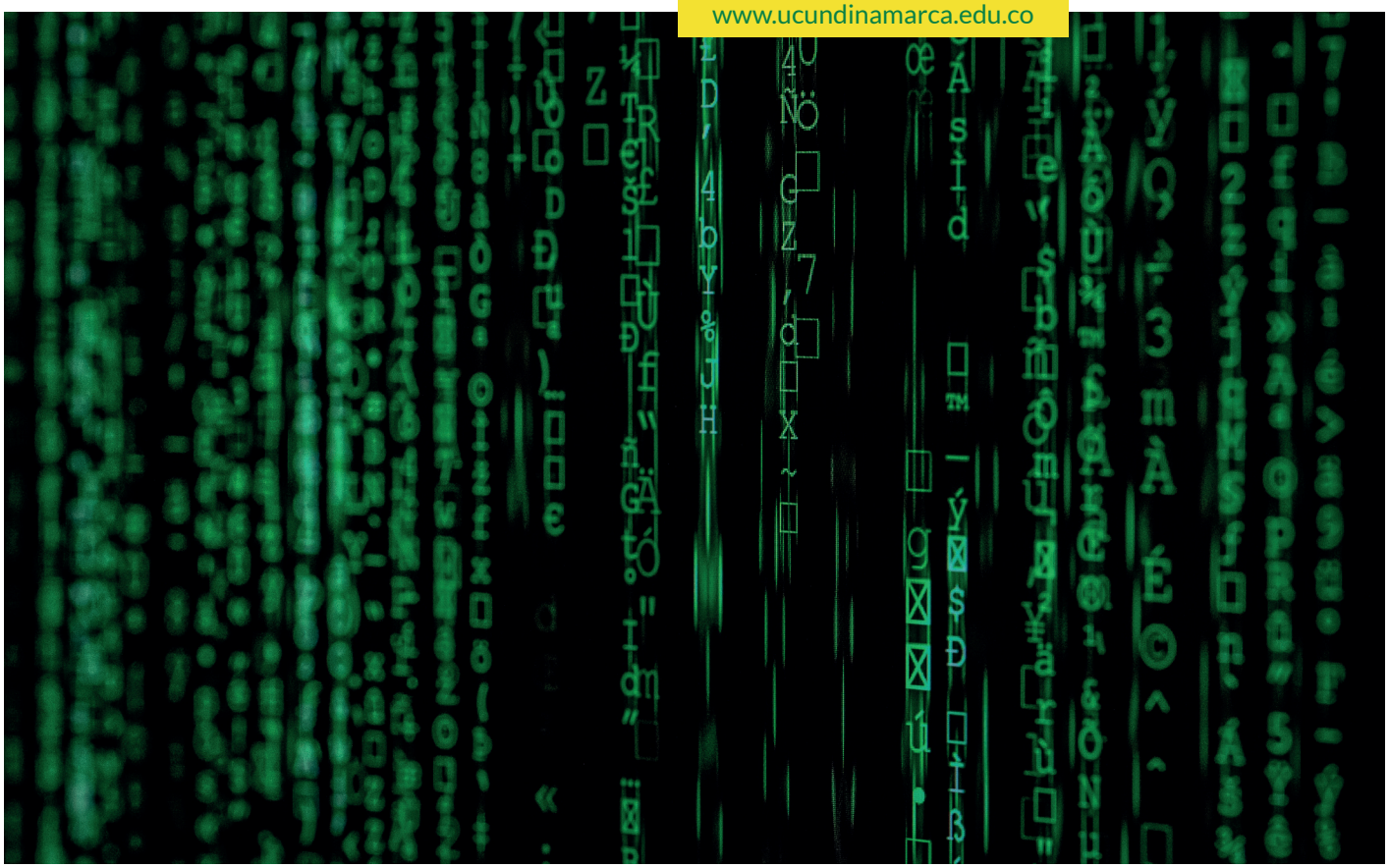
www.ucundinamarca.edu.co



Sensibilización en Seguridad y Privacidad de la Información

Sistema de Gestión Seguridad de la Información

SGSI

2022

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SGSI

UDEC UNIVERSIDAD DE CUNDINAMARCA

30 AÑOS

Rector
Adriano Muñoz Barrera

Secretaria General
Isabel Quintero Uribe

Vicerrector Académico
Víctor Hugo Londoño Aguirre

Vicerrectora Administrativa y Financiera
Myriam Lucía Sánchez Gutiérrez

Dirección de Sistemas y Tecnología
Daniel Andrés Rocha Ramírez

Sistema de Gestión de Seguridad de la Información - SGSI

Coordinación
María del Pilar Delgado Rodríguez
e-mail: sgsi@ucundinamarca.edu.co

2022

Equipo Táctico Operativo del SGSI

Ing. Daniel Andres Rocha Ramirez

Ingeniero de Sistemas,
Especialista en Gestión de Sistemas y Tecnologías de la Información para Empresas y Magister en Diseño y Gestión de Proyectos Tecnológicos

Ing. Maria del Pilar Delgado Rodriguez

Ingeniera de Sistemas,
Especialista en Ingeniería del Software, Auditora certificada en los Sistemas de Gestión de Calidad, Ambiental, Seguridad y Salud en el Trabajo, Seguridad de la Información y Protección de Datos Personales.

Ing. Jorge Luis Gaitan Baquero

Ingeniero Electrónico
Especialista en Seguridad Informática
Auditor interno ISO 27001:2013

Ing. Martin Alberto Garzon Guasca

Ingeniero Electrónico
Cursando II semestre de Esp. En Gerencia para el Desarrollo Organizacional

Ing. Lesly Daniela Reyes Perez

Ingeniera Electrónica
Cursando Especialización en Comercio Electrónico

Ing. Jhon Alexander Cristancho

Ingeniero Electrónico
Certificación ISO 27001- Lead EAD Implementer

Eimy Daniela Melo Rodriguez

Administradora de Empresas
Cursando II semestre de Esp. En Gerencia para el Desarrollo Organizacional

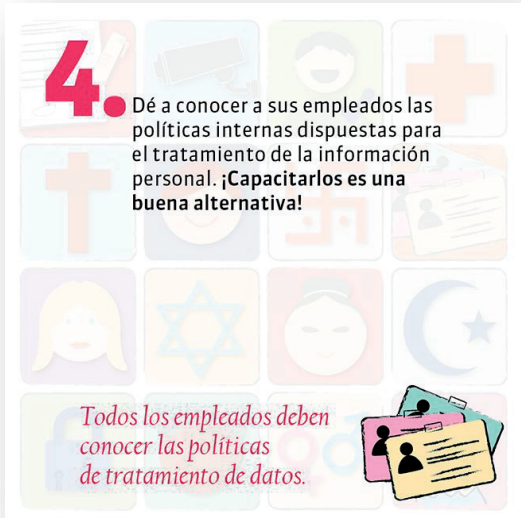
Ezequiel Morales Rivera

Tecnólogo en Análisis y Desarrollo de Sistemas de Información
Próximo a obtener el titulo de Ingeniero de Sistemas

