



UDEC
UNIVERSIDAD DE
CUNDINAMARCA

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



2021

WWW.UCUNDINAMARCA.COM | AGOSTO 2021

Vigilada MinEducación



UDEC
UNIVERSIDAD DE
CUNDINAMARCA

Rector

Adriano Muñoz Barrera

Secretaria General

Isabel Quintero Uribe

Vicerrectora Académica

María Eulalia Buenahora Ochoa

Vicerrectora Administrativa y Financiera

Myriam Lucía Sánchez Gutiérrez

Dirección de Sistemas y Tecnología

Edilson Martínez Clavijo

Sistema de Gestión de Seguridad de la Información

Coordinación María del Pilar Delgado Rodríguez

e-mail: sgsi@ucundinamarca.edu.co

2021

TABLA DE CONTENIDO

Pág.

04

Identificación del Sistema de Gestión de Seguridad de la Información.

Pág.

07

Matriz de Identificación y Seguimiento al Cumplimiento de Requisitos Legales y otros del SGSI

Pág.

09

Políticas institucionales de Seguridad y Privacidad de la Información.

Pág.

11

Roles y Responsabilidades en el Modelo de Seguridad y Privacidad de la Información.

Pág.


15

Etapas del Modelo de Gestión de Seguridad de la Información.

Pág.

24

Registro Nacional de Base de Datos – RNBD.

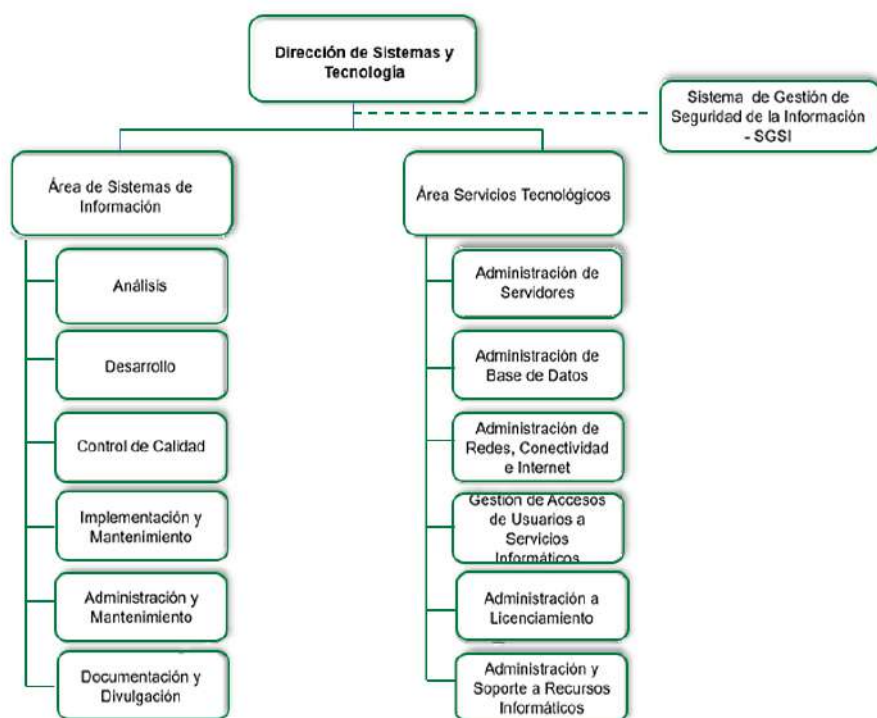


IDENTIFICACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

Sistema de Gestión de Seguridad de la Información - SGSI

El Sistema de Gestión de Seguridad de la Información – SGSI busca diseñar, implementar y mantener a través del ciclo Deming, las políticas, lineamientos y demás, que gestionen de forma eficiente la información, asegurando los principios de confidencialidad, integridad y disponibilidad, buscando minimizar la materialización de los riesgos e incidentes de seguridad de la información.

