-SSI-F002- Acuerdo de confidencialidad para miembros del talento humano, pasantes y monitores., previa contratación y antes de que se le otorgue acceso las instalaciones, plataforma, sistemas de información e información física.

  Nota: La firma de los documentos ESG-SSI-F001 y ESG-SSI-F002, se realizará una vez por cada vigencia y cubrirá la contratación de los dos periodos académicos de cada funcionario administrativo y docente.

- Todos los funcionarios que por sus funciones hagan uso de la información física o digital de la Universidad de Cundinamarca, deben dar cumplimiento a las políticas, normas, procedimientos, manuales, directrices y lineamientos de Seguridad y Privacidad de la Información, así como asistir a las capacitaciones, charlas o eventos referentes al mismo.
- Mantener la confidencialidad de las contraseñas y/o credenciales para el acceso a la plataforma institucional, correo electrónico de áreas y personal, aplicaciones, sistemas de información y recursos informáticos.
- Utilizar la información proporcionada por la Universidad y/o área específica, únicamente para los fines y propósitos autorizados por la institución.
- Asistir y/o participar de las jornadas de sensibilización en los temas de seguridad y privacidad de la información en general y las jornadas de entrenamiento en temas en particular, cursar y aprobar anualmente el aula virtual del SGSI, así como de charlas o eventos referentes al mismo.

- Participar de la jornada de entrenamiento para el registro de activos de información y los directores, jefes de área, decanos y directores y/o coordinadores de programas académicos, deberán realizar el registro de activos de acuerdo con el procedimiento ESG-SSI-P01 y demás documentos de referencia, mediante la herramienta que dispone el SGSI para adelantar el ejercicio anualmente, en cumplimiento de la Ley 1712 de 2014, en lo que respecta a Información Clasificada y Reservada.
- Informar al Sistema de Gestión de Seguridad de la Información – SGSI, al correo sgsi@ucundinamarca.edu.co o pdpsgsi@ucundinamarca.edu.co, cualquier incidente u oportunidad de mejora de seguridad de la información o protección de datos personales.
- No divulgar, compartir, suministrar, utilizar o enviar información contenida en los sistemas, plataformas, aplicativos, aulas virtuales, repositorios y otros recursos informáticos, a los cuales tenga acceso el funcionario para el desarrollo de su trabajo y actividades de manera remota, presencial o mixto, debe realizar una adecuada utilización y mantener la debida confidencialidad, integridad y disponibilidad de seguridad de la información y la protección de datos privados, semiprivados y sensibles.
- En auditorías internas o auditorias de certificación del Sistema de Seguridad de la Información, deberán atender con responsabilidad y proporcionar al equipo auditor la información necesaria y objetiva para asegurar un proceso de auditoría eficiente y eficaz.

7.2 DESVINCULACIÓN, LICENCIAS, VACACIONES O CAMBIO DE LABORES DE LOS FUNCIONARIOS

La Universidad de Cundinamarca asegurará que sus funcionarios administrativos y docentes con cualquier tipo de contratación serán desvinculados o reasignados a otro cargo de forma controlada, ordenada y segura, velando por la confidencialidad, integridad y disponibilidad de la información de la Institución, así como de los datos personales de titulares.

7.2.1 Normas dirigidas a la Dirección de Talento Humano

- La Dirección de Talento Humano debe realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios administrativos y docentes en cualquier tipo de contratación, por medio de procedimientos y dando cumplimiento a los controles establecidos.

7.2.2 Normas dirigidas a Supervisores de contrato, Directores de área Jefes de Oficina, Decanos y Directores de Programa

- Cada Supervisor de contrato, Director de área, Jefe de oficina, Decano o Director de programa, debe monitorear y reportar de forma inmediata la desvinculación o cambio de labores de cualquier funcionario administrativo y docente a la Dirección de Talento Humano.

- Cada Supervisor de contrato, Director de área, Jefe de oficina, Decano o Director de Área debe verificar que los activos de la información devueltos por el funcionario y consignados en el formato ESG-SSI-F010 – Checklist para entrega y devolución de activos de la información, sean los mismos que se asignaron al momento de la vinculación.
- Cada Supervisor de contrato, Director de área, Jefe de oficina, Decano o Director de Área debe solicitar a la Dirección de Sistemas y Tecnología, así como verificar que se haga el respectivo cambio de contraseñas de ingreso al correo electrónico del área al que el funcionario tenía acceso, así como el retiro de roles en la plataforma institucional y/o cualquier otro sistema de información al cual tuviese acceso y que albergue información sensible de la institución o datos personales de los titulares de la misma.