ESG-SSI-PL01 - Plan de sensibilización y entrenamiento en seguridad y privacidad de la información

- ISO 27001:2013 numeral 7.3 – toma de conciencia
- Guía 14 ”plan de capacitación, sensibilización y comunicación de seguridad de la información” – mspi
- SIC- tip 4: todos los empleados deben conocer las políticas de tratamiento de datos

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	



JORNADAS DE SENSIBILIZACION EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACION
CIERRE 30 DE SEPTIEMBRE DE 2021
INDICADOR DE PARTICIPACION
Total de funcionarios que participaron en las jornadas de sensibilización del SGSI _____ Total de funcionarios de la Universidad de Cundinamarca **Resultado: 744/1308= 57%**

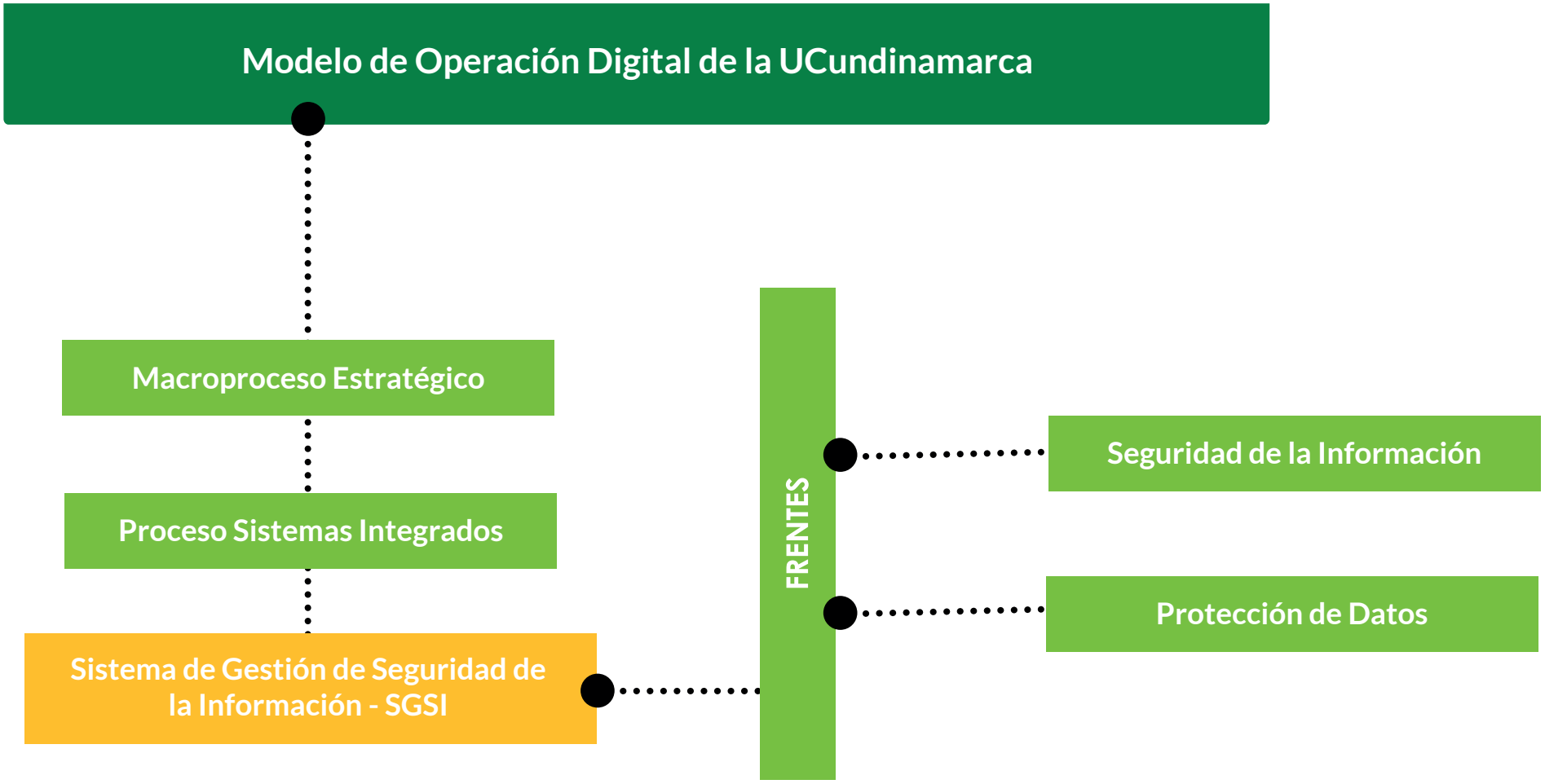

Modelo de Operación Digital de la UCundinamarca
Macroproceso Estratégico
Proceso Sistemas Integrados
Sistema de Gestión de Seguridad de la Información - SGSI
FRENTES
Seguridad de la Información
Protección de Datos

Tabla de contenidos

1

Matriz de identificación y seguimiento al cumplimiento de requisitos legales y otros del SGSI

Matriz de identificación y seguimiento al cumplimiento de requisitos legales y otros del SGSI

Constitución Política de Colombia 1991

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.

Congreso de la República

Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales" - 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." (Articulo 13,14) - Decreto 1377 de 2013 "Por el cual se reglamenta parcialmente la Ley 1581 de 2012."

Gobierno Nacional

Decreto 1074 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Comercio" (Capítulo 25 "Reglamenta parcialmente la Ley 1581 de 2012", (Capítulo 26 "Registro Nacional de Base de Datos") Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"(Titulo 9 "Políticas y lineamientos de tecnologías de la información") – Capítulo 1. Política de Gobierno Digital (Capítulo subrogado por el Art.1 del Decreto 767 de 2022).

Organización Internacional de Normalización Comisión Electrotécnica Internacional

Norma Técnica NTC-ISO IEC Colombiana 27001 de 2013 - Norma Técnica IEC NTC-ISO Colombiana de 2018

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)

Resolución 500 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital"

Consejo nacional de política económica y social república de colombia

CONPES 3854 DE 2016 –"Política Nacional de Seguridad Digital"

Macroproceso: Estratégico

Proceso: Gestión Sistemas Integrados

Sistema de Gestión de Seguridad de la Información- SGSI

Matriz de identificación y seguimiento al cumplimiento de requisitos legales y otros del sgsi

Resolución 088 de 2017 "Por la cual se adopta el Sistema de Seguridad de la Información – SGSI y se establece la Política, Objetivos y Alcance del Sistema de Seguridad de la Información de la Universidad de Cundinamarca".

Resolución 000050 de 2018 "Por la cual se establece la Política de Tratamiento de Datos de los Titulares de la Universidad de Cundinamarca".

Resolución 000058 de 2019 "Por la cual se modifica la Resolución N.º 000050 "Por la cual se establece la Política de Tratamiento de Datos de los Titulares de la Universidad de Cundinamarca" del 7 de mayo de 2018, en sus artículos 2° y 13°".