Estructura Interna de la Dirección de Sistemas y Tecnología



Fuente: Dirección de Sistemas y Tecnología

La Dirección de Sistemas y Tecnología, liderada por el ingeniero Edilson Martínez Clavijo pertenece al Macroproceso de Apoyo – Proceso Gestión Sistemas y Tecnología, está compuesta por dos áreas asociadas de forma directa, Área de Sistemas de Información, encargada del desarrollo, implementación y mantenimiento de aplicativos propios y Área de Servicios Tecnológicos, encargada de administrar la infraestructura tecnológica de la Institución, servidores, soporte y mantenimiento de equipos, entre otros. Y asociado de forma transversal, se encuentra **el Sistema de Gestión de Seguridad de la Información – SGSI**, que, por decisión de la Comisión de Gestión y Revisión por la Dirección de la vigencia 2020, pasó a formar parte del Macroproceso Estratégico – Proceso Gestión Sistemas Integrados.

Ciclo Deming: Este ciclo es un instrumento que se enfoca en la solución de problemas y el mejoramiento continuo, por medio de un diagnóstico inicial, se identifican las fallas para mejorar comparando los planes con los resultados, luego se analiza el resultado no deseado se replantea un nuevo diseño de medidas que anulen el problema y no vuelva a repetirse y conseguir un resultado aceptable. (Tomado de "El modelo Deming (PHVA) como estrategia competitiva para realzar el potencial administrativo. Castillo Pineda, Lady. Universidad Militar Nueva Granada)

Modelo Integrado de Planeación y Gestión - MIPG

MIPG opera a través de 7 dimensiones que agrupan las políticas de gestión y desempeño institucional, que, implementadas de manera articulada e intercomunicada, permitirán que el MIPG funcione. El SGSI se alinea con la **dimensión 3 "Gestión con Valores para resultados"**, el propósito de esta Dimensión es permitirle a la organización realizar las actividades que la conduzcan a lograr los resultados propuestos ya a materializar las decisiones plasmadas en su planeación institucional, en el marco de los valores del servicio público.



Dimensiones

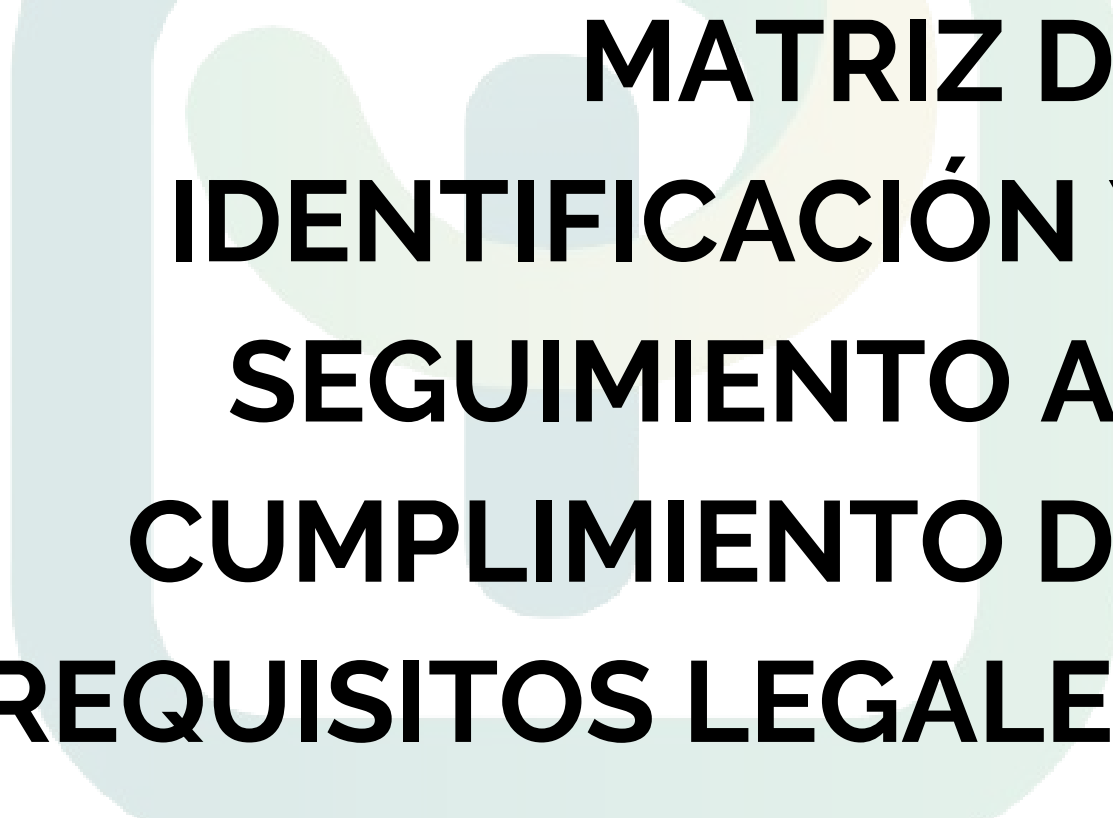
Lineamientos de la Política de Gobierno Digital