7.2.3 Normas dirigidas al Oficial de Protección de Datos Personales

- El Oficial de Tratamiento de Datos Personales debe garantizar que el funcionario haya hecho entrega de todos los activos asignados y que la Dirección de Sistemas y Tecnología haya realizado el retiro de roles en la plataforma institucional y/o cualquier otro sistema de información al cual tuviese acceso y que albergue información sensible de la institución o datos personales de los titulares de esta.

7.2.4 Normas dirigidas a todo el personal administrativo y docente de la Institución

- Los funcionarios administrativos y docentes que se desvinculen de la Universidad o realicen un cambio de labores o de cargo, deben hacer la respectiva entrega de los activos de la información a su jefe inmediato, haciendo uso del formato ESG-SSI-F010 – Checklist para entrega y devolución de activos de la información.

8. BIBLIOGRAFÍA Y WEB GRAFÍA

DEPARTAMENTO NACIONAL DE PLANEACIÓN, Consejo Nacional De Política Económica y Social República De Colombia, CONPES 3854 de 2016 [sitio web]. Bogotá D.C. [Consultado: 4 de agosto de 2022]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

HOSPITAL GENERAL DE MEDELLÍN. Manual de Seguridad de la Información. Disponibleen:https://www.hgm.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=203

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN. Guía N. 21 para la Gestión y Clasificación de Incidentes de Seguridad de la Información. Seguridad y Privacidad de la Información. [Sitio web] Bogotá D.C: MINTIC. [Consultado: 11 julio 2021] Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN. Guía N. 4 de Roles y Responsabilidades. Seguridad y Privacidad de la Información. [Sitio web] Bogotá D.C: MINTIC. [Consultado: 11 julio 2021] Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.Pdf

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de Seguridad y Privacidad de la Información. Seguridad y Privacidad de la Información. [Sitio web] Bogotá D.C: MINTIC. [Consultado: 11 julio 2021] Disponible en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150517_Modelo_de_Seguridad_Privacidad.pdf

UNIVERSIDAD DE CUNDINAMARCA. Manual de Sistemas y Tecnología. [sitio web]. Fusagasugá. [Consultado: 19 de septiembre de 2022]. Disponible en: https://plataforma.ucundinamarca.edu.co/aplicaciones/calidad/apl_gen_ini.jsp?id=10

CONTROL DE CAMBIOS				
VERSIÓN	FECHA DE APROBACIÓN			DESCRIPCIÓN DEL CAMBIO
	AAAA	MM	DD	
1	2021	02	23	Emisión del documento. Transición del ASIM010.
2	2021	06	10	Cambio de nombre de “Manual de roles y responsabilidades para la protección de datos personales” a “Manual de roles y responsabilidades en seguridad y privacidad de la información” e inclusión de roles y responsabilidades referentes al SGSI.
3	2022	09	21	Inclusión rol de vial de seguridad de la información, nuevas responsabilidades para el personal de la Universidad en todas las modalidades de contratación.
4	2022	11	28	Se anexa numeral 6.6 referente a los roles y responsabilidades del equipo de respuesta inmediata a incidentes de seguridad de la información. De igual incluye responsabilidades al rol de vigía de seguridad de la Información.
5	2023	05	29	Se ajusta el numeral 5.8 FUNCIONARIOS ADMINISTRATIVOS Y DOCENTES y se anexa numeral 5.9 referente a los roles y responsabilidades de los funcionarios del Centro Académico Deportivo – CAD.
6	2023	10	02	Se agregan responsabilidades de nivel directivo, respecto a la gestión de activos, gestión de autorizaciones y planes de mejoramiento del SGSI
7	2024	04	04	Se realiza la actualización de la normatividad legal vigente y se modifica la resolución 088 de 2017 por la 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”, además de incluir ítems del Oficial de Protección de Datos Personales. Se replantean los objetivos específicos de acuerdo con los lineamientos institucionales en seguridad y privacidad de la información a nivel institucional

ELABORÓ	
NOMBRES Y APELLIDOS	CARGO
Fabian Libardo Parra Gutiérrez	Técnico
REVISÓ	
NOMBRES Y APELLIDOS	CARGO

María del Pilar Delgado Rodríguez	Coordinadora del Sistema de Gestión de Seguridad de la Información - SGSI

APROBÓ (GESTOR RESPONSABLE DEL PROCESO)				
NOMBRES Y APELLIDOS	CARGO	FECHA		
		AAAA	MM	DD
María del Pilar Delgado Rodríguez	Coordinadora del Sistema de Gestión de Seguridad de la Información - SGSI	2024	04	04