Resolución 027 de 2018 "Por la cual se establecen los roles y responsabilidades de los Sistemas de Gestión de la Universidad de Cundinamarca".

Resolución 026 de 2020, "Por la cual se modifica la resolución 156 del 1 de noviembre de 2017 "por la cual se crea el sistema de aseguramiento de la calidad de la Universidad de Cundinamarca SAC - Ucundinamarca"

Universidad de Cundinamarca

Macroproceso: Estratégico

Proceso: Gestión Sistemas Integrados
Sistema de Gestión de Seguridad de la Información- SGSI

2

Políticas Institucionales de Seguridad y Privacidad de la Información.

Implementación sistema gestión de seguridad de la información

La Universidad de Cundinamarca, comprende la importancia de proteger la confidencialidad, integridad y disponibilidad de la información como activo esencial para la prestación de sus servicios de formación y aprendizaje, ciencia, tecnología e innovación e interacción universitaria, por lo tanto es prioritario la implementación de un Sistema de Seguridad de la Información – SGSI, como herramienta que permita identificar, analizar, valorar y tratar los riesgos, manteniendo el mejoramiento continuo, acorde con las necesidades de los diferentes grupos de interés identificados.

La demás políticas que se generen como producto de la implementación del SGSI, serán adoptadas y de obligatorio cumplimiento por todos los grupos de interés.

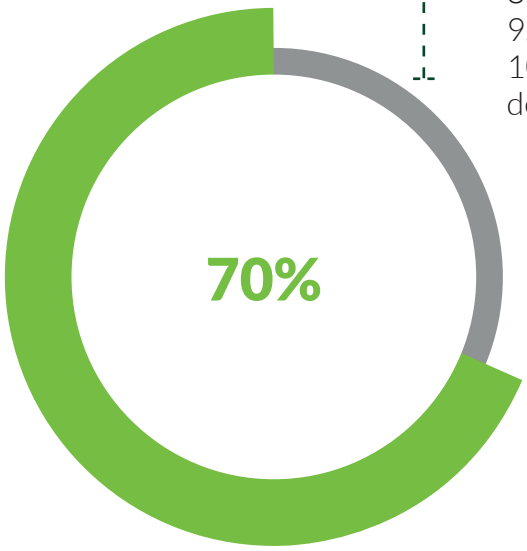
Seguridad de la información y tratamiento de datos personales

Políticas para la implementación de controles de seguridad de la información

Políticas

Realizado

1. Organización de la seguridad de la información
2. Gestión de activos
3. Privacidad y confidencialidad
4. Gestión de incidentes de seguridad de la información
5. Capacitación y sensibilización en seguridad de la información
6. Control de acceso
7. Registro y auditoría



En Proceso

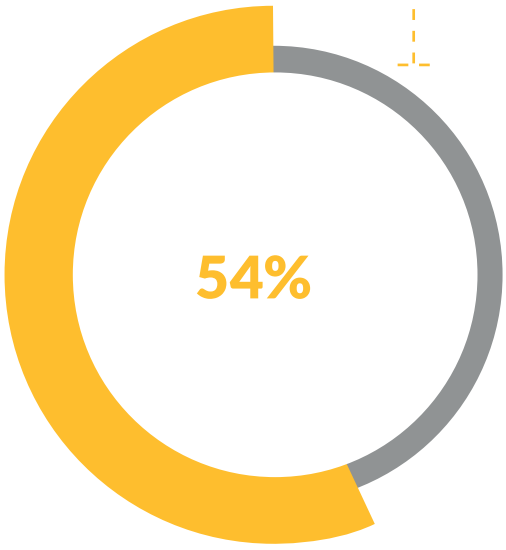
8. No repudio
9. Integridad
10. Disponibilidad del servicio e información

Procedimientos de seguridad de la información

Procedimientos

Realizado

1. Capacitación y sensibilización del personal
2. Identificación y clasificación de activos
3. Ingreso seguro a los sistemas de información
4. Gestión de usuarios y contraseñas
5. Mantenimiento de equipos
6. Gestión de cambios
7. Transferencia de información
8. Tratamiento de la seguridad en los acuerdos con los proveedores
9. Adquisición, desarrollo y mantenimiento
10. Control de software
11. Gestión de incidentes de seguridad de la información
12. Ingreso y desvinculación del personal



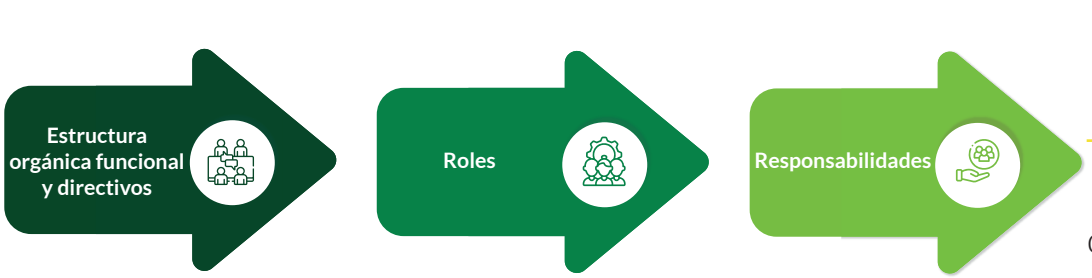
En Proceso

13. Control de acceso físico
14. Controles criptográficos
15. Gestión de llaves criptográficas
16. Protección de activos
17. Retiro de activos
18. Gestión de capacidad
19. Separación de ambientes
20. Protección contra códigos maliciosos
21. Aseguramiento de servicios en la red
22. Gestión de continuidad del negocio

3

Roles y responsabilidades en el Modelo de Seguridad y Privacidad de la Información

ESG-SSI-M004 V2
Manual de roles y responsabilidades en seguridad y privacidad de la información



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.

- Asegurar los mecanismos idóneos para reportar los incidentes de seguridad que se presenten con sus bases de datos.

- Revisar periódicamente las diferentes políticas o propuestas realizadas por el SGSI, aprobándolas o comunicando los ajustes a los que haya lugar. Promover las medidas administrativas suficientes para lograr el cumplimiento de los objetivos del SGSI, por parte de todos los funcionarios de la institución.

Oficial de tratamiento 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.

- 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.

- Reportar las actualizaciones y novedades de reclamos e incidentes de seguridad sobre las bases de datos de la universidad en la plataforma del Registro Nacional de Bases de Datos – RNBD.

- Aprobar las modificaciones que se realicen a los procedimientos internos, relacionados con la protección de datos personales.

- Revisar de forma periódica y socializar internamente la Política de Protección de Datos Personales.

Responsable de seguridad de la información: director de sistemas y tecnologia

- 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.

Alta dirección, directores y jefes de área, decanos y directores de programa

- Impulsar los funcionarios administrativos, docentes y estudiantes de la sede, seccionales, extensiones y oficina de Bogotá, las diferentes políticas, procedimientos, manuales, guías e instructivos derivados del Sistema de Gestión de Seguridad de la Información.