La Universidad de Cundinamarca, como sujeto obligado, debe implementar la Política de Gobierno Digital, esta cuenta con los componentes tic para el estado y tic para la sociedad, así como con tres habilitadores transversales, servicios ciudadanos digitales, arquitectura TI y Seguridad y Privacidad, este último se logra a través del Modelo de Seguridad y Privacidad de la Información propuesto por el MinTIC y su objetivo es que las entidades públicas integren la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información e infraestructura, con la finalidad de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

COMPONENTES



HABILITADORES TRANSVERSALES



MATRIZ DE IDENTIFICACIÓN Y SEGUIMIENTO AL CUMPLIMIENTO DE REQUISITOS LEGALES Y OTROS DEL SGSI

Contextualización

El Sistema de Gestión de Seguridad de la Información – SGSI, cuenta con un marco normativo tanto externo como interno que posibilita una correcta implementación del SGSI y el Programa Integral de Gestión de Datos Personales – PIGDP.

1

E
X
T
E
R
N
A

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.

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."

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

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

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

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 2º y 13º".

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"

I
N
T
E
R
N
A

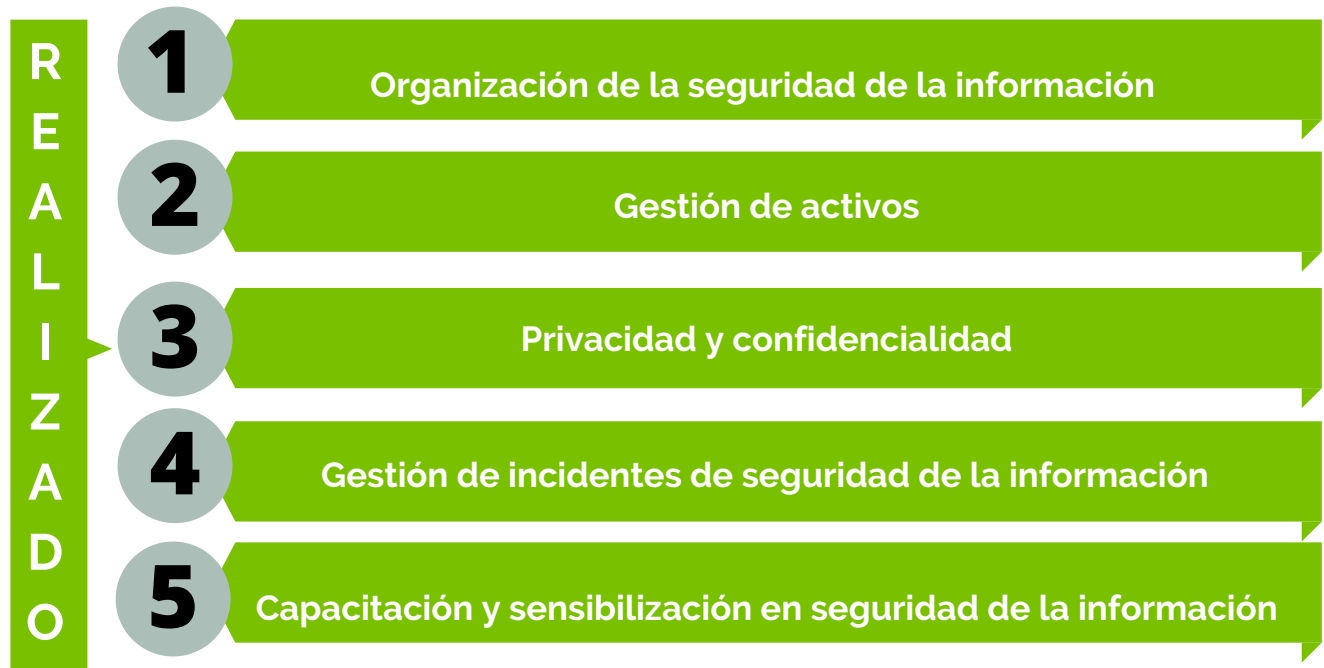
2



POLÍTICAS INSTITUCIONALES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

POLÍTICAS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Dentro de los requerimientos realizados por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, para la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, está la adopción de 10 políticas específicas enfocadas dar cumplimiento tanto a los numerales y controles de la norma ISO 27001:2013 como a la normatividad legal vigente en materia de protección de datos personales.



Fuente: Sistema de Gestión de Seguridad de la Información - SGSI



ROLES Y RESPONSABILIDADES EN EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

MANUAL DE ROLES Y RESPONSABILIDADES EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - ESG-SSI-M004

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 Sistema de Gestión de Seguridad de la Información - SGSI, a fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información, así como dar cumplimiento a la Ley de Protección de Datos Personales y la Guía de Responsabilidad Demostrada de la Superintendencia de Industria y Comercio - SIC.

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.

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.

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 presente 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.