- Incentivar el adecuado uso del correo electrónico institucional para envío y recepción de información entre funcionarios, así como para el contacto con entidades externas a nombre de la Universidad.

- Velar por la adopción y cumplimiento del Manual de Roles y Responsabilidades entre los funcionarios administrativos de la Institución, sin importar su tipo 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.

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 Seguridad de la Información a los órganos directivos pertinentes en la Universidad.

Equipo táctico – operativo del SGSI

- Apoyar el Sistema 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.

- 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.

Funcionarios administrativos y docentes

- Reportar cualquier irregularidad que se llegaré a presentar con cada una de las bases de datos de la Universidad al Oficial de Tratamiento de Datos Personales.

- Abstenerse de compartir la información con terceros no autorizados, dando así cumplimiento al deber de confidencialidad.

- Prestar la ayuda requerida dentro de las investigaciones que llegare a realizar el Oficial de Tratamiento de Datos y/u Oficial de Seguridad de la Información, para determinar la responsabilidad en caso de incumplimiento a los protocolos de seguridad en el manejo de las bases de datos.

- Asistir y participar de las capacitaciones organizadas por el Oficial de Tratamiento de Datos Personales y/u Oficial de Seguridad de la Información, para lograr el cabal cumplimiento de las disposiciones establecidas dentro del PIGDP y el SGSI.

- Cumplir las disposiciones definidas en la Política de Protección de Datos Personales, el **Manual ESG-SSI-M001 MANUAL DE POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION** y cualquier documento que las desarrolle o complemente.

Vigias de seguridad de la informacion

- 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 27001 y conocer la normatividad a nivel nacional en Seguridad y privacidad de la Información, de igual forma la normatividad interna.

- 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, deberán realizar 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, como son las jornadas de sensibilización y entrenamiento, el aula virtual del SGSI, la campaña de protección de datos, el correo del sgsi@ucundinamarca.edu.co
- y el correo de alertas@ucundinamarca.edu.co.

- 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, 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 y fortalezas encontradas y que son buenas o malas prácticas por parte de los funcionarios y que son eventos que se pueden convertir en posibles riesgos.

4

Resultados de la Auditoria Interna I del SGSI

Plan de mejoramiento de la auditoria interna I del SGSI

Reunión cierre Auditoría Interna I y entrega informe final

01 dc abril dcl 2022

SCIR010 - informe de auditoría

Total de Hallazgos
213

Acompañamiento en Planes de Mejoramiento
18 dc abril a 2 mayo dcl 2022

27

Decisión

Hallazgos Transversales

3

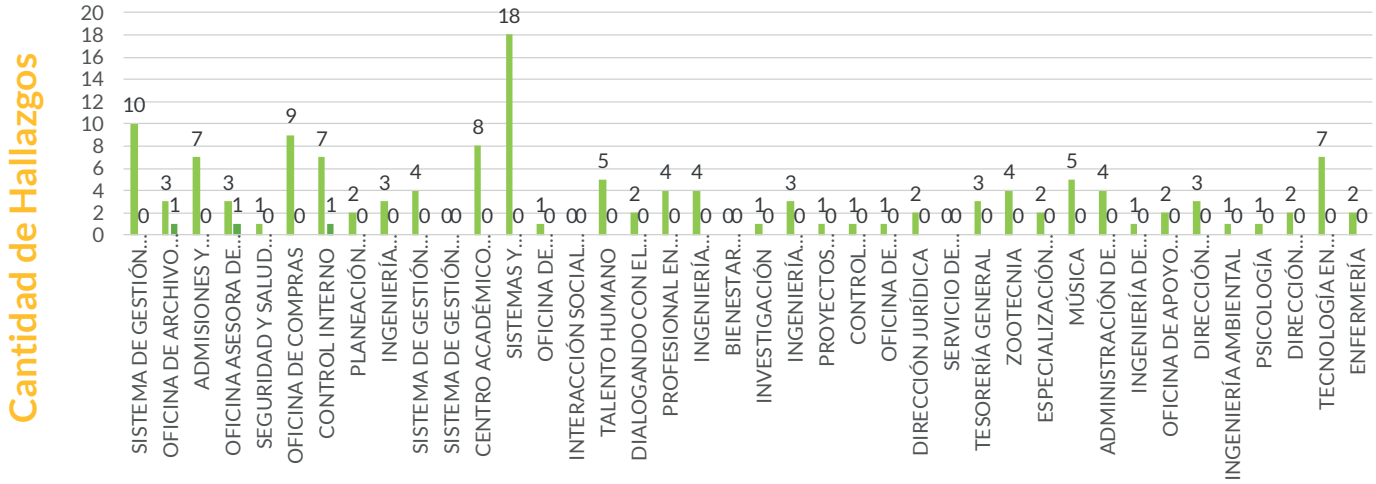
Consolidación de informe de auditoría i - SGSI

Hallazgos transversales

No.	Descripción del Hallazgo	Responsable
1.	Lo activos de información se realiza de manera inadecuada, el concepto de activos de información es confundido con inventario de activos, evidenciando activos fijos como “sillas de ruedas”, “basurero” entre otros, adicionalmente la clasificación de activos de estos activos no es claro el concepto dando la clasificación de manera inadecuada a los activos.	SGSI
2.	Los riesgos de seguridad de la información, se maneja de manera genérica por tipo de activos, el cual no se logra evidenciar que riesgos se está asociando a un activo especifico en caso de materializarse un riesgo, adicionalmente la matriz no cuenta con riesgo residual dando un inadecuado manejo a los riesgos del SGSI.	SGSI
3.	Se evidencia en todas las áreas el incumplimiento de política pantalla y escritorio limpio, se evidencia archivos sensibles, notas con correos y contraseñas sensibles, papeles en el escritorio e impresoras con información y la papelera del escritorio llena	SGSI

Plan de mejoramiento de la auditoria interna i del SGSI

resultados generales de auditoria interna i sgsi



No conformidad	137
Observaciones	3

No conformidad
Observaciones

Total de hallazgos 140

Tratamiento no conformidades transversales

Acciones de mejora y preventivas
Desarrollo del plan de tratamiento de riesgos de seguridad y privacidad

Acciones de mejora y preventivas
Modificación curso del aula virtual SGSI 2

Acciones de mejora y preventivas

- Modificación al procedimiento EGS-SSI-P01
- Ajusta al aplicativo "Gestión de activos"
- Actualización del instructivo ESG-SSI-I001
- Actualización de la guía ESG-SSI-G001

5

Etapas del Modelo de Gestión de Seguridad de la Información

Modelo de gestión integral de seguridad de la información

Norma ➡ Norma Internacional ISO/IEC 27001

¿Qué es? ➡ Es el conjunto de gestiones alineado de manera coherente con los objetivos de la institución, permiten el avanzar en el nivel de madurez del Sistema de Gestión de Seguridad de la Información.