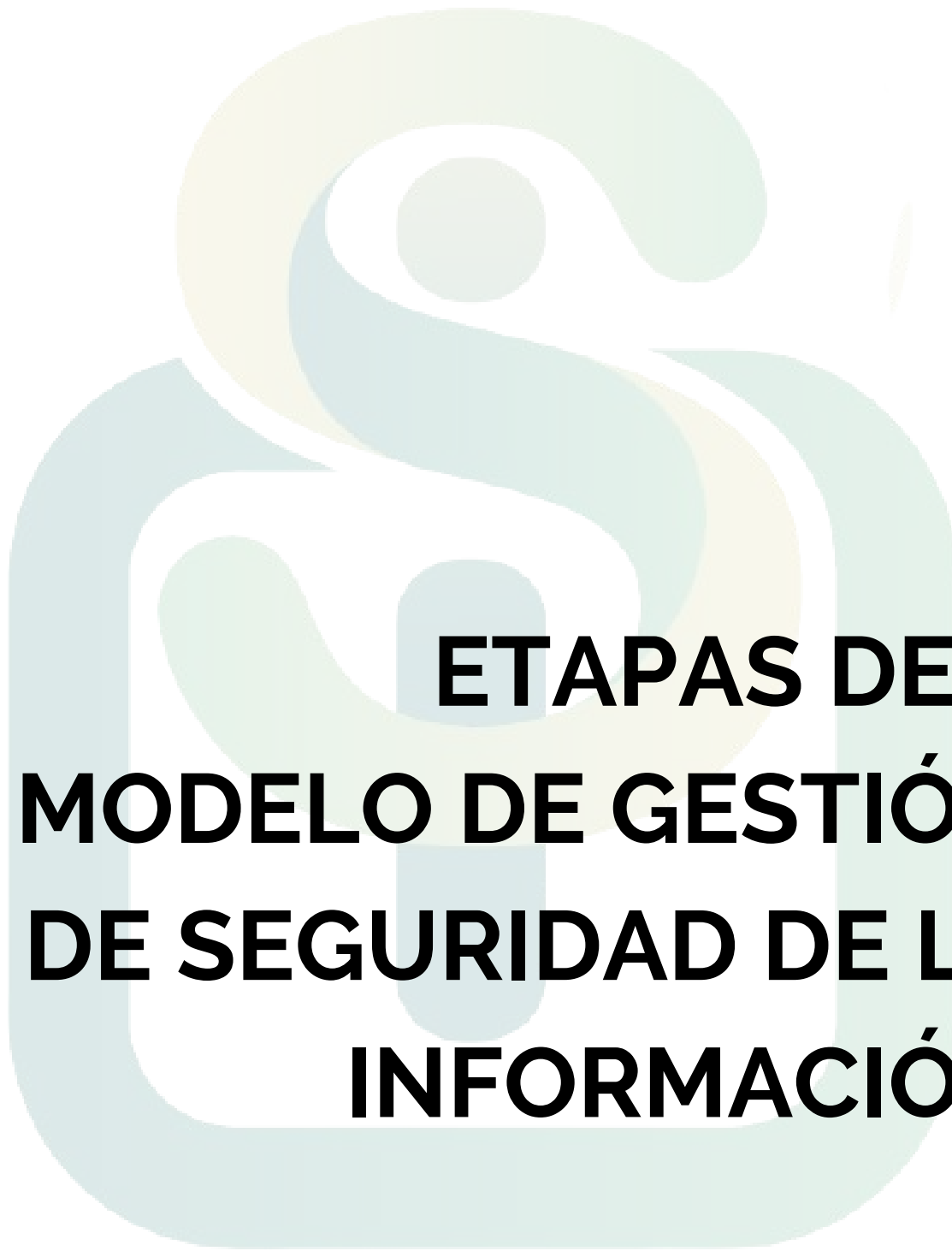
COMITÉ DEL SISTEMA DE ASEGURAMIENTO DE LA CALIDAD – SAC Y COMISIÓN DE GESTIÓN

- 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.

FUNCIONARIOS ADMINISTRATIVOS Y DOCENTES

- Reportar cualquier irregularidad que se llegare 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.

Fuente: MANUAL DE ROLES Y RESPONSABILIDADES EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - ESG-SSI-M004



ETAPAS DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

ISO 27001 | Gestión Integral de la Seguridad de la Información | SGSI

Descripción General

La implementación del Sistema de Gestión de Seguridad de la Información – SGSI, se realiza a través de 6 etapas articuladas en torno a la Gestión de la Estrategia, así como asegurar los principios de confidencialidad, integridad y disponibilidad de la información como activo esencial en una organización.

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.



Fuente: ISO 27001 | Gestión Integral de la Seguridad de la Información | SGSI

Etapa 1 : Gestión de Activos de la Información

Descripción General

En el desarrollo de esta primera etapa se siguen los lineamientos planteados en la norma ISO 27001:2013 para la gestión de activos de información, entendiendo que se denomina activo de la Información a todo aquello que tiene valor para la institución, ya que es un elemento que contiene información, manipula información o ayuda a los funcionarios a generar información de valor para la institución y que por tanto se debe proteger.

01

ACTIVO DE INFORMACIÓN

Es el elemento de información que la institución recibe o produce en el ejercicio de sus funciones. Tiene un valor y se debe proteger.

ROLES EN LA CLASIFICACIÓN Y MANEJO DE LOS ACTIVOS DE INFORMACIÓN

02

RESPONSABLE DE LA PRODUCCIÓN DE LA INFORMACIÓN (PROPIETARIO)

Es una parte designada de la institución, responsable del proceso que tiene el compromiso de garantizar que la información y los activos se clasifiquen adecuadamente, además definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta la confidencialidad, integridad y disponibilidad de los mismos.

03

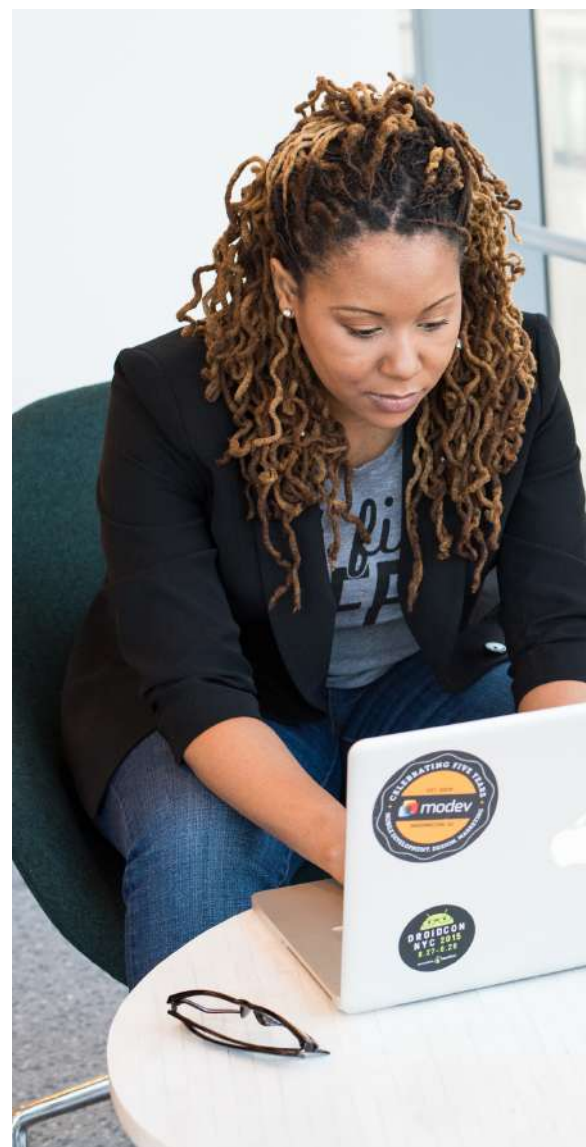
RESPONSABLE DE LA INFORMACIÓN (CUSTODIO)