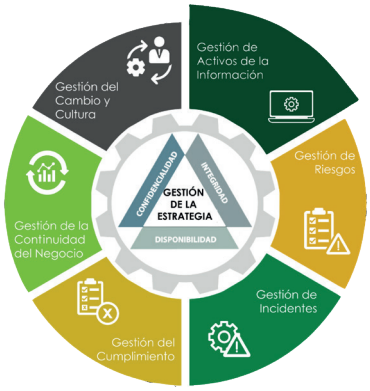
¿Cómo se desarrolla? ➡ Para cada una de las gestiones se presenta su definición, la relación con cada una de las etapas del ciclo de mejora continua PHVA (Planear, Hacer, Verificar, Actuar) y la relaciones y dependencias que existen entre cada una de estas.

Modelo de Gestión Integral de Seguridad de la Información

El SGSI opera a través de 6 etapas que agrupadas engranan la gestión de la estrategia.

Etapa 1 : Gestión de Activos de la 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.



Activo de información

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 auditoria, entre otros.

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.

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.

Software

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

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

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)

Principios para resguardar los activos de información

La información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

Propiedad de salvaguardar la exactitud y estado completo de los activos.

Propiedad de mantener un activo de información accesible y utilizable por solicitud de un individuo, entidad o proceso autorizado

ESG-SSI-P01 - gestión de activos de la información

El procedimiento de gestión de activos establece y socializa los lineamientos pertinentes, en cumplimiento de la normatividad legal vigente, para el registro de activos de la información por parte de los responsables identificados por la institución, permitiendo la identificación, clasificación y valoración de los activos de información de la Universidad de Cundinamarca…

Entrenamiento en gestión de activos

Cronograma Sesiones de entrenamiento para la gestión de activos			
Fecha	**No. Sesión**	**Jornada**	**Procesos que integran el macroproceso**
13/09/22	1	Jornada mañana **9:00am - 10:30am**	Misional
	2	Jornada tarde **4:00pm - 5:30 pm**	
15/09/22	3	Jornada mañana **9:00am - 10:30am**	Estratégico
	4	Jornada tarde **3:00pm - 4:30 pm**	
16/09/22	5	Jornada mañana **9:00am - 10:30am**	Apoyo
	6	Jornada tarde **3:00pm - 4:30 pm**	
20/09/22	7	Jornada mañana **9:00am - 10:30am**	Seguimiento, medición, análisis y evaluación
	8	Jornada tarde **4:00pm - 5:30 pm**	
22/09/22	9	Jornada mañana **9:00am - 10:30am**	Unificado
	10	Jornada tarde **3:00pm - 4:30 pm**	
Lugar: Sala de formación de usuarios M-204 CGCA, Fusagasugá			

Etapa 2 : Gestión de Riesgos

Para la identificación, valoración y tratamiento de riesgos, la Universidad de Cundinamarca tiene presente los lineamientos dispuestos tanto a nivel internacional con la Norma ISO 27001:2013, como a nivel nacional, siguiendo las directrices emanadas del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC como del Departamento Administrativo de la función pública - DAFP.

Etapa 3 : Gestión de Incidentes

En esta etapa, para realizar una correcta gestión de los incidentes de seguridad de la información, es necesario identificar y clasificar los diferentes eventos e incidentes que puedan presentarse en la Institución, relacionados a seguridad de la información y privacidad de los datos personales.

Etapa 4 : Gestión del Cumplimiento

La Universidad de Cundinamarca establece el respectivo Programa Integral de Gestión de Datos Personales – PGIDP, Plan de Sensibilización y Entrenamiento en Seguridad y Privacidad de la Información, los procedimientos reglamentarios y demás normatividad legal vigente en materia de protección de datos personales.

Modelo de gestión integral de seguridad de la información

Ninguna empresa puede usar los datos personales de sus clientes sin autorización. Ahora hay **SANCIONES.**

CONSTITUCION POLITICA DE 1991

Articulo 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.

Articulo 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 ESTATUTARIA 1581 DE 2012

Artículo 9°. 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 NACIONAL 1377 DE 2013

CAPÍTULO II
Autorización
Artículo 4°. Recolección de los datos personales.
Artículo 5°. Autorización.

DECRETO UNICO 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".
Inhabilidades por delitos sexuales cometidos contra menores: Las personas que hayan sido condenados por la comisión de delitos contra la libertad, integridad y formación sexuales de persona menor de 18 años de acuerdo con el Título IV de la presente ley; serán inhabilitadas para el desempeño de cargos, oficios o profesiones que involucren una relación directa y habitual con menores de edad en los términos que establezca el Instituto Colombiano de Bienestar Familiar, o quien haga sus veces.

Resolución 000013 de 2021 DIAN

"Por la cual se implementa y desarrolla en el sistema de facturación electrónica lafuncionalidad del documento soporte de pago de nómina electrónica y se adopta el anexo técnico para este documento".
Artículo 31 Transferencia de datos personales.
Articulo 32. Obligaciones del responsable de la información
Artículo 33. Disposición final de los datos personales.
Artículo 34. Responsabilidad.
Artículo 35. Confidencialidad y reserva de la información.

Ley estatutaria 1581 de 2012 excepciones

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

1. Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;
2. Datos de naturaleza pública;
3. Casos de urgencia médica o sanitaria;
4. Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;
5. Datos relacionados con el Registro Civil de las Personas.

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

Ley estatutaria 1581 de 2012 excepciones

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

1. **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.
2. **Suspensión de las actividades relacionadas** con el Tratamiento hasta por un término de seis (6) meses.
3. **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;
4. **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.

El objetivo de la SIC es incluir bajo los mismos lineamientos a personas naturales y a las entidades de naturaleza pública, pues la Ley de Protección de Datos no le permite a esta entidad sancionar a las empresas estatales

Resolucion 462 del 26 de abril de 2019

"Adelantar en primera instancia las actuaciones disciplinarias que correspondan por conductas relacionadas en el incumplimiento de las obligaciones contenidas en la Ley 1581 de 2012 y demás disposiciones que la desarrollen, modifiquen y reglamenten a cargo de los sujetos vinculados con las autoridades públicas…"

Normatividad interna protección de datos personales

RESOLUCIÓN 000050 DE 2018

"Por la cual se establece la Política de Tratamiento de Datos de los Titulares de la Universidad de Cundinamarca".

ARTÍCULO 8° — AUTORIZACION Y CONSENTIMIENTO DEL TITULAR

RESOLUCIÓN 000058 DE 2019

"Por la cual se modifica la Resolución N.º 000050 "Por la cual se establece la Política de Tratamiento de Datos de los Titulares de la Universidad de Cundinamarca" del 7 de mayo de 2018, en sus artículos 2° y 13°"

Entidad regulatoria remitida por la SIC: Procuraduría General de Nación

RESOLUCIÓN 000050 DE 2018

“Por la cual se establece la Política de Tratamiento de Datos de los Titulares de la Universidad de Cundinamarca”.

Artículo décimo. - deberes de la universidad de cundinamarca como responsable y encargada de los datos personales

La Universidad de Cundinamarca, reconoce la titularidad de los datos personales que ostentan las personas y en consecuencia ellas de manera exclusiva pueden decidir sobre los mismos.

Son deberes de La Universidad de Cundinamarca, en calidad de responsable del tratamiento de datos personales los siguientes:

1. Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

2. Solicitar y conservar, copia de la respectiva autorización otorgada por el titular para el tratamiento de datos personales.

3. Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten en virtud de la autorización otorgada.

4. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
5. Garantizar que la información sea veraz, completa, exacta, actualizada, comprobable y comprensible.

6. Actualizar oportunamente la información, atendiendo de esta forma todas las novedades respecto de los datos del titular. Adicionalmente, se deberán implementar todas las medidas necesarias para que la información se mantenga actualizada.

7. Rectificar la información cuando sea incorrecta y comunicar lo pertinente.

8. Tramitar las consultas y reclamos formulados en los términos señalados por la ley.

9. Identificar cuando determinada información se encuentra en discusión por parte del titular.

10. Informar a solicitud del titular sobre el uso dado a sus datos.

11. Cumplir los requerimientos e instrucciones que imparta la Superintendencia de Industria y Comercio sobre el tema en particular.

12. Velar por el uso adecuado de los datos personales de los niños, niñas y adolescentes, en aquellos casos en que se entra autorizado el tratamiento de sus datos.

13. Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio

14. Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.

15. Usar los datos personales del titular sólo para aquellas finalidades para las que se encuentre facultada debidamente y respetando en todo caso la normatividad vigente sobre protección de datos personales

Datos personales

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

Clasificación de los datos personales

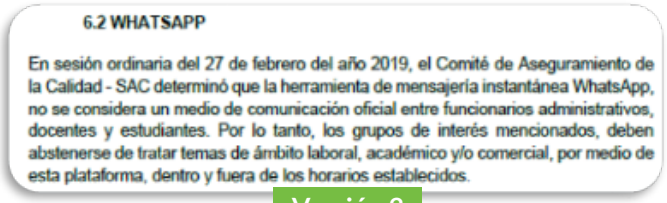
Tipo de dato	Definición	Ejemplos	Nivel de seguridad requerido
Públicos	Es el dato que la ley o la Constitución Política determina como tal, así como todos aquellos que no sean semiprivados o privados.	Número de cédula Nombres y apellidos Correo electrónico corporativo Domicilio de trabajo	**Básico**
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 financieros Afiliaciones a seguridad social Teléfono personal Correo personal Domicilio	**Medio**
Privados	Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular de la información.	Comunicaciones personales Contraseñas **Solo por orden judicial**	**Medio - Alto**
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)	Orientación sexual, filosófica, política y religiosa; Datos de salud Datos biométricos	**Alto**

Respuesta del concepto jurídico del uso del Whatsapp, teletrabajo

ESG-SSI-M003 -Manual de Directrices para Contacto por Mensajería Instantánea

Concepto Jurídico sobre uso WhatsApp desde la Dirección Jurídica

25 dc fcbrcro dcl 2022



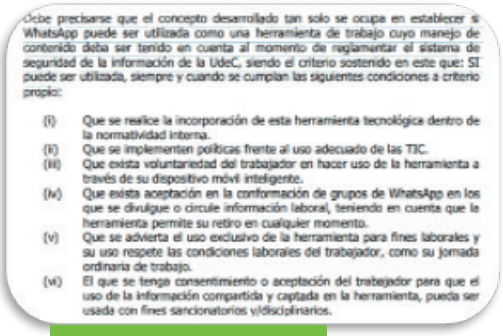
6.2 WHATSAPP

En sesión ordinaria del 27 de febrero del año 2019, el Comité de Aseguramiento de la Calidad - SAC determinó que la herramienta de mensajería instantánea WhatsApp, no se considera un medio de comunicación oficial entre funcionarios administrativos, docentes y estudiantes. Por lo tanto, los grupos de interés mencionados, deben abstenerse de tratar temas de ámbito laboral, académico y/o comercial, por medio de esta plataforma, dentro y fuera de los horarios establecidos.

Versión 3

6.2 WHATSAPP

A.13.2 Transferencia de información
A.13.2.3 Mensajería electrónica: Control; Se debe proteger adecuadamente la información incluida en la mensajería electrónica.



Debe precisarse que el concepto desarrollado tan solo se ocupa en establecer si WhatsApp puede ser utilizada como una herramienta de trabajo cuyo manejo de contenido deba ser tenido en cuenta al momento de reglamentar el sistema de seguridad de la información de la UdeC, siendo el criterio sostenido en este que: SI puede ser utilizada, siempre y cuando se cumplan las siguientes condiciones a criterio propio:

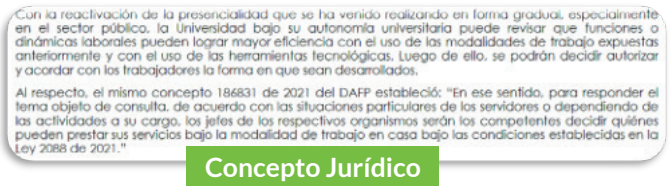
(i) Que se realice la incorporación de esta herramienta tecnológica dentro de la normatividad interna.
(ii) Que se implementen políticas frente al uso adecuado de las TIC.
(iii) Que exista voluntariedad del trabajador en hacer uso de la herramienta a través de su dispositivo móvil inteligente.
(iv) Que exista aceptación en la conformación de grupos de WhatsApp en los que se divulgue o circule información laboral, teniendo en cuenta que la herramienta permite su retiro en cualquier momento.
(v) Que se advierta el uso exclusivo de la herramienta para fines laborales y su uso respete las condiciones laborales del trabajador, como su jornada ordinaria de trabajo.
(vi) El que se tenga consentimiento o aceptación del trabajador para que el uso de la información compartida y captada en la herramienta, pueda ser usada con fines sancionatorios y/disciplinarios.

Propuesta Versión 4

Concepto técnico referente a la modalidad de contratación en teletrabajo

Concepto Jurídico sobre Teletrabajo desde la Dirección Jurídica

25 dc marzo dcl 2022



Con la reactivación de la presencialidad que se ha venido realizando en forma gradual, especialmente en el sector público, la Universidad bajo su autonomía universitaria puede revisar que funciones o dinámicas laborales pueden lograr mayor eficiencia con el uso de las modalidades de trabajo expuestas anteriormente y con el uso de las herramientas tecnológicas. Luego de ello, se podrán decidir autorizar y acordar con los trabajadores la forma en que sean desarrollados.

Al respecto, el mismo concepto 186831 de 2021 del DAFP estableció: "En ese sentido, para responder el tema objeto de consulta, de acuerdo con las situaciones particulares de los servidores o dependiendo de las actividades a su cargo, los jefes de los respectivos organismos serán los competentes decidir quiénes pueden prestar sus servicios bajo la modalidad de trabajo en casa bajo las condiciones establecidas en la Ley 2088 de 2021."