Es una parte designada de la institución, un cargo, proceso o un área institucional encargada de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado

04

USUARIO DE LA INFORMACIÓN

Cualquier persona (estudiante, docente, administrativo, proveedor o comunidad), entidad, cargo, proceso o un área institucional, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital o a través de los sistemas de la información de la institución, para propósitos propios de su labor (que estén autorizados previamente por el Propietario para su uso y/o disposición).



PRINCIPIOS PARA RESGUARDAR LOS ACTIVOS DE INFORMACIÓN

05 CONFIDENCIALIDAD

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

06 INTEGRIDAD

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

07 DISPONIBILIDAD

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 da a conocer las actividades necesarias para realizar la identificación, clasificación y etiquetado de los activos de información de la Institución.

GUIA PARA REGISTRO EN EL APLICATIVO
DENOMINADO GESTIÓN DE ACTIVOS -
ESG-SSI-G001

INSTRUCTIVO PARA EL REGISTRO
DE ACTIVOS DE LA INFORMACIÓN
- ESG-SSI-I001

CHECKLIST PARA ENTREGA Y
DEVOLUCIÓN DE ACTIVOS DE LA
INFORMACIÓN - ESG-SSI-F010

Etapa 2 : Gestión de Riesgos

Descripción General

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.

Numeral 6 - 8 de la norma ISO IEC 27001/2013

Guía 7 Gestión de Riesgos del Modelo de Seguridad y Privacidad de la Información – MSPI – MinTIC

Guía para la administración del riesgo y el diseño de controles en entidades públicas , Versión 5 del 2020, emitida por el Departamento Administrativo de la Función Pública – DAFP

Anexo 4 - Lineamientos para le gestión de riesgos de seguridad digital en entidades públicas generada por el MinTIC.

ESG-SSI-P12- GESTIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A través de este procedimiento se da a conocer la metodología adoptada para la gestión de riesgos asociados a seguridad y privacidad de la información, siguiendo los lineamientos de MinTIC y el Departamento Administrativo de la Función Pública - DAFP en sus respectivas guías, para la identificación, valoración y tratamiento de riesgos.

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

A través de este manual se da a conocer la metodología adoptada para la gestión de riesgos asociados a seguridad y privacidad de la información, siguiendo los lineamientos de MinTIC y el Departamento Administrativo de la Función Pública - DAFP en sus respectivas guías, para la identificación, valoración y tratamiento de riesgos.

Etapa 3 : Gestión de Incidentes

Descripción General

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.

Este procedimiento describe las actividades que se siguen dentro de la Universidad al momento de identificarse o materializarse un incidente de seguridad que pueda comprometer la confidencialidad, integridad o disponibilidad de la información; asignando responsabilidades y documentando lo sucedido como lecciones aprendidas.

ESG-SSI-P09 - GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

MANUAL DE ROLES Y RESPONSABILIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - ESG-SSI-M004

ESG-SSI-P10- REPORTE DE INCIDENTES DE PROTECCION DE DATOS PERSONALES

El procedimiento informa a la comunidad universitaria el paso a paso que deben realizar si identifican o sospechan la materialización de un incidente de seguridad relacionado con la recolección, almacenamiento, uso o circulación de datos personales de Titulares dentro de la Institución.