Concepto Jurídico

13 de mayo del 2022

Sistema de Gestión de Seguridad de la Información
Para: Luz Etelvina Lozano Soto y 1 usuarios más
CC: DIRECCIÓN DE SISTEMAS Y TECNOLOGIA y 1 usuarios más
Cco: MARIA DEL PILAR DELGADO RODRIGUEZ y 2 más

13.1

Fusagasugá, 2022-05-13

Doctora
LUZ ETELVINA LOZANO SOTO
Directora Talento Humano
Ciudad

Asunto: Solicitud de concepto técnico referente a la modalidad de contratación en teletrabajo

Respetada doctora Lozano:

Comedidamente, el Sistema de Gestión de Seguridad de la Información – SGSI, dando cumplimiento a la implementación del SGSI, referente a la norma NTC-ISO/IEC 27001 en su anexo A.6 Organización de la seguridad de la información

A.6.2 Dispositivos móviles y teletrabajo
A.6.2.2 Teletrabajo: Control; Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en os que se realiza teletrabajo

Procedimientos de gestión de datos personales

- ESG-SSI-PL01 - Plan institucional de sensibilización y entrenamiento en seguridad y privacidad de la información
- ESG-SSI-PG01 - Programa integral de gestión de datos personales - pigdp
  - ESG-SSI-P03 – Recolección y almacenamiento de datos personales
  - ESG-SSI-P05 - uso y circulación de datos personales
  - ESG-SSI-P06 - Supresión de datos personales
  - ESG-SSI-P07 - Transferencia internacional de datos personales
  - ESG-SSI-P13 - Registro nacional de bases de datos

Etapa 5 : Gestión de la Continuidad del Negocio

En esta etapa que actualmente se encuentra en desarrollo, se pretende establecer un plan de continuidad de negocio en caso de materializarse un incidente de seguridad de la información, que impida continuar con las operaciones y funciones misionales de la Institución.

Etapa 6 : Gestión del Cambio y la Cultura

La etapa 6, se desarrolla de forma constante y busca crear un compromiso, conciencia y responsabilidad de toda la comunidad universitaria, respecto a la implementación del Sistema de Gestión de Seguridad de la Información - SGSI y el Programa Integral de Gestión de Datos Personales – PIGDP, armonizando el rol que cada grupo de interés tiene dentro de estos.

Principios básicos de la protección de datos

Es fundamental que la persona esté informada claramente y sepa cómo se tratará su información, así como quién lo hará.

Principio de legalidad en materia de Tratamiento de Datos

El tratamiento de datos es una actividad reglada, la cual deberá estar sujeta a las disposiciones legales vigentes.

Principio de libertad

El tratamiento de los datos personales sólo puede realizarse con el consentimiento, previo, expreso e informado del Titular.

Principio de trasparencia

La Universidad de Cundinamarca garantizará al Titular su derecho de obtener en cualquier momento y sin restricciones, información o dato personal que sea de su interés.

Principio de finalidad

Deberá ser informada al respectivo titular de los datos personales.

Principio veracidad o calidad

La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.

Principio de acceso y circulación restringida

El tratamiento de datos personales esta sujeta a los límites que se derivan de la naturaleza de éstos, de las disposiciones de la ley y la Constitución.

Principio de seguridad

La información sujeta a tratamiento por La Universidad de Cundinamarca se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Principio de confidencialidad

Todas las personas que en La Universidad de Cundinamarca, obligadas a garantizar la reserva de la información, por lo que se comprometen a conservar y mantener de manera estrictamente confidencial y no revelar a terceros.

Buenas prácticas en seguridad y la protección de datos

Buenas prácticas en seguridad

Realizar copias de seguridad con regularidad

ASIP25
Copia de seguridad
de la informacion

ASIM008
manual para realizar proceso,
seguimiento y recuperación
de backups

Aseguramiento de los sistemas

- **Sistema con contraseñas seguras.**
  1. Incluir números, letras mayúsculas y minúsculas
  2. Basadas en una frase u oración (Mmeuhct5mysneP)
  3. Gestor de contraseñas
- **Sistema con contraseñas seguras.**
- **Bloqueo de sesión y salida segura.**

- **Creación de usuarios con accesos restringidos.**
  1. Sesión de aplicaciones por tipo de usuario
  2. Deshabilitar las carpetas compartidas al público.

Mantener actualizado el sistema operativo y las aplicaciones

ASII014
instructivo para el soporte,
mantenimiento y monitoreo
a la infraestructura de red y
recursos tecnologicos

- Solucionar errores
- Corregir fallas
- Solucionar vulnerabilidades
- Incluir nuevas funciones

Precaución con los archivos desconocidos

- Acceder únicamente a sitios de confianza.
- Impedir la ejecución de archivos desde sitios web sin verificar previamente.
- Revisar el dominio de la dirección que envía el mensaje y verifica que coincida con el corporativo.

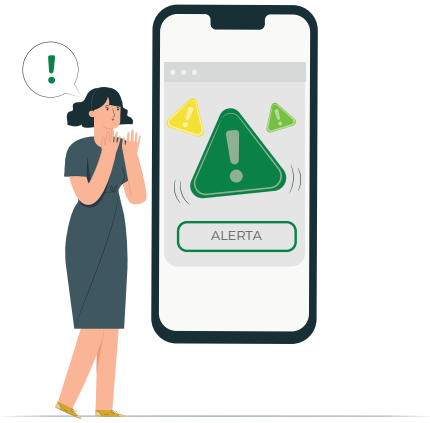
VIRUSTOTAL

- Sitio web que proporciona de forma gratuita el análisis de archivos y páginas web a través de antivirus.

Ataques informáticos

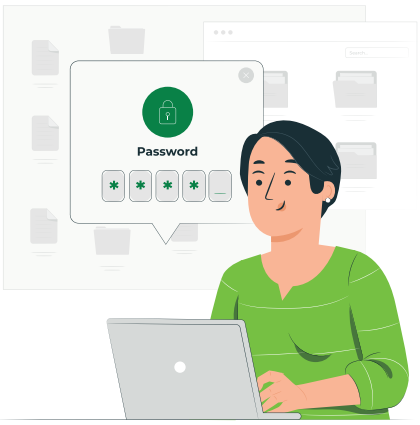
Los ataques informáticos son formas de vulnerar las tres propiedades de la seguridad de la información las cuales son la disponibilidad, integridad y confidencialidad mediante la explotación de vulnerabilidades conocidas en los sistemas informáticos.