GUIA PARA REALIZAR REPORTE Y VALORACIÓN DE INCIDENTES DE PROTECCIÓN DE DATOS PERSONALES - ESG-SSI-G004

REPORTE DE INCIDENTES DE PROTECCIÓN DE DATOS PERSONALES - ESG-SSI-F025

CONSOLIDADO DE INCIDENTES DE PROTECCIÓN DE DATOS PERSONALES - ESG-SSI-F026

¿Cómo proteger la información y los datos personales ?

- 1 No dejar el computador desbloqueado cuando deje el sitio de trabajo.
- 2 Descarga archivos únicamente de sitios certificados.
- 3 Comprueba la veracidad del correo recibido puedes ponerte en contacto con la empresa o el servicio que supuestamente te ha enviado el correo.
- 4 Tener contraseñas distintas para mi aula virtual, plataforma y correo institucional.
- 5 Nunca respondas a correos que te soliciten datos confidenciales
- 6 Usa contraseñas fuertes mezclando mayúsculas, minúsculas y números. Tienen que ser fáciles de recordar para usted y difíciles de adivinar por otros.

Etapa 4 : Gestión del Cumplimiento

Descripción General

A través de esta etapa, 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.

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 Afilaciones 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

Dando cumplimiento a los lineamientos dados por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, se ha adoptado el ESG-SSI-PL01 – Plan de Sensibilización y Entrenamiento en Seguridad y Privacidad de la Información, así como el ESG-SSI-PG01 – Programa Integral de Gestión de Datos Personales que a su vez reúne 6 procedimientos referentes a la recolección, almacenamiento, uso y circulación, consultas y reclamos, supresión y transferencia internacional 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-P02 - CONSULTAS Y RECLAMOS DE DATOS PERSONALES

ESG-SSI-P05 - USO Y CIRCULACIÓN DE DATOS PERSONALES

ESG-SSI-P03 - RECOLECCIÓN DE DATOS PERSONALES

ESG-SSI-P06 - SUPRESIÓN DE DATOS PERSONALES

ESG-SSI-P04 - ALMACENAMIENTO DE DATOS PERSONALES

ESG-SSI-P07 - TRANSFERENCIA INTERNACIONAL DE DATOS PERSONALES

Etapa 5 : Gestión de la Continuidad del Negocio en proceso

Descripción General

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 en proceso

Descripción General

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.



REGISTRO NACIONAL DE BASE DE DATOS – RNBD

Registro Nacional de Base de Datos – RNBD

Descripción General

El Registro Nacional de Base de Datos – RNBD es un requerimiento realizado por la Superintendencia de Industria y Comercio – SIC, a todas las entidades que cumplan los requisitos dispuestos en el capítulo 26 del Decreto Único 1074 de 2015 referente a las bases de datos sujetas a la aplicación de la Ley 1581 de 2012.

ESG-SSI-P13 - REGISTRO NACIONAL DE BASES DE DATOS

Establecer los lineamientos a seguir, conforme lo establece el manual de usuario para el Registro Nacional de Bases de Datos de la superintendencia de Industria y Comercio - SIC, atendiendo la normatividad legal vigente.

ESG-SSI-G005 - GUIA PARA EL REGISTRO DE LAS BASES DE DATOS INSTITUCIONALES

ESG-SSI-F030 - REGISTRO DE LAS BASES DE DATOS INSTITUCIONALES

ESG-SSI-F031 - CONSOLIDADO DEL REGISTRO DE LAS BASES DE DATOS INSTITUCIONALES

¿Pasos para registrar las base de datos ?

- 1** IDENTIFICAR LA FINALIDAD EN EL ESG-SSI-M001 - MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (Numeral 5.1).
- 2** REPORTAR DE LA BASES DE DATOS EN EL FORMATO ESG-SSI-F032 - REGISTRO DE LAS BASES DE DATOS INSTITUCIONALES.
- 3** REGISTRO AL RNBD POR EL OFICIAL DE TRATAMIENTO DE DATOS - OTD ESG-SSI-F033-CONSOLIDADO DEL REGISTRO DE LAS BASES DE DATOS INSTITUCIONALES
- 4** REPORTE DE NOVEDADES



UDEC
UNIVERSIDAD DE
CUNDINAMARCA

Dirección de Sistemas y Tecnología
Sistema de Gestión de Seguridad de la Información

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