Tipos de ataques informáticos



Ingeniería Social

Ataque mediante técnicas de persuasión psicológica que tiene como objetivo engañar a los usuarios de cualquier índole para que estos compartan información personal, todo mediante diferentes métodos como una llamada telefónica un correo electrónico entre otros

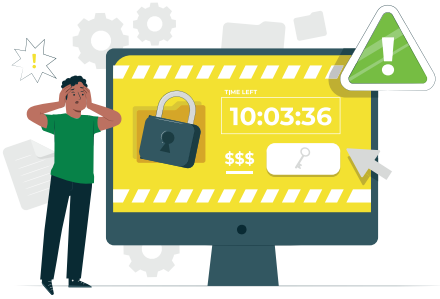


Ataque de fuerza bruta

Este es un ataque que consiste en emplear una seria de combinaciones conocidas para descifrar contraseñas con el objetivo de hacerse con información personal. Por lo general el atacante usa una serie de diccionarios con contraseñas conocidas.

Phishing y spear phishing

Es una técnica que consiste en envió de correos electrónicos o mensajesdetexto,conelpropósito de convencer al destinatario de abrir un enlace malicioso para el robo de información personal y/o de la organización.



Malware

Programa malicioso que afecta a dispositivos electrónicos de forma secreta con la finalidad invadir, dañar y/o deshabilitar ordenadores, sistemas informáticos entro otros. Los mas comunes troyanos y spyware.

Ransomware

Programa malicioso que afecta a dispositivos electrónicos con la finalidad de secuestrar datos almacenados en estos mediante bloqueo del equipo, en esta modalidad de ataque el atacante solicita un pago para liberar información, estos pagos por lo general son en Bitcoin.

Man in the middle (Ataque de intermediario)

Técnica donde el atacante busca crear una conexión intermedia entre el usuario y algún aplicativo web, con el propósito de capturar el trafico que sale de alguna consulta del usuario hacia la internet.

Formas de prevención

Definir las áreas y/o grupos especializados en utilizar las herramientas mas eficaces a la hora de contener y mitigar los ataques informáticos que se presenten en la infraestructura TI, como también establecer las estrategias mas pertinentes para capacitación a usuarios.

Por lo general los ciberataques siempre ocurren en los usuarios menos capacitados de la organización, es por esto que se resalta la importancia de que estos entiendan el valor del buen uso de los activos de información.

Usar software que este aprobado por la organización, sin embargo la Universidad de Cundinamarca restringe la instalación mediante parámetros establecidos por el área encargada.

Tener mucho cuidado con los correos electrónicos que se reciben, se debe verificar dominios, nombres entre otros parámetros.

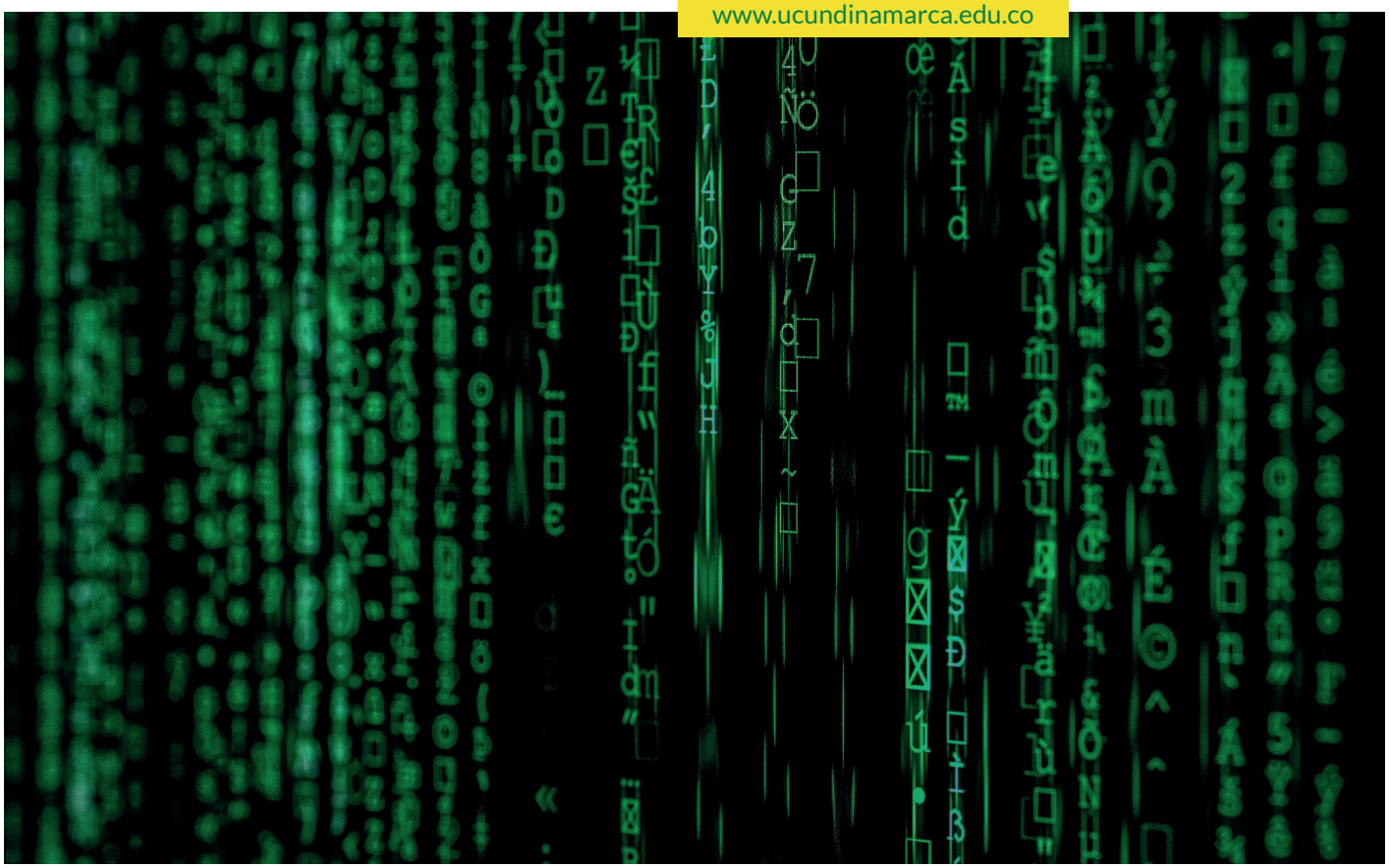
Evitar dar clic a cualquier enlace desconocido que lo lleve a descargar archivos.

No inserción de dispositivos de almacenamiento que no sean de confianza.

Tener cuidado de dar nuestros datos personales en redes publicas

Cambiar la contraseña que usamos en nuestras cuentas personales y/o en aplicativos de la organización, por lo menos una vez al mes y que esta no contenga los combinaciones como fechas, nombres o combinaciones conocidas.

www.ucundinamarca.edu.co



Dirección de Sistemas y Tecnología

Sistema de Gestión de Seguridad de la Información - SGSI

e-mail: sgsi@ucundinamarca.edu.co
Diagonal 18 N° 20-29
Línea gratuita 01 800 180 414
Línea fija (+57 1) 8281483
e-mail: info@ucundinamarca.edu.co

SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SGSI

UDEC UNIVERSIDAD DE CUNDINAMARCA

30 AÑOS